*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

---

**TITLE:**
**Information Warfare in the Digital Age – Propaganda, Cyberattacks and the Protection of Democratic Institutions**

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

**AUTHOR:**

Major Isaac Shults

AY 2021-22

---

MMS Mentor Team and Oral Defense Committee Member: Paul D. Gelpi, PhD

Approved: _____
Date: _____

MMS Mentor Team and Oral Defense Committee Member: James H. Joyner, Jr., PhD

Approved: _____
Date: _____

# Executive Summary

**Title**: Information Warfare in the Digital Age – Propaganda, Cyberattacks and the Protection of Democratic Institutions

**Author:** Major Isaac Shults, United States Marine Corps

**Thesis:** To counter threats posed by information warfare, the United States must protect its interests and uphold the values and institutions of democratic governance through proactive, rational, and unbiased security policy and oversight, technology advancements, and digital literacy education and public awareness.

**Discussion:** State and nonstate actors use cyberspace and the information environment to engage in gray zone conflict against the United States. Information warfare and cyberattacks conducted by government-controlled, government-sponsored, and nonstate actors exploit the vulnerabilities of US civil liberty protections and exacerbate extant political polarization to attack and undermine US institutions and interests. The incorporeal nature of threats in cyberspace and the information environment is further complicated by misinformation and disinformation campaigns designed to cast doubt on the credibility of individuals and institutions attempting to warn and guard against the threat. There are technological, psychological, and procedural conditions that contribute to US susceptibility to information warfare attacks. These three conditions are the categories that must be considered when developing solutions to combat threats and attacks in the information environment in order to develop a comprehensive approach to address the threats posed by malevolent actors while maintaining the public trust.

**Conclusion:** The United States must ensure that national security solutions to information warfare attacks strike the appropriate balance between liberty and security to maintain public trust and defend national interests through security policy and oversight, technology advancements, and digital literacy education and public awareness.

# DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

# TABLE OF CONTENTS

# *Acknowledgements*

I would like to take this opportunity to thank the Marine Corps University Command and Staff College faculty whose input and tutelage were integral to the completion of this paper and my continued professional development. To Dr. Paul Gelpi and Dr. James Joyner, I am truly grateful for the opportunity to have been a member of your Strategic Dialogue. Your class was invaluable for developing strategic level perspective for my professional level application. Dr. Gelpi, your input and guidance on how to conceptualize information for my MMS are tools that I will use for the rest of my career.

I would also like to thank Dr. Claire Metelits and Dr. Lon Strauss, the Civilian Faculty Advisors for Conference Group 1. Your engagement, critical feedback, and challenge of assumptions have made Command and Staff College a rewarding experience.

## Introduction

Threats and attacks in the information environment and cyberspace pose clear and definite risks to US national security. However, the US public is unaware of the extent of the threat posed by malevolent actors such as China, Russia, and violent extremist organizations (VEOs) because of ambiguity about the nature of the conflict, opacity of the parties involved, and uncertainty about the relevant policy and legal framework applicable to such threats.[1]

Cyberattacks have the potential to infiltrate and disrupt the information systems necessary for US economic and national security activities. However, when combined with a holistic information warfare campaign, the repercussions of cyberattacks extend far beyond their immediate financial and physical security impacts. Information attacks targeting the credibility of our system of government damage the public trust in institutions necessary to the functioning of a liberal democracy. Without care, the policy and security solutions implemented to counter information warfare will undermine the democratic institutions and ideals the United States seeks to protect. Policies implemented in fear and based on misinformation and disinformation are ineffective and advance the cause of those attacking the United States. Therefore, the United States must protect its interests and uphold the values and institutions of democratic governance through proactive, rational, and unbiased security policy and oversight, technology advancements, and digital literacy education and awareness.

State and nonstate actors use cyberspace and the information environment to engage in gray zone conflict against the United States. The hybrid integration of information warfare, cyberattacks, psychological warfare, cybercrime, and cyberespionage against a US government established on free speech and the right to privacy presents a complex problem set. Information

warfare and cyberattacks conducted by government-controlled, government-sponsored, and nonstate actors exploit the vulnerabilities of US civil liberty protections and exacerbate extant political polarization to attack and undermine US institutions and interests. The result is a politically divided US population that is as fearful and suspicious of solutions to counter foreign information warfare as the threat posed by malicious actors.

The incorporeal nature of threats in cyberspace and the information environment makes it difficult for the US population to understand the threat. This is further complicated by misinformation and disinformation campaigns designed to cast doubt on the credibility of individuals and institutions attempting to warn and guard against the threat. The distrust sown by information warfare attacks renders US officials and institutions seeking to implement legal and policy solutions designed to address foreign information warfare threats vulnerable to information attacks.

The complexity of defining and addressing threats in the information and cyber domains is illustrated in the analogies used to discuss them. For example, cyberattacks are referred to as a "Cyber Pearl Harbor" and "Cyber Armageddon."[2] In addition, discussions regarding protected speech often fail to distinguish social media from the internet and incorrectly describe both terms as the "new public square"[3] While these analogies are employed to relate complex and ambiguous threats to familiar concepts, they fail to achieve the desired effect because the nuance is lost in the simplicity of the analogy. A "Cyber Pearl Harbor" does not result in the visual and emotionally jarring scenario of US Navy ships burning and sinking in US ports. Propagandists on social media are not identifiable as foreign adversaries shouting in the public square. Analogies used to highlight danger and importance become counterproductive when they fall

short of expectations, are subsequently ignored by the public or become incorporated into the very information warfare attacks the analogies are intended to address.

The United States has dealt with foreign threats and the fear of foreign threats before, and it bears the scars of those reactions. The Red Scares after World War I and World War II are part of social consciousness in memories of McCarthyism, Japanese internment camps, and the abuses of US intelligence and law enforcement during the 1950s, 1960s, and 1970s.[4] In recent years, information leaked by hackers, activists, and whistleblowers has contributed to public distrust of US intelligence collection programs.[5] Foreign adversaries exploit this public distrust, and US efforts to guard against foreign aggression in the information environment are viewed with skepticism. US policymakers and national security professionals face the difficult task of guarding against attacks that exploit US legal protections and play upon public distrust of government remedies. In order to accomplish this task, the US must develop a comprehensive model of technological solutions, public-private partnerships, public awareness/education, and narrowly focused legislation and policy reform to target malevolent actors without infringing upon the rights of US citizens or losing public trust.

Part I of this paper outlines pertinent terms and definitions that play an essential role in understanding the nature of threats and attacks in the information environment and cyberspace. Part II notes various state and nonstate actors that execute activities in the information environment and cyberspace. It also discusses Russian operational units that conduct information and cyberattacks. Part III examines the technological, psychological, and procedural conditions that contribute to US susceptibility to information warfare attacks. It also provides a case study of the SolarWinds attack. Part IV sets forth the categories that must be considered when

developing solutions to combat threats and attacks in the information environment. It also includes suggestions to develop a comprehensive approach to address the threats posed by malevolent actors while maintaining the public trust.

**Key Terms and Definitions**

Several terms play an important role in understanding the complexities of threats and attacks in the information environment and cyberspace. First, the *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[6] *Information operations* are the "integrated employment … of information-related capabilities … to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries."[7] These *information-related capabilities* are tools, techniques, or activities employed within a dimension of the information environment to create effects and operationally desirable conditions.[8] Information-related capabilities are the weapons of information warfare, which uses and manages information to pursue a competitive advantage, including both offensive and defensive operations.[9] The dissemination of factual information is an important element of information operations, but the United States must guard against propaganda, misinformation, and disinformation employed by adversaries to undermine US national interests.

Further, how information is distributed within the information environment is critical to understanding the nature of the threat and countering it. As such, the use of cyberspace for the distribution of information is central to this discussion. The information environment encompasses more than cyberspace alone, but the characteristics of cyberspace increase its prevalence in the context of information warfare. Cyberspace is a global domain within the information environment that consists of the interdependent network of information technology

infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.[10] Cyberspace has given rise to new versions of old activities, like cybercrime, cyberterrorism, and cyberespionage, but with the technical and policy complexities of defending against these threats in the cyber domain.

Information-related capabilities that utilize cyberspace present an especially complex set of problems for the United States, both from a technical and policy standpoint. It is essential to differentiate between cyberattacks/cyberterrorism/cybercrime and cyber-enabled activity. A criminal activity that occurs in cyberspace is not necessarily a cyberattack. For example, cyberterrorism is the "unlawful attack and threat of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[11] However, cyberterrorism is distinguishable from cyber-enabled terrorist attacks or activities, such as a terrorist organization that uses social media and online banking to recruit, plan, and fund terrorist activities. Both have elements within cyberspace, but only cyberterrorism would be considered a cyberattack. This difference is essential to understanding the means and methods of countering attacks and which organizations have the authority and ability to do so.

It is also important to differentiate between crime and espionage enabled by cyber activity and criminal and espionage operations conducted using cyber tools/attacks. Cyber-attacks use malicious computer code to disrupt computer processing or steal data, as opposed to computer-enabled social engineering attacks that exploit human behavior to gain access to information or systems. [12] A comprehensive discussion of cyber-attacks is well beyond the scope of this paper, but there are a few terms that are specifically relevant to the examples that will be discussed. The first is *ransomware*, defined as malicious software, or malware, that prevents

access to computer files, systems, or networks and demands a ransom for their return. Ransomware attacks result in costly disruptions to operations and critical information and data loss.[13] The second term is *Advanced Persistent Threat* (APT), which is an adversary with sophisticated levels of expertise and significant resources. Through the use of cyber, physical, and deception methods, APTs generate opportunities to achieve objectives by establishing and extending footholds within the information technology infrastructure of organizations.[14] This allows APTs to continually exfiltrate information or undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future.[15] In addition, APT is sometimes used to refer to the attack itself rather than the actor.[16]

Finally, the term *gray zone conflict* is important to this discussion as it describes the nature of the ongoing conflict and operations undertaken by adversaries of the United States. *Gray zone challenges* are competitive interactions among and within state and nonstate actors that fall between the traditional war and peace duality and are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks.[17] Consequently, gray zone conflict is "another type war, new in its intensity, ancient in its origin."[18] Aggressive yet ambiguous operations in cyberspace and the information environment are potent elements of gray zone conflict.

**State and Non-State Malevolent Actors**

There are numerous examples of state and nonstate actors that execute various activities in the information environment and cyberspace. Many state and nonstate actors use information-related technologies for a variety of operations. The methods and tools of these actors are as numerous as the actors who conduct them. The capabilities and goals of malevolent actors

dictate the tools and tactics to achieve their ends. The variety of threats in the information environment necessitates various solutions, and the United States must be prepared to address a wide variety of threats with a wide variety of solutions.

This paper focuses on Russia, China, and VEOs, but these are only three of the numerous malevolent actors operating in the information environment and cyberspace. North Korea and Iran are additional examples of nation-states with well-resourced and sophisticated cyber-attack and information warfare capabilities. North Korea and Iran pose significant threats to US interests, both in their sophistication and willingness to attack and undermine US interests, but they are currently not as pervasive as China nor as disruptive as Russia.[19] The focus is predominantly on Russia because it displays a range of capabilities and tactics in cyber space and the information environment similar to threats posed by many other state and nonstate actors.

*Violent Extremist Organizations*

VEO like Al-Qaida and the Islamic State (ISIS) are examples of adversarial nonstate entities operating in cyberspace and the information environment with goals counter to the United States. These entities use cyberspace and the information environment to promote ideology, recruit, raise funds and spread fear. Organizations like Al-Qaida and ISIS create and use public and private websites to support their training, education, and recruitment goals and illicit funds. They are active on social and traditional media and will engage in cybercrime to raise and distribute funds.[20] ISIS, for example, employs a full-spectrum information operations campaign that links military operations to political/ideological objectives to create a unified narrative far beyond the geographic areas of Iraq and Syria. It promotes terrorist activities conducted in one region to garner financial and ideological support from a dispersed online

community. ISIS tailors its messages and propaganda to radicalize and appeal to potential recruits, thus establishing a network of supporters willing to collect information, conduct operations, and relay funds and messages worldwide, despite having no centralized physical location of leadership and coordination. The broad and decentralized dispersion of ISIS propaganda attracts followers, who then conduct terrorist activities amplified and promoted through the ISIS messaging campaign, thereby drawing additional followers.

VEO activities in cyberspace are not purely ideological. Al-Qaida, ISIS, and other VEOs engage in cybercrime to raise funds for terrorist activities, and the use of cybercrime for this purpose further illustrates the interrelated nature of activities in cyberspace. For example, a group of terrorists in the UK was convicted of using stolen credit card information to purchase military equipment online, including night vision and GPS, hundreds of prepaid cell phones, and over 250 airline tickets for jihadist fighters. The group registered hundreds of internet web domains and laundered thousands in stolen money. The terrorists charged more than $3.5 million using a database containing more than 37,000 stolen credit card numbers.[21] These individuals provided equipment, funds, and information to support terrorist activities while harboring under the protections of a democratic country that upholds the laws of free speech and privacy that they used to espouse their beliefs and hide their activities.

*China*

VEOs and nonstate actors are not the only malevolent organizations that benefit from global communications technologies and democratic civil liberties. China is an example of a state actor routinely active in the information environment and cyberspace. China does not take the same information warfare and propaganda approach as Russia or VEOs. While both Russia

and China mix cyber and information operations with other elements of national power, China takes a more measured approach to disseminating information and offensive cyber tactics. To better explain the contrast between China and Russia, if Russia is best described as a hurricane due to its visibly disruptive and damaging tactics, China's implacable and pervasive slow advance would be comparable to climate change.[22] The centralized, measured, controlled, and long-term outlook of Chinese actions in cyberspace and the information environment are characteristic of Chinese strategy for information warfare.

China is known to adopt a holistic and measured approach in its information warfare campaigns. For example, China's consistent messaging concerning its claims in the South China Sea is part of a coherent narrative to legitimize its activities. In addition, China's offensive cyber operations are primarily focused on governmental, economic, and industrial espionage. General Keith Alexander, who directed the National Security Agency from 2005 to 2014 and dual-hatted as the first commander of US Cyber Command from 2010 to 2014, described China's success in these endeavors as "the greatest transfer of wealth in history."[23] In contrast to the disruptive tactics of Russian aligned hackers, China focuses on "slow burn" offensive cyber operations, where their goal is not to break the current world order in which they hold a strong position but rather to shape the current world order for continued advantage.[24] For instance, the cybersecurity group FireEye has identified at least ten APTs operated by the Chinese Communist Party, with nine such threats focused on industrial espionage.[25] China's creation of the Strategic Support Force (SSF) to combine cyber operations with space, electronic warfare, and psychological warfare is part of the Chinese strategy for an integrated campaign for conflict with the United States.[26] China also co-opts a large civilian hacker network when necessary. Through its extensive and intrusive domestic cyber monitoring practices, China knows the identities and

activities of Chinese civilian hackers. It uses these hackers as a proxy force extension of the state to retain deniability while maintaining an intrusive forward cyber presence.[27] These efforts are part of the Chinese strategy to obtain information superiority in future conflicts against a more powerful adversary like the United States.

*Russia*

Russia is one of the most active US adversaries in cyberspace and the information environment. Russia integrates political, economic, and informational elements into its cyber operations in a hybrid warfare model called "asymmetric methods."[28] Russia's integrated strategy of using information warfare early and often is indicative of the fact that it makes no distinction along the spectrum of conflict as to when information operations are employed. Russia takes the approach that the holistic use of information operations is a valid and valuable counter to the United States' asymmetric advantage in conventional military power. Russia does not view the current world order as beneficial to its interests and is more willing to accept risk in its disruptive approach.[29] Russia does not wield the same economic and political clout as China, and it acts aggressively in cyberspace and the information environment to offset its weaker political and economic position.[30]

Russian information warfare provides examples of numerous capabilities and actions in cyberspace and the information environment and how these capabilities are integrated. Russian offensive cyber operations consist of combinations of high volumes of brazen cyber-attacks along with highly sophisticated and technically advanced persistent threat attacks. Russian activities in cyberspace and the information environment include the implanting of malicious software (malware) for information gathering (e.g., Solar Winds), use of ransomware for

financial gain (e.g., the Colonial Pipeline attack), dissemination and reinforcement of propaganda and disinformation using bots and false personas on social media (e.g., Fancy and Cozy Bear), and the use of media outlets, such as the *Russian Times*. Russia's propaganda is overwhelming in volume and employs combinations of outright disinformation with more subtle and ambiguous misinformation distributed by an array of actors in cyberspace.[31] The Russian "firehose of falsehood" for propaganda is consistent with its overall cyber and information operations approach.[32] Russia has multiple operational elements capable and authorized to execute offensive and defensive cyber operations as well as information warfare operations in the cyber domain. Russian cyber activities are associated with four primary elements within Russia. Each element has an area of focus and specialization. However, due to the holistic approach Russia takes with information operations and cyber activities, there is some inherent overlap that can sometimes result in inefficiencies and the activities of one element interfering with the activities of another. Russia seems content with these perceived inefficiencies as worthwhile tradeoffs for the advantages of wide-ranging and high-volume activity against the US and other adversaries.

## The Main Directorate of The General Staff

The Main Directorate of The General Staff (GRU) is Russia's military intelligence agency. It is often characterized by brazen and aggressive operations, including hack and dump attacks against political targets in the United States and Europe.[33] In addition to information gathering by penetrating networks and databases, units of the GRU have also been responsible for the delivery of malicious code, or malware, as in the NotPetya Attack of 2017 and numerous Ukrainian targets in 2016 which ultimately spread to countries and businesses beyond Ukraine.[34] Along with cyber-attacks to penetrate and compromise networks to steal information and deliver

malware, other elements of the GRU are responsible for psychological operations, including the spreading of misinformation and disinformation online via social media and news sites.[35]

## The Federal Security Service

The Federal Security Service (FSB) is a Russian domestic security agency responsible for counterintelligence operations and internal security for the Russian government. Its mission includes monitoring domestic civilian hackers and foreign cyberattacks against Russia. In line with Russia's broad approach to cyber operations and information warfare, the FSB has also expanded into foreign intelligence collection and offensive cyber operations in a defend-forward tactic. The FSB has the ability to develop advanced malicious software, and there is evidence that it was responsible for a 2017 hack of Yahoo and an overarching focus on the penetration of infrastructure and energy sector targets, as well as state and local government targets, likely to deliver malware that can be used in future attacks. Additionally, the FSB works closely with civilian hackers to augment staff and operations.

## The Internet Research Agency

One civilian organization with strong links to Russian sanctioned cyber operations is the Internet Research Agency (IRA). While a private company, it is funded by a Russian oligarch known to back the Kremlin. The IRA is a significant player in spreading Russian disinformation and propaganda, primarily through internet trolls and bots on social media.[36] A report provided to the Senate Select Committee on Intelligence (SSCI) estimates that during the 2016 election, the IRA directly reached as many as 30 million individual users in the United States on Facebook and Instagram. IRA messages were then shared, reaching as many as 126 million additional users.[37]

### The Foreign Intelligence Service

The Foreign Intelligence Service (SVR) is Russia's civilian foreign intelligence branch. It collects foreign intelligence using human intelligence, signals intelligence, and various cyber methods. Unlike the brazen operations of the GRU, the SVR emphasizes secrecy and detection avoidance. The SVR is an Advanced Persistent Threat (APT) in that they seek to collect intelligence using high levels of technical expertise to gain and retain long-term access inside compromised networks. Elements of the SVR, known variously as APT29, Cozy Bear, and the Dukes, have been associated with numerous clandestine cyber operations. The most notable of these, referred to by some security officials as a kind of Cyber Pearl Harbor, was the SolarWinds attack against US Government computer information systems.

## Us Susceptibility to Information Warfare Attacks

Many variables contribute to US susceptibility to information warfare and cyber-attacks. However, this section discusses the primary conditions that render information warfare and cyber-attacks conducted by foreign adversaries against the United States particularly potent and difficult to defend. First, foreign adversaries exploit foundational US legal protections intended for US citizens. Second, adversarial actors are increasingly skilled at leveraging technology to enhance psychological warfare techniques. Finally, advances in technology have led to a society increasingly dependent on digital technology providing endless targets and opportunities to exploit the natural tendencies of human psychology, US legal protections, and critical infrastructure and key resources.

*US Legal Protections*

The United States prides itself on the protection of civil liberties, open public dialogue, and free and fair elections. These elements are interwoven and necessary to a well-functioning liberal democracy. The First Amendment of the US Constitution protects freedom of speech, the press, and assembly, and the Fourth Amendment protects against unreasonable search and seizure by the government. Political speech is the most protected form of speech under the First Amendment, and laws that regulate it are subject to the highest level of scrutiny.[38] The First and Fourth Amendments are foundational to the civil liberties of the citizens of the United States, but they offer protection to enemies of the United States who exploit the free flow of information and ideas provided by our society. The US legal framework designed to protect Americans restricts the United States' ability to counter information warfare and cyber-attacks.[39] Guarding national security without undermining US civil liberties is a difficult balance to strike.

*Psychological Susceptibility to Propaganda, Misinformation, and Disinformation*

Adversarial actors are increasingly skilled at leveraging technology to enhance psychological warfare attacks that are particularly difficult to defend. Information warfare exploits an audience's biases and preconceived notions, reinforcing what they want to hear, playing on existing fears, and casting doubt on counter-narratives.[40] Past oversteps in US authority resonate in the consciousness of the US population and raise fears of future governmental overreach. [41] Russian information campaigns incorporate these fears in their propaganda to undermine confidence in US institutions and stimy unified efforts to combat Russian information warfare and cyber-attacks. Information warfare attacks are designed to inflate this fear and overwhelm an audience with sheer volume, whereby competing messages

are drowned out, and the quantity of reinforcing sources of information adds credibility to the message, regardless of its accuracy.[42]

For example, Russian propaganda is described as a "firehose of falsehood."[43] Russia's approach is predicated on a 1) high volume of information, 2) rapid, continuous, and repetitive dissemination of a message, 3) a lack of commitment to objectivity, and 4) a lack of consistency. First, Russian actors like the IRA's army of trolls and bots distribute a high volume of information across information channels, such as the internet, social media, radio and television. The information is disseminated rapidly, continuously, and repetitively. The speed, volume, and multiple avenues of dissemination often lead to discrepancies in a unified message, but this is an accepted characteristic of Russian propaganda. So long as propaganda is carried out along loosely defined themes to sow dissent, increase polarization, or undermine confidence, Russia accepts the lack of consistency in exchange for speed and volume of messaging.[44]

Russian information warfare is designed to exploit basic psychological traits. Multiple sources of information are viewed as supporting evidence for each other, especially when the same conclusion is presented as having been reached from multiple arguments. Additionally, by using bots and false personas, Russia can deliver messages that appear to come from within a social group and from the perspective that the receiver already agrees with on other topics. If it appears that many people within a social group already believe a given piece of information, the more likely other members of that same group will be to believe the information, regardless of voracity. Russian propaganda's rapid, continuous, and repetitive nature also plays on the resiliency of first impressions, the impacts of repeated exposure, and confidence in and favoritism for familiar information.[45]

The Russian information operations during the 2015-2016 election cycle are prime examples of cyber based information operations and political warfare. The 2016 election interference undermined confidence in US elections and institutions by highlighting and amplifying the perception that democratic institutions are corrupt and untrustworthy.[46] These effects were exacerbated when Russian activities received mixed, politically motivated responses within the United States, with some US officials condemning Russian interference and others downplaying the interference to leverage the politically advantageous information revealed by the attacks.[47] Foreign information warfare hit its disruptive stride within this environment of domestic political debate and maneuvering, protected by US laws and customs and amplified by communication technology.

*Technology-Based Vulnerabilities*

The information revolution brought significant and continuous developments in information and communication technologies. Technologies used to increase convenience and accessibility have also increased the vulnerability of information to worldwide attacks. Networked technologies for communication, entertainment, banking, industry, and national defense, to name but a few, exponentially increase the opportunities and methods for state and nonstate actors to gain an advantage in the information age. Whether by stealing or disseminating information, disrupting services, or exploiting vulnerabilities for financial gain, the many advantages of networked technological advancements have also exposed individuals and institutions to threats that know no geographic boundary, operate behind the veil of cyber anonymity, and prey on ubiquitous dependence on digital technology.[48] Every online system is another opportunity to exploit a weak password, un-updated security patches, or inherently weak programming or system architecture. The number of networked systems and devices used by

people, governments, and industries has increased the targets and opportunities to exploit the natural tendencies of human psychology, US legal protections, and critical infrastructure and key resources.

SolarWinds – *A Case Study in the Confluence of Information Warfare and Cyberwarfare*

The events surrounding the SolarWinds cyber-attack provide an informative case study of the effectiveness of gray zone warfare tactics and the exploitation of US legal protections, technological opportunities, and psychological traits present within American society. Even after the United States discovered and eliminated the SolarWinds cybersecurity threat, Russian information operations capitalized on opportunities to exploit partisan divides, sow discontent, and undermine democratic institutions by leveraging messaging platforms established and protected within the US framework of free and protected expression.

The SolarWinds attack disclosed in December 2020 was one of the most sophisticated and large-scale cyber operations ever identified.[49] Approximately 18,000 private and public sector victims downloaded infected software between March and April 2020. A joint statement from the Federal Bureau of Investigation (FBI), Office of the Director of National Intelligence (ODNI), and National Security Agency (NSA) described the attack as "an Advanced Persistent Threat (APT) actor, likely Russian in origin" responsible for cyber compromises of both government and non-governmental networks.[50] The ambiguous characteristics of gray zone conflict, information operations, and cyberattacks left US officials wanting to convey the severity of the Russian attack in terms the American public could conceptualize, resulting in the SolarWinds attack being described as a Cyber Pearl Harbor. [51]

However, the information environment within the US had already been shaped by Russian information campaigns well before the SolarWinds attack. Russian information operation campaigns and hacking attacks exacerbating and amplifying partisan divides in the 2015-2016 election cycle continued through the mid-term elections of 2020. These events were made public by the intelligence community. Domestic figures attempted to capitalize on these attacks and employed the Cyber Pearl Harbor analogy to describe alleged interference in election machines to question the 2020 election results.[52]

In this heightened cyber threat environment against the background of an American public contending with worsening political polarization, the Russians further benefited from the SolarWinds attack when a debate arose over the use and efficacy of the Cyber Pearl Harbor analogy. [53] An open discourse, necessary in a democratic society, ensues regarding the nature and severity of the threat and its implications when an article, "The Cyber Pearl Harbor That Wasn't" is published by scholars within the United States discussing the dangers and misuse of the Cyber Pearl Harbor analogy for addressing threats in cyberspace. Selective parts of this free and open discourse are integrated into Russian information operations when the article is picked up and posted in December 2020 by the Strategic Culture Foundation, an online site controlled by the Russian SVR, ostensibly as part of the ongoing Russian campaign to downplay the threat of their activities and undermine US response efforts.[54]

By early 2021, the US Treasury Department named the Strategic Culture Foundation and 15 other websites in its "Assessment of Foreign Threats to the 2020 US Federal Election."[55] In response, conservative US websites not affiliated with Russia or its proxies respond that the US Government is attacking independent journalism and political dissent.[56] The US government's attempt to limit foreign agent media outlets is portrayed as an attack on independent journalism

and political discourse, reinforcing Americans' fears of government overreach and further undermining confidence in crucial US institutions.[57]

The events surrounding the SolarWinds attack are significant in that the actions and second and third-order effects were neither choreographed nor premeditated. Instead, the Russians exploited American society's interconnected and polarized nature, free speech, political rivalry, and partisan divides. The far-reaching connections of information technologies enhanced the opportunities for exploitation within a society that promotes freedom of expression and the protection of individual liberties. In the natural and necessary interactions and frictions between domestic groups in a liberal democracy, foreign actors found fertile ground to sow discontent and exploit confusion. Meanwhile, because of the nature of the threat and the environment, the US government's efforts to convey the attacks' severity to the American public were undermined, limiting the United States' capacity to respond effectively.

## Recommendations

There is no single solution to a problem as complicated as defending the United States against cyberattacks and information warfare attacks. US policymakers and national security professionals must develop and implement targeted countermeasures designed to address the vulnerabilities in legislation, policy, technology, and human nature that malevolent actors exploit. The following categories must be considered when developing solutions to combat threats and attacks in the information environment and cyberspace.

### *Legislation and Policy*

To combat threats and attacks in the information environment and cyberspace, US officials must address legislation and policy governing surveillance activities by law

enforcement and intelligence communities to strike the appropriate balance between granting of authority and oversight. Executive Order 12333, the Patriot Act, the USA FREEDOM Act, and FISA are government measures that sought to strike a balance between security and liberty. Executive Order 12333 governs the conduct of American intelligence activities and specifies the circumstances in which intelligence agencies can engage in foreign intelligence surveillance outside the United States.[58] It serves a vital role in oversight of the intelligence community. It requires intelligence agencies to execute their missions "in a vigorous, innovative, and responsible manner consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded."[59] Conversely, the Patriot Act, which granted law enforcement more powers to prevent terrorist attacks, has been criticized as an overbroad law that weakened American civil liberties for reasons unrelated to fighting terrorism.[60] Any new legislative or policy changes in the complex environment of cyberspace and information warfare must be narrowly tailored to balance national security with civil liberties through proper oversight and enforcement to withstand strict scrutiny review. However, they must still account for foreign adversaries' unprecedented volume and sophistication of targeted information warfare campaigns. The level to which malevolent actors can manipulate the presentation of information to specific, targeted audiences in the echo chambers of social media is unprecedented in human history. Further, the response to public fear or mistrust of government overreach cannot result in a backlash that hamstrings national security and law enforcement efforts. These solutions must be specific, technically accurate, and narrowly focused to meet the challenges of defending against attacks in cyberspace and the information environment. As we have seen in the past, the potential for abuse exists, but the answer is better oversight, not complete elimination of legal authority. The House and Senate Oversight

Committees on Intelligence, FISA Courts, public watchdogs, and whistleblower protection policies all contribute to the checks and balances necessary to uphold US national values while protecting US national interests.

US officials must consider enacting legislation and policy solutions to combat threats and attacks in the information environment and cyberspace. These measures could include regulations restricting foreign adversaries' abilities to interfere in the electoral process, such as by requiring that any paid political advertisements on social media include a clear statement of who paid for or is disseminating a message, similar to the requirements for traditional media.[61] Additionally, Congress should consider legislation to codify the application of the Third Party Doctrine, which allows the government access to personal information that has been shared with a third party and is an important tool for combating threats in the information environment but has come under judicial scrutiny.[62] Further, the US legislative and policy framework should make distinctions between the methods of intelligence gathering (e.g., electronic surveillance, collection of metadata, monitoring of social media), the context of intelligence gathering (e.g., for law enforcement, national security, wartime, peacetime, counter-terrorism efforts), and finally the targets of intelligence gathering (e.g., China, Russia, nonstate actors).[63] Finally, although political pressure and social responsibility have encouraged online platforms like Facebook, Twitter, and Google, to alter their platforms to combat fake news, the government could require online platforms to provide specific information to its users as an additional tactic to respond to the disinformation threat. [64]

*Technology*

In addition to legislative and policy measures to address threats and attacks in the information environment and cyberspace, the US must seek superiority in cyberspace and the

information environment through information technology research and development. This solution is simple in concept but highly complex in execution, and it involves the development and advancement of a wide array of related technologies. Artificial intelligence and machine learning are critical to processing the vast amounts of data necessary to identify and defend against threats in cyberspace. Advances in cryptology will be necessary to protect information and give the United States access to enemy information. Quantum computing opens new possibilities for encryption and decryption of information. Government agencies may be at the forefront of leading these efforts, but they will be unable to accomplish these tasks alone. Partnerships with private industry are critical for developing technologies and executing strategies to defend US institutions and critical infrastructure. Finally, the United States must continue to leverage the expertise of private industry for the mitigation and detection of malicious cyber activity, just as the Cyber Security & Infrastructure Security Agency has partnered with private security companies like FireEye and the MITRE Corporation.[65]

*Reducing the Efficacy of Information Warfare Attacks*

Attacks exploiting psychological vulnerabilities are challenging to defend. Examples include attacks designed to overwhelm an audience with sheer volume, whereby competing messages are drowned out, and the number of reinforcing sources of information adds credibility to the message, regardless of its accuracy.[66] Information warfare plays on an audience's biases and preconceived notions, reinforcing what they want to hear and casting doubt on counter-narratives.[67] Complete elimination of psychological vulnerabilities to propaganda and information attacks is unattainable. Nevertheless, the United States can take steps to reduce the efficacy of information warfare attacks drastically.

First and foremost, the United States must continue to promulgate accurate and credible information to expose and counter disinformation and misinformation campaigns. The success of any counter-messaging campaign relies upon the production of credible, consistent, and voluminous counter-speech. To that end, the US government and national security apparatus must be viewed as credible sources, and the US must safeguard its reputation as stringently as it safeguards data and critical infrastructure.

While the United States has viewed counter-speech as the best weapon against propaganda and false information, psychological studies on how people receive and process information cast doubt on the validity of these assumptions.[68] Confidence in the efficacy of counter-speech assumes people can discern between true and false information, that more information is always better, and that there will be as much valid information as false information in a person's environment.[69]

The thought is that the American public, provided with full access to information from all sides in a debate or issue, will be best placed to identify false information and inconsistencies and choose the course of action best for themselves and the country. The problem with this belief is that it rests on several assumptions that may not be true in general and, more specifically, may not be accurate in a modern networked communication and social media environment. Therefore, the United States must educate the population on the nature and elements of malicious information warfare to inoculate the US public against the effects of propaganda, disinformation, and misinformation. [70] US officials should consider developing a digital literacy plan for implementation across the US to teach the public how to recognize deepfake videos and exercise

critical-thinking skills, such as those used by Scandinavian and Baltic countries to combat Russian propaganda.[71]

## Conclusion

The ambiguous and opaque nature of information warfare tactics in cyberspace and the modern information environment increases the complexity of responding to gray zone conflict tactics employed against the United States by state and nonstate actors. The emphasis that the United States places on protecting freedom of expression and privacy creates an environment that offers protections to US adversaries conducting information operations while simultaneously making the US public fearful of security solutions perceived as threatening those freedoms. The result is that information warfare attacks intended primarily to undermine confidence in US institutions and sow discontent have the secondary effect of hindering the United States' ability to respond to the attacks. The United States must ensure that solutions strike the appropriate balance between liberty and security to maintain public trust while defending national interests. Therefore, the United States must protect its interests and uphold the values and institutions of democratic governance through proactive, rational, and unbiased security policy and oversight, technology advancements, and digital literacy education and public awareness.

---

[1] USSOCOM. "Report on Gray Zone Conflict." United States Special Operations Command. Washington D.C., September 9, 2015.
[2] Lawson, Sean and Michael K. Middleton. "Cyber Pearl Harbor_ Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016," First Monday, March 1, 2019. https://journals.uic.edu/ojs/index.php/fm/article/download/9623/7736#author.
[3] Goldenziel, Jill I., and Manal Cheema. "The New Fighting Words? How U.S. Law Hampers the Fight Against Information Warfare," SSRN Electronic Journal, 2018. https://doi.org/10.2139/ssrn.3286847.
[4] Johnson, Loch K. "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability," Intelligence and national security 23, 23, no. 2 (April 1, 2008): 198–225. https://doi.org/10.1080/02684520801977337.

[5] Walsh, Patrick F, and Seumas Miller. “Rethinking ‘Five Eyes’ Security Intelligence Collection Policies and Practice Post Snowden,” Intelligence and National Security 31, 31, no. 3 (April 15, 2016): 345–68. https://doi.org/10.1080/02684527.2014.998436
[6] *Department of Defense Strategy for Operations in the Information Environment* (Washington, D.C.: Department of Defense, 2016). http://purl.fdlp.gov/GPO/gpo82473.
[7] *Department of Defense Strategy for Operations in the Information Environment* (Washington, D.C.: Department of Defense, 2016). http://purl.fdlp.gov/GPO/gpo82473Formatting...
[8] *Department of Defense Strategy for Operations in the Information Environment* (Washington, D.C.: Department of Defense, 2016). http://purl.fdlp.gov/GPO/gpo82473
[9] “Defense Primer on Infomation Operations,” n.d.
[10] Theohary, Catherine A. “Defense Primer: Cyberspace Operations Overview.” Congressional Research Service, December 1, 2021.
[11] Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” Congressional Research Service (CRS) Reports and Issue Briefs. Congressional Research Service (CRS) Reports and Issue Briefs, November 1, 2007.
[12] Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” Congressional Research Service (CRS) Reports and Issue Briefs. Congressional Research Service (CRS) Reports and Issue Briefs, November 1, 2007.
[13] “Ransomware — FBI.” Www.Fbi.Gov, April 3, 2020. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.
[14] “Advanced Persistent Threat (APT) - Glossary _ CSRC.” Computer Security Resource Center, n.d. https://csrc.nist.gov/glossary/term/advanced_persistent_threat.
[15] “Advanced Persistent Threat (APT) - Glossary _ CSRC.” Computer Security Resource Center, n.d. https://csrc.nist.gov/glossary/term/advanced_persistent_threat.
[16] “What Is an Advanced Persistent Threat (APT)_ - Cisco.” Www.Cisco.Com, n.d. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.
[17] USSOCOM. “Report on Gray Zone Conflict.” United States Special Operations Command. Washington D.C., September 9, 2015.
[18] USSOCOM. “Report on Gray Zone Conflict.” United States Special Operations Command. Washington D.C., September 9, 2015.
[19] “USCYBERCOM-Preventing a Pearl Harbor Environment,” 2012
[20] Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” Congressional Research Service (CRS) Reports and Issue Briefs. Congressional Research Service (CRS) Reports and Issue Briefs, November 1, 2007.
[21]Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” Congressional Research Service (CRS) Reports and Issue Briefs. Congressional Research Service (CRS) Reports and Issue Briefs, November 1, 2007.
[22] "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," last modified -01-21T08:50:27+00:00, accessed Apr 15, 2022, https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.
[23] “Gen. Alexander: Greatest Tranfer of Wealth in History.” YouTube, n.d. https://www.youtube.com/watch?v=JOFk44yy6IQ.
[24] "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," last modified -01-21T08:50:27+00:00, accessed Apr 15, 2022, https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.
[25] Grzegorzewski, Mark and Christopher Marsh. “Incorporating the Cyberspace Domain_ How Russia and China Exploit Asymmetric Advantages in Great Power Competition - Modern War Institute,” The Modern War Institute at West Point, March 15, 2021. https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/.
[26] Grzegorzewski, Mark and Christopher Marsh. “Incorporating the Cyberspace Domain_ How Russia and China Exploit Asymmetric Advantages in Great Power Competition - Modern War Institute,”
[27] Grzegorzewski, Mark and Christopher Marsh. “Incorporating the Cyberspace Domain_ How Russia and China Exploit Asymmetric Advantages in Great Power Competition - Modern War Institute,”

[28] Grzegorzewski, Mark and Christopher Marsh. “Incorporating the Cyberspace Domain_ How Russia and China Exploit Asymmetric Advantages in Great Power Competition - Modern War Institute,”
[29] "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare,"
[30] "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare,"
[31] Bowen, Andrew S. “Russian Cyber Units.” Congressional Research Service, 2020. https://doi.org/10.51980/2686-939X_2020_3_238.
[32] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[33] Wallis, Jake. “China and Russia Aren’t the Same When It Comes to Information Warfare _ The Strategist,” The Strategist - Australian Strategic Policy Institute, September 25, 2019. https://www.aspistrategist.org.au/china-and-russia-arent-the-same-when-it-comes-to-information-warfare/.
[34] Bowen, Andrew S. “Russian Cyber Units.” Congressional Research Service, 2020. https://doi.org/10.51980/2686-939X_2020_3_238.
[35] Bowen, Andrew S. “Russian Cyber Units.” Congressional Research Service, 2020. https://doi.org/10.51980/2686-939X_2020_3_238.
[36] Bowen, Andrew S. “Russian Cyber Units.” Congressional Research Service, 2020. https://doi.org/10.51980/2686-939X_2020_3_238.
[37] Ortutay, Barbara and Mary Jaye Jalonick. “AP Report_ Russia-Linked Posts May Have Reached 126 Million Facebook Users _ PBS NewsHour.” Associated Press, October 30, 2017. https://www.pbs.org/newshour/nation/ap-report-russia-posts-may-have-reached-126-million-facebook-users.
[38] Gamreklidze, Ellada. “Political Speech Protection and the Supreme Court of the United States _ National Communication Association.” Www.Natcom.Org, October 1, 2015. https://www.natcom.org/communication-currents/political-speech-protection-and-supreme-court-united-states.
[39] Goldenziel, Jill I., and Manal Cheema. “The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare,” SSRN Electronic Journal, 2018. https://doi.org/10.2139/ssrn.3286847.
[40] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[41] Johnson, Loch K. “The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability,” Intelligence and national security 23, 23, no. 2 (April 1, 2008): 198–225. https://doi.org/10.1080/02684520801977337.
[42] Paul, Christopher and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*RAND Corporation,[2016]).
[43] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[44] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[45] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[46] Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. “Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist.” Journal of Strategic Studies 42. Informa UK Limited, January 10, 2019. https://doi.org/10.1080/01402390.2018.1559152.
[47] Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. “Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist.” Journal of Strategic Studies 42. Informa UK Limited, January 10, 2019. https://doi.org/10.1080/01402390.2018.1559152.
[48] Degaut, Marcos. “Spies and Policymakers: Intelligence in the Information Age,” Intelligence and national security 31, 31, no. 4 (June 6, 2016): 509–31. https://doi.org/10.1080/02684527.2015.1017931.
[49] “The SolarWinds Cyberattack.” Electronic. United States Senate Republican Policy Committee. United States Senate Republican Policy Committee, January 29, 2021. https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack.
[50] “The SolarWinds Cyberattack.” Electronic. United States Senate Republican Policy Committee. United States Senate Republican Policy Committee, January 29, 2021. https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack.

[51] Impelli, Matthew. “Colorado Representative Says SolarWinds Hack Could Be ‘Cyber Equivalent of Pearl Harbor.’” Newsweek, December 18, 2020. https://www.newsweek.com/colorado-representative-says-solarwinds-hack-could-cyber-equivalent-pearl-harbor-1555994
[52] Lawson, Sean and Brandon Valeriano. “The Russian ‘Cyber Pearl Harbor’ That Wasn’t — Strategic Culture,” December 18, 2020. https://www.strategic-culture.org/.
[53] Lawson, Sean and Brandon Valeriano. “The Russian ‘Cyber Pearl Harbor’ That Wasn’t — Strategic Culture,” December 18, 2020. https://www.strategic-culture.org/.
[54] Lawson, Sean and Brandon Valeriano. “The Russian ‘Cyber Pearl Harbor’ That Wasn’t — Strategic Culture,” December 18, 2020. https://www.strategic-culture.org/.
[55]“Treasury Escalates Sanctions Against the Russian Government’s Attempts to Influence U.S. Elections _ U.S. Department of the Treasury.” US Department of the Treasury, April 15, 2021. https://home.treasury.gov/news/press-releases/jy0126.
[56] Cunningham, Finian. “The Ron Paul Institute for Peace and Prosperity _ US Blacklists Strategic Culture Foundation in Attack on Independent Journalism and Political Dissent.” Ron Paul Institute for Peace and Prosperity, November 18, 2021. http://ronpaulinstitute.org/archives/featured-articles/2021/november/18/us-blacklists-strategic-culture-foundation-in-attack-on-independent-journalism-and-political-dissent/.
[57] Cunningham, Finian. “The Ron Paul Institute for Peace and Prosperity _ US Blacklists Strategic Culture Foundation in Attack on Independent Journalism and Political Dissent.” Ron Paul Institute for Peace and Prosperity, November 18, 2021. http://ronpaulinstitute.org/archives/featured-articles/2021/november/18/us-blacklists-strategic-culture-foundation-in-attack-on-independent-journalism-and-political-dissent/.
[58] “Executive Order 12333 of United States Intelligence Activities.” Digital National Security Archive - DNSA: Document Records (Unstructured), December 4, 1981. https://search.proquest.com/docview/1679112949.
[59] “Fact Sheet: Executive Order 12333 Csis.Org/Analysis/Fact-Sheet-Executive-Order-12333-0,” February 27, 2014.
[60] Goldenziel, Jill I., and Manal Cheema. “The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare,” SSRN Electronic Journal, 2018. https://doi.org/10.2139/ssrn.3286847.
[61] Goldenziel, Jill I., and Manal Cheema. “The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare,” SSRN Electronic Journal, 2018. https://doi.org/10.2139/ssrn.3286847.
[62] Peikoff, Amy L. “Of Third-Party Bathwater: How to Throw out the Third-Party Doctrine While Preserving Government’s Ability to Use of Secret Agents,” St. John's law review 88, 88, no. 2 (June 22, 2014): 349. https://search.proquest.com/docview/1672623780
[63] Walsh, Patrick F, and Seumas Miller. “Rethinking ‘Five Eyes’ Security Intelligence Collection Policies and Practice Post Snowden,” Intelligence and National Security 31, 31, no. 3 (April 15, 2016): 345–68. https://doi.org/10.1080/02684527.2014.998436
[64] Goldenziel, Jill I., and Manal Cheema. “The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare,” SSRN Electronic Journal, 2018. https://doi.org/10.2139/ssrn.3286847.
[65] Agency, Cybersecurity and Infrastructure Security. “Russia Cyber Threat Overview and Advisories _ CISA.” CISA.Gov, n.d. https://www.cisa.gov/uscert/russia.
[66] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[67] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[68] Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.
[69] Goldenziel, Jill I., and Manal Cheema. “The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare,” SSRN Electronic Journal, 2018. https://doi.org/10.2139/ssrn.3286847.
[70] Fitzpatrick, Meghan, Ritu Gill, and Jennifer F Giles. “Information Warfare: Lessons in Inoculation to Disinformation.” The US Army War College Quarterly: Parameters 52. United States Army War College Press, March 9, 2022. https://doi.org/10.55540/0031-1723.3132.
[71] Fitzpatrick, Meghan, Ritu Gill, and Jennifer F Giles. “Information Warfare: Lessons in Inoculation to Disinformation.” The US Army War College Quarterly: Parameters 52. United States Army War College Press, March 9, 2022. https://doi.org/10.55540/0031-1723.3132.

## Bibliography


"Advanced Persistent Threat (APT) - Glossary _ CSRC." Computer Security Resource Center, n.d. https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

Agency, Cybersecurity and Infrastructure Security. "Russia Cyber Threat Overview and Advisories _ CISA." CISA.Gov, n.d. https://www.cisa.gov/uscert/russia.

Aldrich, Rick. "PRIVACY'S THIRD-PARTY DOCTRINE IN THE WAKE OF CARPENTER." GPSolo 36. Chicago: American Bar Association, May 1, 2019. https://search.proquest.com/docview/2262670485.

"Application of the Posse Comitatus Act to Assistance to the United States National Central Bureau," July 3, 1989.

Bedi, Monu Singh. "Fourth Amendment Doctrine Mash-Up: The Curious Case of Cell Phone Location Data," SSRN Electronic Journal, 2015. https://doi.org/10.2139/ssrn.2641115.

Borch, Fred L. "Comparing Pearl Harbor and '9/11': Intelligence Failure? American Unpreparedness? Military Responsibility?," The Journal of Military History 3, 3, no. 67 (July 2003): 845.

Borer, Douglas A, Stephen Twing, and Randy P Burkett. "Problems in the Intelligence-Policy Nexus: Rethinking Korea, Tet, and Afghanistan," Intelligence and national security 29, 29, no. 6 (November 2, 2014): 811–36. https://doi.org/10.1080/02684527.2013.851875.

Bowen, Andrew S. "Russian Cyber Units." Congressional Research Service, 2020. https://doi.org/10.51980/2686-939X_2020_3_238.

Brotherton, Elspeth A. "Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine," Emory law journal 61, 61, no. 3 (January 1, 2012): 555. https://search.proquest.com/docview/1016162107.

Caparini, Marina. *The United States Department of Defense Intelligence Oversight Programme: Balancing National Security and Constitutional Rights*. Democratic Control of Intelligence Services. Routledge, 2007. https://doi.org/10.4324/9781315576442-16.

"Carpenter v United States," 2017.

Cunningham, Finian. "The Ron Paul Institute for Peace and Prosperity _ US Blacklists Strategic Culture Foundation in Attack on Independent Journalism and Political Dissent." Ron Paul Institute for Peace and Prosperity, November 18, 2021. http://ronpaulinstitute.org/archives/featured-articles/2021/november/18/us-blacklists-strategic-culture-foundation-in-attack-on-independent-journalism-and-political-dissent/.

Curran, John and Brian Hammond. “Former Judge: FISA Court Not Suited For ‘Programmatic’ Decisions,” Wolters Kluwer Law & Business Journal 79, 79, no. 14 (July 15, 2013): 45–46.

Davis, Jack. “Intelligence Analysts and Policymakers: Benefits and Dangers of Tensions in the Relationship,” Intelligence and national security 21, 21, no. 6 (December 1, 2006): 999–1021. https://doi.org/10.1080/02684520601046325.

“Defense Primer on Infomation Operations,” n.d.

Degaut, Marcos. “Spies and Policymakers: Intelligence in the Information Age,” Intelligence and national security 31, 31, no. 4 (June 6, 2016): 509–31. https://doi.org/10.1080/02684527.2015.1017931.

“Department of Defense Strategy for Operations in the Information Environment.” Washington, DC: Department of Defense, 2016. http://purl.fdlp.gov/GPO/gpo82473.

Derrick, Douglas C, Karyn Sporer, Sam Church, and Gina Scott Ligon. “Ideological Rationality and Violence: An Exploratory Study of ISIL’s Cyber Profile,” Dynamics of asymmetric conflict 9, 9, no. 1–3 (September 1, 2016): 57–81. https://doi.org/10.1080/17467586.2016.1267866.

Doney, Lauren. “PRACTICAL LIMITATIONS TO THE 3rd Party Doctrine,” National Security Law Journal 3, 3, no. 2 (2015): 462–97.

Dwoskin, Elizabeth. “Facebook Says Russia Still Biggest Disinformation Player - The Washington Post.” The Washington Post, May 26, 2021. https://www.washingtonpost.com/technology/2021/05/26/facebook-disinformation-russia-report/.

Eriksson, Gunilla. “A Theoretical Reframing of the Intelligence–Policy Relation,” Intelligence and national security 33, 33, no. 4 (June 7, 2018): 553–61. https://doi.org/10.1080/02684527.2018.1452558.

“Executive Order 12333 of United States Intelligence Activities.” Digital National Security Archive - DNSA: Document Records (Unstructured), December 4, 1981. https://search.proquest.com/docview/1679112949.

“Fact Sheet: Executive Order 12333 Csis.Org/Analysis/Fact-Sheet-Executive-Order-12333-0,” February 27, 2014.

Fenske, Martin. “The Association between Levels of Cortisol Secretion and Fear Perception in Patients with Remitted Depression Predicts Recurrence,” The journal of nervous and mental disease 195, 195, no. 3 (March 2007): 270. https://doi.org/10.1097/01.nmd.0000258303.22562.49.

Fitzpatrick, Meghan, Ritu Gill, and Jennifer F Giles. “Information Warfare: Lessons in Inoculation to Disinformation.” The US Army War College Quarterly: Parameters 52. United States Army War College Press, March 9, 2022. https://doi.org/10.55540/0031-1723.3132.

Gamreklidze, Ellada. “Political Speech Protection and the Supreme Court of the United States _ National Communication Association.” Www.Natcom.Org, October 1, 2015. https://www.natcom.org/communication-currents/political-speech-protection-and-supreme-court-united-states.

“Gen. Alexander: Greatest Tranfer of Wealth in History.” YouTube, n.d. https://www.youtube.com/watch?v=JOFk44yy6IQ.

Gentry, John A. “Toward a Theory of Nonstate Actors’ Intelligence,” Intelligence and national security 31, 31, no. 4 (June 6, 2016): 465–89. https://doi.org/10.1080/02684527.2015.1062320.

Goldenziel, Jill I., and Manal Cheema. “The New Fighting Words?: How US Law Hampers the Fight Against Information Warfare,” SSRN Electronic Journal, 2018. https://doi.org/10.2139/ssrn.3286847.

Gonchar, V. V. “ANALYSIS OF THE STATE OF INVESTIGATION OF CYBERCRIME BY INVESTIGATIVE UNITS OF THE RUSSIAN INTERIOR MINISTRY IN 2019,” Научный компонент, no. 3 (2020): 238–44. https://doi.org/10.51980/2686-939X_2020_3_238.

Gross, Leo. “Review Article.” American Journal of International Law 80. New York, USA: Cambridge University Press, January 1986. https://doi.org/10.2307/2202501.

Grzegorzewski, Mark and Christopher Marsh. “Incorporating the Cyberspace Domain_ How Russia and China Exploit Asymmetric Advantages in Great Power Competition - Modern War Institute,” The Modern War Institute at West Point, March 15, 2021. https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/.

Hastedt, Glenn. “The Politics of Intelligence and the Politicization of Intelligence: The American Experience,” Intelligence and national security 28, 28, no. 1 (February 1, 2013): 5–31. https://doi.org/10.1080/02684527.2012.749062.

Howard, P, B Ganesh, D Liotsiou, J Kelly, and C François. “The IRA, Social Media and Political Polarization in the United States, 2012-2018,” December 17, 2018. https://explore.openaire.eu/search/publication?articleId=od_____1064::3fb71ab19130cd13c0362a69978128b2.

Hulnick, Arthur S. “Determining US Intelligence Policy,” International journal of intelligence and counterintelligence 3, 3, no. 2 (January 1, 1989): 211–24. https://doi.org/10.1080/08850608908435100.

———. “Intelligence Producer-Consumer Relations in the Electronic Era,” International journal of intelligence and counterintelligence 24, 24, no. 4 (December 1, 2011): 747–56. https://doi.org/10.1080/08850607.2011.598812.

———. “The Intelligence Producer - Policy Consumer Linkage: A Theoretical Approach,” Intelligence and national security 1, 1, no. 2 (May 1, 1986): 212–33. https://doi.org/10.1080/02684528608431850.

Impelli, Matthew. “Colorado Representative Says SolarWinds Hack Could Be ‘Cyber Equivalent of Pearl Harbor.’” Newsweek, December 18, 2020. https://www.newsweek.com/colorado-representative-says-solarwinds-hack-could-cyber-equivalent-pearl-harbor-1555994.

Jaffer, Jameel. “The Mosaic Theory,” Social research 77, 77, no. 3 (October 1, 2010): 873–82. https://www.jstor.org/stable/40972296.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. “Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist.” Journal of Strategic Studies 42. Informa UK Limited, January 10, 2019. https://doi.org/10.1080/01402390.2018.1559152.

Johnson, Loch K. “The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability,” Intelligence and national security 23, 23, no. 2 (April 1, 2008): 198–225. https://doi.org/10.1080/02684520801977337.

Kelly, Meg and Elyse Samuels. “Why Russia’s Weaponization of Social Media Will Continue in 2020 - The Washington Post.” The Washington Post, November 18, 2019. https://www.washingtonpost.com/politics/2019/11/18/how-russia-weaponized-social-media-got-caught-escaped-consequences/.

Kerr, Orin S. “Michigan Law Review Michigan Law Review The Case for the Third-Party Doctrine The Case for the Third-Party Doctrine,” n.d.

Lawson, Sean and Brandon Valeriano. “The Russian ‘Cyber Pearl Harbor’ That Wasn’t — Strategic Culture,” December 18, 2020. https://www.strategic-culture.org/.

Lawson, Sean and Michael K. Middleton. “Cyber Pearl Harbor_ Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016,” First Monday, March 1, 2019. https://journals.uic.edu/ojs/index.php/fm/article/download/9623/7736#author.

Mahnken, Thomas G. *Competitive Strategies for the 21st Century (2012)*, 2012.

Marchio, Jim. “Analytic Tradecraft and the Intelligence Community: Enduring Value, Intermittent Emphasis,” Intelligence and national security 29, 29, no. 2 (March 4, 2014): 159–83. https://doi.org/10.1080/02684527.2012.746415.

“Office of the Director of National Intelligence 2012 Data Mining Report,” January 1, 2012.

Ortutay, Barbara and Mary Jaye Jalonick. “AP Report_ Russia-Linked Posts May Have Reached 126 Million Facebook Users _ PBS NewsHour.” Associated Press, October 30, 2017. https://www.pbs.org/newshour/nation/ap-report-russia-posts-may-have-reached-126-million-facebook-users.

Paul, Christopher and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND. RAND Corporation, 2016.

Peikoff, Amy L. “Of Third-Party Bathwater: How to Throw out the Third-Party Doctrine While Preserving Government’s Ability to Use of Secret Agents,” St. John's law review 88, 88, no. 2 (June 22, 2014): 349. https://search.proquest.com/docview/1672623780.

Perera, David. “Leahy Calls for End to Bulk Storage of Telephony Metadata.” FierceGovernmentIT. Newton: Questex, LLC, September 25, 2013. https://search.proquest.com/docview/1466237230.

Porche, Isaac R. and Colin P. Clarke. “Following Online Footprints to Catch Terrorists _ RAND.” Www.Rand.Org, December 28, 2015.

“Preventing and Defending Against Cyber Attacks,” June 1, 2011.

“Preventing and Defending Against Cyber Attacks,” October 1, 2011.

Price, Michael W. “ARTICLES Rethinking Privacy: Fourth Amendment ‘Papers’ and the Third-Party Doctrine,” n.d.

“Ransomware — FBI.” Www.Fbi.Gov, April 3, 2020. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

Rathmell, Andrew. “Towards Postmodern Intelligence,” Intelligence and national security 17, 17, no. 3 (September 1, 2002): 87–104. https://doi.org/10.1080/02684520412331306560.

“Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare.” War on the Rocks, 2020. https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.

Seabrook, Nicholas R, and Nicholas C Cole. “Secret Law: The Politics of Appointments to the US Foreign Intelligence Surveillance Court,” The Justice system journal 37, 37, no. 3 (July 2, 2016): 259–71. https://doi.org/10.1080/0098261X.2015.1110468.

“Section702-Basics-Infographic,” n.d.

Smith, Don C. “Cybersecurity in the Energy Sector: Are We Really Prepared?,” Journal of energy & natural resources law 39, 39, no. 3 (July 3, 2021): 265–70. https://doi.org/10.1080/02646811.2021.1943935.

Teitalbaum, Lorne. “The Impact of the Information Revolution on Policymakers’ Use of Intelligence Analysis.” RAND, 2004.

Temple-Raston, Dina. “How Russia Used SolarWinds To Hack Microsoft, Intel, Pentagon, Other Networks _ NPR.” NPR, April 16, 2021. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

“The SolarWinds Cyberattack.” Electronic. United States Senate Republican Policy Committee. United States Senate Republican Policy Committee, January 29, 2021. https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack.

“The Truth About Executive Order 12333,” n.d.

“THE VIRTUAL CALIPHATE: ISIS’S INFORMATION WARFARE Harleen Gambhir,” December 1, 2016.

Theohary, Catherine A. “Defense Primer: Cyberspace Operations Overview.” Congressional Research Service, December 1, 2021.

“To Catch a Terrorist.” Intel.Gov. Accessed January 17, 2022. https://www.intelligence.gov/index.php/mission/intel-stories/367-to-catch-a-terrorist.

“Treasury Escalates Sanctions Against the Russian Government’s Attempts to Influence US Elections _ US Department of the Treasury.” US Department of the Treasury, April 15, 2021. https://home.treasury.gov/news/press-releases/jy0126.

“USCYBERCOM-Preventing a Pearl Harbor Environment,” 2012.

USSOCOM. “Report on Gray Zone Conflict.” United States Special Operations Command. Washington DC, September 9, 2015.

Wallis, Jake. “China and Russia Aren’t the Same When It Comes to Information Warfare _ The Strategist,” The Strategist - Australian Strategic Policy Institute, September 25, 2019. https://www.aspistrategist.org.au/china-and-russia-arent-the-same-when-it-comes-to-information-warfare/.

Walsh, Patrick F, and Seumas Miller. “Rethinking ‘Five Eyes’ Security Intelligence Collection Policies and Practice Post Snowden,” Intelligence and National Security 31, 31, no. 3 (April 15, 2016): 345–68. https://doi.org/10.1080/02684527.2014.998436.

“What Is an Advanced Persistent Threat (APT)_ - Cisco.” Www.Cisco.Com, n.d. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.

Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” Congressional Research Service (CRS) Reports and Issue Briefs. Congressional Research Service (CRS) Reports and Issue Briefs, November 1, 2007.

Wirtz, James J. “The Cyber Pearl Harbor,” Intelligence and national security 32, 32, no. 6 (September 19, 2017): 758–67. https://doi.org/10.1080/02684527.2017.1294379.

———. “The Cyber Pearl Harbor Redux: Helpful Analogy or Cyber Hype?,” Intelligence and national security 33, 33, no. 5 (July 29, 2018): 771–73. https://doi.org/10.1080/02684527.2018.1460087.