# Research on Pre-Electoral Intervention by Foreign Countries in a Digital World

# Research on Pre-Electoral Intervention by Foreign Countries in a Digital World

Syed Gilani

A Thesis in the Field of International Relations

for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

November 2018

Abstract

The election is now over,
The result is now known.
The will of the people
Has clearly been shown.
Let's all get together;
Let bitterness pass.
I'll hug your Elephant;
And you kiss my Ass.
—Hillary Clinton, 2018

The 2016 U.S. presidential election is long over, but the will of the people is still being contested in the media and by many in the general public. Bitterness has severely divided the nation along ideological fault lines, and hugs and kisses are far from reality. Alleged Russian intervention in the U.S. national elections, in favor of Republican nominee Donald J. Trump, has been named as one of the major problems of this recent post-election discord across America.

Foreign governments have intervened in the pre-election processes of other countries for a long time, often by overtly or covertly using economic and military muscle. For the first time, however, a major world power has used cyberspace and digital media to try to alter the outcome of elections held by another major world power.

Digital media, especially social media, is a relatively new phenomenon. It is not easy to clearly associate the actions of rogue individuals and organizations who may have engaged in cyber espionage, coercion, and/or unlawful intervention with the specific policies and actions of their respective governments. For some time now, countries have been exploring the potential of cyberspace to extend their political, economic, and

strategic influence beyond permissible and customary international law and treaties. In the 2016 U.S. presidential elections, U.S. intelligence chiefs, social media experts, political pundits, and representatives in the U.S. Congress became confident that the Russian government was directly involved in various attempts to influence the election outcome.

I examine the principles of nonintervention and sovereignty under current international legal frameworks and compares current practices of nonintervention between countries with customary international law and treaties. The research specifically focuses on the role of digital media, in particular social media, as a tool for effective pre-election intervention in a country by a foreign government. It evaluates different digital intervention tactics frequently used by a foreign government while at the same time skirting around the nonintervention charter of the United Nations and customary international laws.

I also provide a fuller understanding of the challenges of attribution, that is, associating the actions of citizens with a country. I recommend steps for managing possible threats to the principles of sovereignty and nonintervention as they exist under current international legal frameworks.

# Dedication

To my wife, Aasma, for being the voice of reason and energy in my life. My journey at Harvard was made possible by your continuous support.

To my children—Zayna, Myda, Ali Asad and of course Rehma—for their flexibility and willingness to cooperate with my study schedules during this Master's degree process. And to my son residing in heaven, Samad Ali—although I didn't get to spend much time with you, I will always miss you.

I am forever grateful for each one of you.

Acknowledgements

I would like to express my deepest gratitude to my thesis advisor, Dr. Doug Bond, for his constant encouragement, guidance, and support. I would also like to thank my thesis director, Professor Gabriella Blum for her patience, engagement, and comments throughout this thesis process.

Profound gratitude to my dear wife, Aasma, and to my parents, Anujan and Abujan, for their support throughout my degree program. I am forever thankful for your love and support.

Table of Contents

List of Figures

# Chapter I

## Introduction

In recent years, powerful countries have begun to interfere in the electoral processes of other countries, either covertly or overtly, using economic and military espionage and coercion. Since the advent of cyberspace and digital media, cross- border dialogue between people has taken new shapes as a result of a new generation of platforms like Facebook, YouTube, Google, and Twitter—each managing and promoting information in different ways. Global norms of nonintervention have been long settled in Customary International Law (CIL) through various international and regional agreements[1] and international treaties. Yet these platforms have expanded public engagement at all levels and increased the likelihood of some level of influence on the outcome of foreign electoral processes through misinformation and/or coercive campaigns. The U.S. has a long history of pre-electoral intervention in other countries but recent allegations of Russia's use of digital media platforms, either by hacking or distributing fake news, raises questions about state sovereignty and non-intervention policies by U.N. member states. Further, the involvement of non-state shadow groups,

[1] U.N. General Assembly, "A/RES/20/2131: Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty." http://www.un-documents.net/a20r2131.htm. Accessed 14 November 2018; also Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations, 21 March, 1986. Preamble. http://legal.un.org/ilc/texts/instruments/english/conventions/1_2_1986.pdf ; also U.N. Resolution A/RES/47/130. 1992, **"**Recognizing that the Principles of National Sovereignty and Non-Interference in the Internal Affairs of any State Should be Respected in the Holding of Elections." http://www.un.org/documents/ga/res/47/a47r130.htm. Accessed 14 November 2018.

like APT28 and their multi-layered tactics, have made attribution of such intrusions even more complicated.

On July 27, 2016 while addressing a news conference in Florida, then presidential candidate Donald Trump suggested that Russia should interfere in the election campaign of his rival, Democratic nominee Hillary Clinton, by hacking into her email server. The Republican nominee said: "I will tell you this, Russia: if you're listening, I hope you're able to find the 30,000 emails that are missing."[2] Wikileaks subsequently ended up releasing several of Clinton's emails along with other documents from Democratic National Committee (DNC) computer servers. On April 24, 2017, the campaign of French President Emmanuel Macron was targeted by a cyber espionage group aligned with Russia called Pawn Storm. Feike Hacquebord, a researcher with security firm Trend Micro, told Reuters: "We have seen that phishing sites were set up and the fingerprints were really the same actors as in the DNC breach."[3]

Interference in pre-election processes by powerful foreign countries is not a new phenomenon. Between 1946 and 2000, the US and the Soviet Union/Russia intervened in perhaps one of every nine competitive national-level executive elections and 117 foreign elections.[4] Although most pre-election interventions were undertaken by major world powers like the United States and Soviet Union/Russia, it would be naïve to think they were the only countries that interfered either overtly or covertly in major foreign

---

[2] Michael Crowley, "Trump urges Russia to hack Clinton's email," *Politico*, July 27, 2016. https://www.politico.com/ story/2016/07/trump-putin-no-relationship-226282. (Accessed 14 November 2018.)

[3] Eric Auchard, "Macron campaign was target of cyber attacks by spy-linked group," Reuters World News, April 24, 2017. https://www.reuters.com/article/us-france-election-macron-cyber/macron-campaign-was-target-of-cyber-attacks-by-spy-linked-group-idUSKBN17Q200. (Accessed 14 November 2018.)

[4] Dov H. Levin, "When the Great Power gets a vote: The effects of Great Power electoral interventions on election results," *International Studies Quarterly* 60, no. 2 (2016)..

elections. For example, in Iraq following the fall of Saddam Hussein, Iran seized the opportunity to extend its influence by closely aligning itself with political Shiite allies, including the Islamic Supreme Council of Iraq and the Badr Organization, encouraging them to participate in every election.[5] Former Venezuelan President Hugo Chavez was accused of meddling in at least three presidential elections in Peru.[6] India has also been accused of securing its interest in neighboring countries through electoral intervention in countries like Nepal.[7]

Traditionally, countries have used economic and military coercion to skew election results in their favor. Dov H. Levin[8] provides insight into traditional methods of foreign interventions. Figure 1 outlines some of the overt and covert activities undertaken by major powers for partisan electoral intervention Levin's list does not include intervention done via digital media or cyberspace, a method that has been perfected in recent years by Russia, China, North Korea, and the U.S. Indeed, the digital world has given new platforms to traditional methods of intervention as foreign powers, can hide behind rogue actors or non-state entities, both individuals and organizations, while coordinating elaborate efforts to undermine electoral processes in a foreign country—all done without directly being accused of violating the U.N. charter or infringing on customary international norms of nonintervention.

---

[5] Michael Eisenstadt, Michael Knights, and Ahmed Ali, "Iran's Influence in Iraq," Washington Institute for Near East Policy. http://www.washingtoninstitute.org/policy-analysis/view/irans-influence-in-iraq-countering-tehrans-whole-of-government-approach.

[6] Gavin O'Toole, *Politics Latin America* (NY: Pearson, 2018), 273.

[7] James Lamont and Prateek Pradhan, "Nepal hits back at foreign intervention," *Financial Times,* May 16, 2010. https://www.ft.com/content/2c2ee906-610a-11df-9bf0-00144feab49a. (Accessed 14 November 2018.)

[8] Dov H. Levin, "Partisan electoral interventions by the Great Powers: Introducing the PEIG Dataset," *Conflict Management and Peace Science*, September 19, 2016. http://journals.sagepub.com/. (Accessed 14 November 2018.)

| Main activities coded as interventions | Examples of excluded activities |
|---|---|
| Provision of campaign funds to the favored side either directly (to candidate/party coffers) or indirectly | Invitation of preferred candidate to international conferences, international organizations, a visit to another country (unless includes concrete concessions/promises as well) |
| Public and specific threats or promises by an official representative of intervening country | Photo-ops/meetings of candidate with world leaders/official representatives of the intervener with no concrete results otherwise |
| Training locals (of the preferred side only) in advanced campaigning and get out the vote techniques | Provision of foreign aid of various types in order to enable the holding of free elections and/or improve their quality (without subsequent attempts to affect the results) |
| Covert dissemination of scandalous exposes/ disinformation on rival candidates | Generic/neutral statements of support for the proper conduct of the electoral process (with no endorsements of a particular candidate/side) |
| Design (for the preferred side only) of campaigning materials/sending campaigning experts to provide on-the-spot aid | Secret/open refusal of leader/officials of the intervener to publicly meet with a candidate or his/her representatives |
| Sudden new provision of foreign aid or a significant increase in existing aid and/or other forms of material assistance | Positive/negative things said about a candidate/ party by the intervener before an election with no concrete threats/promises |
| Withdrawal of part or whole of aid, preferred trading conditions, loan guarantees, etc. | Leaks to the press of reports of disagreements between the intervener and the target, etc. "Regular" election monitoring |

Figure 1. Overt and Covert Activities Considered to be Interventions.

Source: Levin, 2016.

International law is clear about nonintervention by nations into the sovereignty of others. The United Nations Charter clearly states that it does not allow members "to intervene in matters which are essentially within the domestic jurisdiction of any state."[9] Further, in Chapter VII of the Charter, it is noted that the United Nations as an institution can only become involved in member states' matters in cases of "the existence of any threat to the peace, breach of the peace, or act of aggression."[10] In 1965, the United Nations adopted another resolution to further enhance its non-interventionist posture by

[9] United Nations. Charter, Chapter 1, Article 2, paragraph 7.

[10] United Nations. Charter, Article VII, Article 39.

passing a declaration on the inadmissibility of intervention in the domestic affairs of states and the protection of their independence and sovereignty. That declaration states:

> No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned."[11]

There are also customary international norms of "non-intervention" adhered to generally by all U.N. member states. Nevertheless, these norms have not stopped individual states from interfering in each others' internal political affairs. Customary International Law relies on *opinio juris* or general practice accepted as a law.[12] Practice may take a wide range of forms. It can include both physical and verbal actions. Manifestations of general practice might include: the conduct of States "on the ground," diplomatic acts and correspondence, legislative acts, judgments of national courts, official publications in the field of international law, statements on behalf of States concerning codification efforts, practice in connection with treaties, and acts in connection with resolutions of organs of international organizations and conferences. Inaction may also serve as practice. The acts (including inaction) of international organizations may also serve as practice.

Disinformation or misinformation propaganda is one of the most effective tools used by countries to influence the outcome of elections in other nations, with the use of traditional media becoming a key to executing effective misinformation campaigns. Politics and the media are expected to work with each other in a democratic system, with

---

[11] UN General Assembly, A/RES/20/2131.

[12] Michael Wood, "Second Report on Identification of Customary International Law," United Nations Dag Hammerskjöld Library, May 22, 2014. http://dag.un.org/handle/11176/307174: 66. (Accessed 14 November 2018.)

one pillar relying on the other to ensure effective public engagement in the political process. The rise of digital media in the twenty-first century has given birth to many highly effective communication and public engagement platforms, providing one of the most powerful tools not only to political actors within a country but also to foreign agents who may be determined to sway public sentiment in their favor.

# Chapter II

## Research, Methodology, and Limitations

My research explores the impact of digital intervention on pre-election processes and compares foreign interference through digital media vis-à-vis traditional methods. Digitally enriched countries offer their citizens appealing and unfiltered platforms for civic engagement as part of their commitment to freedom of speech.

While I have conducted considerable exploratory research, my thesis focuses on the 2016 U.S. presidential election, and the 2017 elections in Germany and France—especially because it is relatively easier to obtain available information about Russian attempts to sway those elections using digital platforms like Facebook, YouTube, Twitter and Google. These case studies highlight two important factors: (1) the rapidly increasing adoption of cyberspace, especially social media platform, in these countries, and (2) the realities of democratic freedom of speech. With almost 80% of U.S. adults using at least one social media site (see Figure 2), and a greater than 60% adoption of digital media

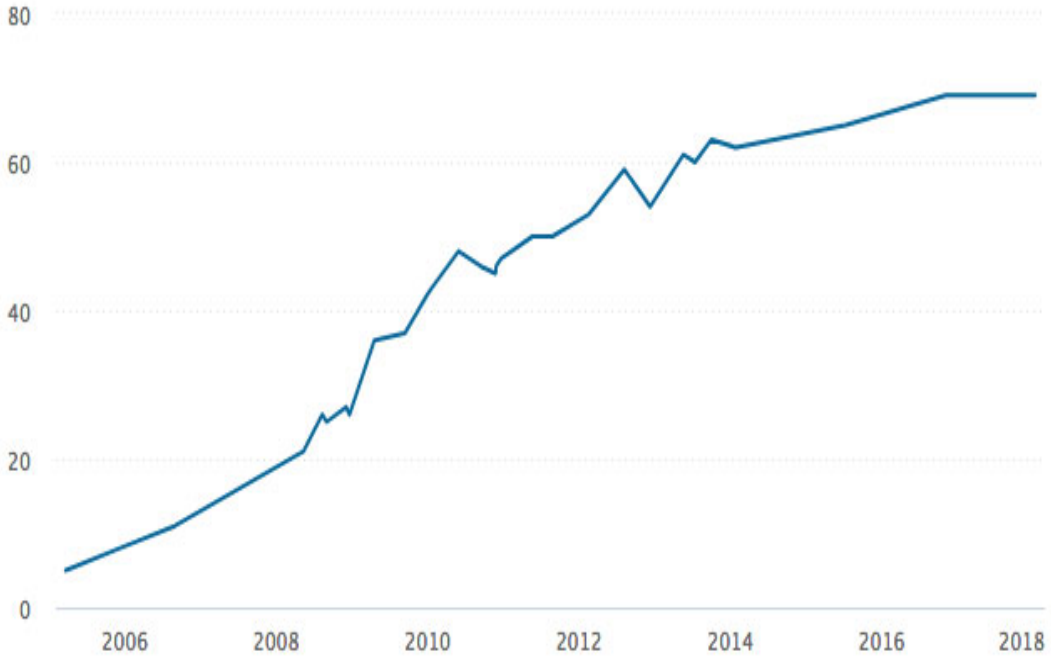


Figure 2. Percent of U.S. Adults Who Use at Least One Social Media Site.

Source: Pew Research Center, 2018

platforms in Europe (see Figure 3), the U.S. and Europe have become a prime target for spreading fake news or hacking into the digital infrastructure.

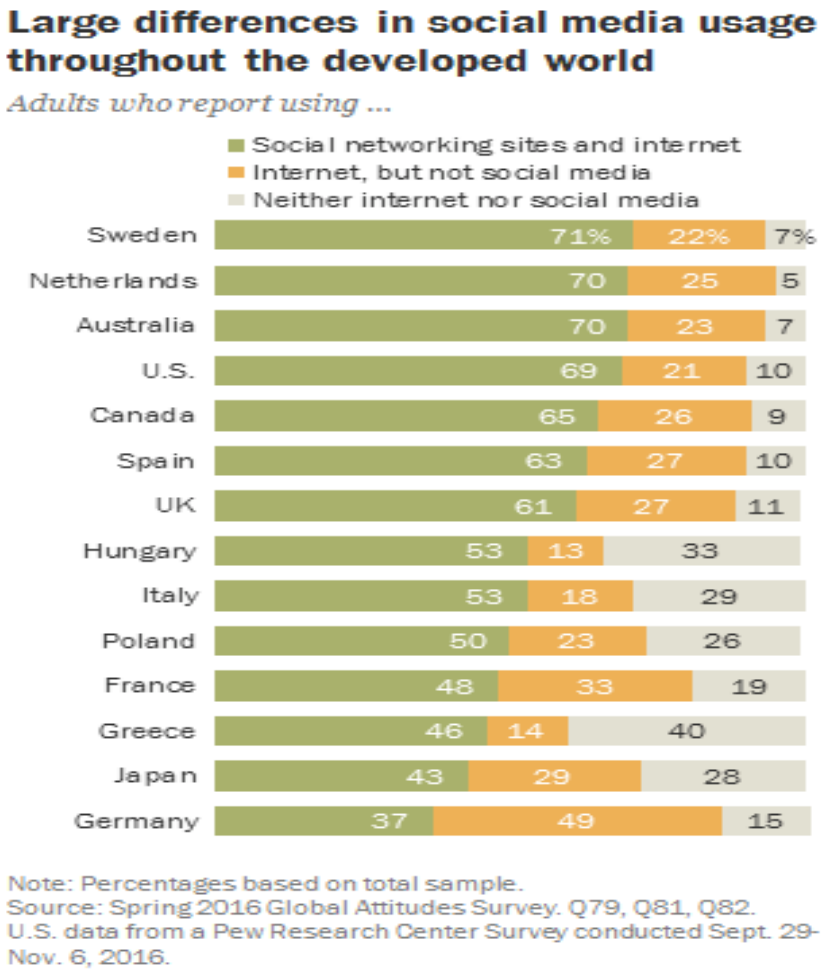


Figure 3. Differences in Social Media Use.

Source: Pew Research Center, 2018

The research also looks into various tactics recently used by other foreign countries, the ease of using these tactics, and their impact on elections in U.S. and Europe. Many intervention strategies rely on the mood of the pre-election political landscape in a country. Further, the level of political divide in a country also influences

whether intervention strategies by foreign powers are direct or indirect. My research will evaluate alleged intervention by Russia as it relates to the current international scene.

My hypothesis is that although countries have interfered in the electoral processes of other countries for decades, foreign intervention through digital media has amplified the impact of these actions so as to influence the results of an election process while avoiding possible direct international action. I focus specifically on digitally integrated societies, in particular the United States and European countries. I evaluate the impact of digital intervention in the form of fake news, hacks, and cyber attacks on election outcomes.

Although these platforms and public dialogues are a key part of the foundation of a healthy democratic society, during recent U.S. and European elections, it has been uncovered that foreign governments like Russia find these platforms to be effective weapons in altering the outcome of a nation's election process in ways that favor certain outcomes. It is only when limitations are introduced on such platforms that challenges arise.

Due to the secretive nature of foreign interventions, as well as the relative infancy of the digital media spectrum, there is not enough generally available literature and supporting data that focuses specifically on intervention via digital media. My research focuses on foreign interventions in electoral processes from 2005 to 2017—a period of time known for the emergence of digital boom. My goal is to offer deeper insights into various digital media platforms that have been used to impact electoral results. This will provide a better understanding of the covert actions taken by a state or a group of countries against another nation. Since the study of foreign intervention through digital

media is relatively new, my research will focus on information that is publicly available through various U.S. and European investigations that have been conducted on Russian intervention into U.S. elections.

## Methodology

As part of my study of intervention in the digital world, I will explore the use of digital media to intervene in the pre-electoral process of a country by a foreign power or a non-state actor especially in the case of Russian intervention in the 2016 U.S. presidential elections along with some reference to the recent European elections.

I will rely on a variety of media accounts, scholarly articles, social media penetration statistics, investigative journalism, government agencies' investigation reports, as well as existing literature on international relations and political science. With the expansion of social media platforms beyond the United States, I will also explore the proliferation of interventionist strategies by foreign powers using digital media as a means to exert influence over other nations.

## Research Limitations

One limitation of my research comes from the fact that all pre-election foreign intervention takes place covertly. No country has openly admitted or revealed their involvement in influencing another country's election process, fearing that such a revelation could produce an opposite outcome, as well as being considered a violation of the U.N. Charter and customary international laws. Most of the information regarding foreign intervention is revealed years after the incident as part of the country's investigation process that produces highly redacted declassified reports. More typically, it

is news reports from investigative journalism that offer some glimpses into such covert activity.

The second limitation derives from the relative newness of digital media, especially social media platforms. Pre-election influence through digital media became more widely mainstream during the 2016 U.S. presidential elections. Hacking and other server-related attacks have occurred since the advent of cyberspace, but the proliferation of leaked and false information put forward by a country is, as a tool, still in the infant stage. Most pre-election intervention is undertaken by rogue groups like Cozy Bear, which are difficult to directly associate with an alleged interfering government.

As the world increases its understanding of the power of social media to influence another country, my thesis could also face a third limitation in the form of generally accepted but unofficial/informal or even undocumented new rules of engagement that permit countries, under specific pretexts, to intervene in another country or respond to cyber aggression from a foreign power using the power of digital media.

# Chapter III

## Definition of Terms

*AIVD*: The Dutch security agency, known as the Central Intelligence and Security Service, in the Ministry of the Interior and Kingdom Relations.

*Cold War*: The Cold War was a decades-long struggle for global supremacy which pitted the United States against the Soviet Union. Although some disagree as to precisely when the Cold War began, it is generally accepted that mid to late 1945 marks the point when relations between Moscow and Washington began deteriorating. The Cold War had lasted for 46 years, and is regarded by many historians, politicians, and scholars as the third major war of the twentieth century.

*Customary International Law*: Law that originates from general practice, accepted as law, among different countries yet still considered binding by the International Court of Justice. Rules of nonintervention under customary international law are widely understood and adopted by most nations.

*DoS:* Denial of Service involves an attack on multiple connected online devices with the aim of generating so much fake traffic that it overwhelms a server and often causes it to shut down. DoS is one of the easier ways to disrupt services in a foreign country. It is also difficult to identify a foreign interventionist who might be behind such an attack, as the government may hide behind malicious individuals or pseudo organizations.

*Espionage*: Usually defined as the overt or covert collection of information about an adversary for the purpose of benefiting the perpetrating country,

*Fake News*: A term frequently used to describe a political story that is damaging to an agency, entity, or person.[13] Misinformation is not a new concept but the term "fake news" made its appearance during the 2016 pre-election campaign of Donald Trump.

*HTTP/S Floods*: HTTP/S floods are a type of DOS attack that allows the attacker to abuse legitimate HTTP applications for the purpose of attacking a web server or application.[14]

*Phishing*: One of the most common ways to defraud people by taking advantage of human nature and the power of the internet. According to the Federal Trade Commission, phishing occurs when a scammer uses fraudulent emails, texts, or copycat websites to persuade users to share personal information such as account numbers, Social Security numbers, login IDs, and/or passwords. Scammers use this information to steal a user's money or identity or both.[15]

*Post-Modern World*: In this world, many believe that the systems of the modern world are collapsing—but into a greater order. The post-modern system does not rely on balance nor does it emphasize sovereignty. The European Union is one example.

---

[13] "The Real Story of 'Fake News'," Merriam-Webster Dictionary. https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news. (Accessed May 28, 2018.)

[14] N. Jeyanthi and R. Thandeeswaran, *Security Breaches and Threat Prevention in the Internet of Things* (Hershey: IGI Global, 2017), 87.

[15] Federal Trade Commission, "Phishing." https://www.consumer.ftc.gov/articles/0003-phishing.

*Social Engineering*: The act of manipulating a person to take an action that may or may not be in their best interest.[16] According to US-CERT, in a social engineering attack, the attacker uses human social skills to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher—even offering credentials to support that identity.[17]

*SQL Injections*: Hackers use SQL injections, a technique for injecting code into a program, which attacks a program's Structured Query Language (SQL) based databases. This enables the attacker to leverage the syntax and capabilities of SQL itself. It is one of the most common methods for attacking a structured database.

[16] Christopher Hadnagy and Paul Wilson, *Social Engineering: The Art of Human Hacking* (Hoboken, N.J.: Wiley, 2013).

[17] "Avoiding Social Engineering and Phishing Attacks," US Computer Emergency Readiness Team (CERT). https://www.us-cert.gov/ncas/tips/ST04-014.

# Chapter IV

## A Normative Approach to Nonintervention

On February 29, 2004, Haitian President Jean Bertrand Aristide tendered his resignation to the U.S. Ambassador in Haiti and boarded a plane to the Central African Republic after giving in to pressure from the United States and from local opposition.[18] Amid strong criticism from Latin American countries, the U.S. provided a pathway for a new government in Haiti.

Governments around the world have grappled with strategies to expand their political, economic, and social influence beyond their geographical borders or to engage in foreign intervention to provide humanitarian relief without breaking international laws of nonintervention. Nations frequently condemn the actions of other countries that intervene in those nations' domestic matters—even as they sometimes engage in similar activities themselves. Customary International Law (CIL) and treaties have long provided a foundation for behavior among nations,[19] especially during the post-World War II era. However, there is a gulf between a normative approach to nonintervention and the realities of current practice among countries.

Foreign intervention is not a new phenomenon. Many aristocrats, states, religious organizations, and individuals have interfered in other states and entities for centuries. The pursuit of power and national interests is often the underlying reason for most of the

---

[18] Daniel P. O'Neill, "When to intervene: The Haitian dilemma," *SAIS Review* 24, no. 2 (2004).

[19] Andrew T Guzmán, *How International Law Works: A Rational Choice Theory* (New York: Oxford University Press, 2010), xx.

foreign interventions that occurred in the medieval and modern ages. But regardless of the pretext, liberal and realist scholars, such as Immanuel Kant[20] and Thomas Hobbes,[21] have long sought to provide justifications for permissible and non-permissible foreign interference in the affairs of state.

The concept of foreign intervention is directly related to an understanding of state "sovereignty." Since their inception, sovereign states have fought to retain control over their domestic affairs. Although scholars believe that the foundations of the modern state were laid out in 1648 with the Treaty of Westphalia,[22] realists like Stephen Krasner argue that aristocratic governments in the Middle Ages had some independence over their domestic affairs, and contend that the Treaty failed to fully address norms of nonintervention in domestic affairs.[23] Later in the eighteenth century, Emer de Vattel and other scholars further elaborated the rules of nonintervention by explicitly forbidding states from interfering in other states' internal affairs.[24]

The idea of nonintervention addresses two facets: (1) the right of sovereign states to be recognized by other countries, and (2) recognizing horizontally aligned smaller or weaker countries as equals with stronger states. John Jackson, a professor of law at Georgetown University, states:

---

[20] Harry Van der Linden, Digital Commons @ Butler University. https://digitalcommons.butler.edu/cgi/viewcontent.cgi?article=1041&context=facsch_papers.

[21] David Singh Grewal, "The Domestic Analogy Revisited: Hobbes on International Order," *Yale Law Journal* 125, no. 3 (January 2016): 560-795. (Accessed 15 November 2018.)

[22] James A Nathan, *Soldiers, Statecraft, and History: Coercive Diplomacy and International Order* (NY: Praeger, 2002), 1.

[23] Stephen D Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 2001), 20.

[24] Krasner, *Sovereignty*, 21.

> The concept of equality of nations is linked to sovereignty concepts because sovereignty has fostered the idea that there is no higher power than the nation-state, so its "sovereignty" negates the idea that there is a higher power, whether foreign or international (unless consented to by the nation-state).[25]

By the twentieth century, efforts were being made to strengthen the modern ideals of nonintervention as the world embarked on forming the foundations of international order under the League of Nations[26] in 1920 and the United Nation in 1945. In its early years, the League of Nations made significant progress toward introducing international order. However, its achievements were short-lived as Europe contemplated engaging in the Spanish Civil War in 1936.[27] To avoid direct conflict, Germany, Britain, France, the Soviet Union, Portugal, Sweden, and Italy all co-signed the Non-Intervention Agreement, in an effort to provide temporary calm in the face of looming potential conflict. Author Stanley Payne states:

> The Non-Intervention Agreement that all the European powers signed was not a treaty and hence all the more difficult to enforce. It permitted all the powers to avoid having to make a declaration of neutrality while they further refused to recognize the right of either side to the status of official belligerent in international law.[28]

The ideals of collective security introduced by the League of Nations did not last long before the world plunged into World War II. After the war, the League of Nation was terminated and its properties were transferred to a new world organization, the

---

[25] John H. Jackson, "Sovereignty - Modern: A New Approach to an Outdated Concept," Scholarship @ GEORGETOWN LAW, last modified 2003, https://scholarship.law.georgetown.edu/facpub/110/.

[26] United Nations Office at Geneva (UNOG), "History of the League of Nations (1919-1946)," https://www.unog.ch/80256EDD006B8954/(httpAssets)/36BC4F83BD9E4443C1257AF3004FC0AE/$file/Historical_overview_of_the_League_of_Nations.pdf. (Accessed May 28, 2018.)

[27] Stanley G. Payne, *The Spanish Civil War* (Cambridge: Cambridge University Press, 2012), 1.

[28] Payne, *Spanish Civil War*, 144.

United Nations.[29] Under the United Nations, international law gave greater clarity on the subject of nonintervention by member states into the sovereignty of other states. The United Nations Charter clearly does not allow member states "to intervene in matters which are essentially within the domestic jurisdiction of any state."[30] However, the charter limits permissible interventions as those taken against "the existence of any threat to peace, breach of the peace, or act of aggression."[31]

In 1965, the United Nations adopted another resolution to further enhance its non-intervention law by passing a declaration on the inadmissibility of intervention in the domestic affairs of states and the protection of their independence and sovereignty. That resolution states:

> No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned.[32]

In addition, there is a customary international norm of non-intervention that is generally adhered to by all member states. Global multilateral and bilateral treaties are complemented with customary international law when it comes to maintaining the state's sovereignty over its domestic affairs. Article 38 (1)(b) of the International Court of Justice (ICJ) underscores state practice as being part of the norms of customary

---

[29] Leland M. Goodrich, "From League of Nations to United Nations," *International Organization* 1, no. 1 (1947): xx.

[30] U.N. Charter, Article 2, paragraph 7.

[31] U.N. Charter, Article 39.

[32] U.N. Resolution 2131.

international law.[33] Whereas treaties are signed and binding agreements made between signatory states, customary international law originates from "general practice, accepted as law"[34] between different countries yet still considered binding as outlined by ICJ. The rules of nonintervention under customary law are widely understood and adopted by the states, even with varied intentions. For instance, NATO's military intervention in Kosovo, although considered illegal under the U.N. charter, was widely viewed by others as legal under customary international law.[35] In many ways, customary international law is more powerful and far-reaching than treaties signed between countries. Customary international law expands treaties to include countries that may not have ratified a treaty.[36] Due to the rapidly growing and lasting nature of customary law, much of the evolving practice of nonintervention and state sovereignty can be handled by customary international law.

The U.N. charter, however, has not stopped states from interfering in each others' internal political affairs. Although the vertical relationship between the United Nations and its member states offers a workable framework for international non-intervention and permissible intervention under the principles of collective security, some countries, such as those in ASEAN and the European Union also engage in bilateral and regional treaties.

---

[33] Birgit Schlütter, *Developments in Customary International Law: Theory and the Practice of the International Court of Justice and the International Ad Hoc Criminal Tribunals for Rwanda and Yugoslavia* (Dordrecht, Netherlands: Brill, 2010), 13.

[34] Schlütter, *Developments in Customary International Law*, 10.

[35] Anthony D'Amato, "New approaches to Customary International Law," *American Journal of International Law* 105, no. 2 (January 2011).

[36] Michael P. Sharf, "Accelerated formation of Customary International Law", *ILSA Journal of International and Comparative Law 20*, Issue 2 (Spring 2014): 309.

In 1986, the ICJ further defined the rules of non-intervention under the U.N. charter by stating:

> Notwithstanding the multiplicity of declarations by States accepting the principle of non-intervention, there remain two questions: first, what is the exact content of the principle so accepted, and secondly, is the practice sufficiently in conformity with it for this to be a rule of customary international law? As regards the first problem—that of the content of the principle of non-intervention—the Court will define only those aspects of the principle which appear to be relevant to the resolution of the dispute. In this respect, it notes that in view of the generally accepted formulations, the principle forbids al1 States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[37]

According to the Report of the International Commission on Intervention and State Sovereignty, states have a duty of nonintervention in other states' internal affairs, and every state has a right to defend its territorial integrity and political independence.[38]

---

[37] International Court of Justice (ICJ), "Military and Paramilitary Activities in and Against Nicaragua," Nicaragua v. United States of America. I.C.J. Reports, 1986. http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf. (Accessed 15 November 2018.)

[38] International Coalition for the Responsibility to Protect (ICRtoP), Chapter 2, Sec. 2: 8, 12. http://responsibilitytoprotect.org/ICISS%20Report.pdf.

## Coercion Under Customary International Law

Coercion is defined as the effort to get a state, the leader of a state, or a group to do something it does not want to do.[39] In a bilateral and multilateral international relationship, states deploy both cooperative and coercive tools to gain political and economic influence in other countries. Economic and military power can be used as an aid or as a threat to gain a desirable international outcome. Article 16 of the Charter of the Organization of American States (OAS) states: "No State may use or encourage the use of coercive measures of an economic or political character in order to force the sovereign will of another State and obtain from it advantages of any kind."[40] However, international custom has understood and adopted the use of both cooperative and coercive nature of state powers. The challenge with International Customary Law is that although states accept it as law, its interpretation is subject to the state's own understanding and convenience as it originates from the organic actions of states over time.[41]

Some scholars believe that coercion has no illegal nature as it originates from common human behavior in general life, and therefore has no normative significance in international customary law.[42] According to Tom Farer, some advocate that coercion is a direct violation of U.N. Article 2, Section 4. Douglas Rushkoff argues that everything is coercive. He says: "The fact is, everything is coercive. . . . There is nothing wrong with

---

[39] Kelly M. Greenhill, and Robert J. Krause, *Coercion: The Power to Hurt in International Politics* (Oxford: Oxford University Press, 2018), 4.

[40] Tom J. Farer, "Political and economic coercion in contemporary international law," *American Journal of International Law* 79, no. 2 (1985): 406.

[41] Guzmán, *How International Law Works*, 2.

[42] Farer, *Political and Economic Coercion*, 406.

attempting to sway others to our own way of thinking, especially if we truly believe we are right. It's how relationships, families, businesses and societies improve themselves."[43]

Countries like the United States have used economic and military coercion as an effective tool to advance their international agenda. As part of acceptable customary international law, economic coercive actions such as embargo were implemented against Cuba, Iran, and North Korea by the international community. The ICJ, through its decision in 1986 on United States v. Nicaragua, made clear that economic coercion is not in accordance with customary international law.[44]

Economic sanctions are considered one of the most potent coercive tools at the disposal of UN Security Council as well as individual states. Although the Security Council decides on the scope and scale of sanctions in response to a perceived threat to international peace and security, some states and regional organizations introduce individual sanctions in addition to or in the absence of Security Council-led coercive sanctions. Natalino Ronzitti concludes: "Economic pressures do not necessarily violate international law, and they do not trigger responsibility if they do not infringe customary or conventional norms."[45]

Despite the controversial nature of coercion under customary international law, states have employed coercive actions to benefit their state interests in order to extend their strategic objectives. However, its important to realize that unilateral economic,

---

[43] David Rushkoff, *Coercion: Why We Listen to What "They" Say?* (NY: Riverhead, 2000), 18.

[44] Richard D. Porotsky, "Economic coercion and the General Assembly: A post-Cold War assessment of the legality and utility of the thirty-five-year-old embargo against Cuba," *Vanderbilt Journal of Transitional Law* 28, no. 4 (1995): 919.

[45] Natalino Ronzitti, as quoted in Chiara Franco, Report of the International Conference on "Coercive Diplomacy, Sanctions and International Law." Istituto Affari Internazionali (IAI), Rome, 13 February 2015. http://www.iai.it/sites/default/files/iai1505.pdf. (Accessed 15 November 2018.)

military, and political coercive actions taken in response to probable aggression should be within the boundaries set forth by the customary law, and their legality can be determined by the nature of each coercive regime.[46]

## Espionage and International Law

Former U.S. President Dwight D. Eisenhower said, on May 11, 1990: "The position of the United States was made clear with respect to the distasteful necessity of espionage activities in a world where nations distrust each other's intentions."[47] As one of the world's oldest professions, espionage is usually defined as overt or covert collection of information about a country's adversary for the purpose of benefiting the perpetrating country. During information-gathering operations, uniformed personnel who are caught behind enemy lines during war are treated under international law.[48] Similar activities undertaken by non-uniformed personnel are treated by their captors under their domestic laws. In an article on espionage, Beim Jared states:

> The simplest and most effective enforcement mechanism often is domestic law. A government can take measures to enforce a prohibition of espionage within its own borders, and none of the above is to say that peacetime espionage violations would not be enforced in this way. However, the specific nature of espionage often precludes enforcement by domestic law, especially in instances where physical agents manage to escape a target country.[49]

---

[46] Chiara Franco, "Report of the International Conference," 7.

[47] Dwight D. Eisenhower, "Our first line of defense: Presidential reflections on U.S. intelligence." https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/our-first-line-of-defense-presidential-reflections-on-us-intelligence/eisenhower.html. (Accessed May 31, 2018.)

[48] The Hague Convention of 1907, "Convention Respecting the Laws and Customs of War on Land," Article 3, 1910. Library of Congress. http://www.loc.gov/law/help/us-treaties/bevans/m-ust000001-0631.pdf.

[49] Beim Jared, "Enforcing a prohibition on international espionage," *Chicago Journal of International Law* 18, no. 2 (2018): 647-672.

Due to the unregulated nature of espionage, there are varying opinions among legal experts about the nature of peacetime espionage under international law and the subject is widely contested among scholars. The Vienna Convention on Diplomatic Relations states that diplomats cannot interfere in the domestic affairs of their host country.[50] Taking a current example, Edward Snowden (accused of espionage and currently living under asylum in Russia, leaked information that not only revealed a U.S. espionage program focused on gaining insights about the leadership of allied countries,[51] but his action also brought into focus a conversation about current tangible practice against both international customary law and treaties.[52] Since there are no formal customary laws or treaties that exclusively forbid espionage, due to the Lotus principle developed by the Permanent Court of International Justice (PCIJ),[53] countries actively engage in peace-time espionage.

From economic to political espionage, countries strive to gain competitive advantage, and such activities cannot be deemed justifiable under the principle of self-

[50] Zahra Baheri and Ali S. Fard, "Status of espionage from the perspective of international laws, with emphasis on countries' diplomatic and consular relations," *Journal of Scientific Research and Development* 2, no. 1 (2015): 41-45.

[51] BBC News, "How the US Spy Scandal Unraveled." http://www.bbc.com/news/world-us-canada-23123964.

[52] Ashley Deeks, "The increasing state practice and *opinio juris* on spying," *Lawfare.* May 6, 2015. https://www.lawfareblog.com/increasing-state-practice-and-opinio-juris-spying. (Accessed 15 November 2018.)

[53] Hugh Handeyside, "The Lotus Principle in ICJ jurisprudence: Was the ship ever afloat?," Michigan Journal of International Law 29, no. 1 (2007): 71-94. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1145&context=mjil.

defense. However, many scholars believe that the act of espionage, especially during peace time, is in direct violation of the principle of state sovereignty.[54]

## State Responsibility for Violations by Non-State Actors

International law holds states accountable for violations by non-state actors if such actions are directed or controlled by the state. In the absence of a legal framework, states can escape accountability by hiding behind non-state actors. Robert Kolb notes: "The State could escape responsibility by merely indicating that these persons are not its de jure organs or agents, and even more, a State could covertly have recourse to such de facto organs and agents in order to avoid international responsibility."[55] Therefore, control lies at the center of the challenge of where attribution lies. Kristen Boon argues that effective control as a *de facto* standard for the secondary rules of attribution is waning, despite the ICJ's affirmation of effective control in the Bosnian genocide decision.[56] Article 8 of the UN General Assembly's "Responsibility of States for Internationally wrongful Acts," also emphasizes a state's control over its organs to prove state attribution.[57]

---

[54] Patrick Terry, "Absolute Friends": United States espionage against Germany and public international law," *Revue québécoise de droit international* 28, no. 2 (2015): 173-203.

[55] Robert Kolb, *International Law of State Responsibility: An Introduction* ( Cheltenham, England: Elgar, 2017), 70-108. https://www.elgaronline.com/view/9781786434708/10_chapter3.xhtml. (Accessed 15 November 2018.)

[56] Kristin E. Boon, "Are control tests fit for the future? The slippage problem in attribution doctrines," *Melbourne Journal of International Law* 15, no. 2 (2014): 329.

[57] United Nations General Assembly, "International Law Commission, Articles on State Responsibility" 2001. https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility.

Attribution of possible illegal activities by citizens of a state has become a challenge in the rapidly evolving digital world. Although customary international law regarding a state's responsibility extends to cyber activities,[58] the actions of non-state actors or citizen-activists pose a challenge to clearly attributing an activity in cyberspace to a specific state. The *Tallinn Manual 2.0* on cyber operations helps explain the challenge of attribution based on the concept of a state's effective control.[59] The *Manual* states: "In the context of unilateral self-help measures, the reality is that states must make *exante* determinations with respect to attribution of a cyber operation to another State before responding."[60]

The International Law Commission struggled with this issue when drafting the Articles on State Responsibility, but did not express a definitive position.[61] Identity masking and use of multiple bypass methods by the alleged cyber attackers make it very challenging for a state to undeniably attribute an individual's actions to a state. The challenge of having the ability to clearly attribute a cyber attack to a state kept Iran[62] and Estonia[63] silent when their infrastructures experienced cyber intrusions. However, with technological advancements and traditional intelligence networks, some countries like the

---

[58] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 80.

[59] Schmitt, *Tallinn Manual 2.0,* 80.

[60] Schmitt, *Tallinn Manual 2.0,* 81.

[61] Schmitt, *Tallinn Manual 2.0*, 81.

[62] Michael B. Kelley, "The Stuxnet attack on Iran's nuclear plant was far more dangerous than previously thought," *Business Insider.* http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[63] Patrik Maldre, "The Russian cyber threat: Views from Estonia," Center for European Policy Analysis, May 18, 2016. https://cepa.ecms.pl/The-Russian-Cyber-Threat-Views-from-Estonia. (Accessed 15 November 2018.)

United States, recently have developed the ability to attribute certain cyber attacks against its infrastructure to the actions of a hostile government.

# Chapter V

## Current Practice and the Normative Approach

The International Court of Justice's judgment rendered in Nicaragua v. United States has significant value for understanding the principles of sovereignty and nonintervention in customary international law. The court made it clear that the principle of nonintervention relates to both internal and external affairs of states.[64] Determining political, economic, and social outcomes falls within the realm of internal affairs, and foreign intervention in the form of direct military intervention or indirect coercive intervention is wrong and against customary international law and treaties. Denise Raynova wrote in a report: "Perceived challenges to state's interests, disruptions to power balances, or challenges to the political status quo can become reasons to intervene in the internal affairs of other states despite the norm against it."[65]

Despite global agreement on the U.N. charter of nonintervention in the internal affairs of member states, powerful states have been overtly and covertly interfering in the political processes of other states as a way to secure their strategic interests. Cyberspace has brought new dimensions to foreign interventions as countries now frequently attack each other's domestic digital infrastructure as part of coercive espionage campaigns or to directly sabotage a victim's digital infrastructure. The launch of Stuxnet to damage Iran's

---

[64] Marcelo Kohen, "The principle of non-intervention 25 years after the Nicaragua judgment," *Leiden Journal of International Law* 25, no. 01 (2012): 158-159.

[65] Denise Raynova, "Toward a Common Understanding of the NonIntervention Principle," European Leadership Network, October 2017. https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/170929-ELN-Workshop-Report-Non-Intervention.pdf.

nuclear infrastructure[66] is one of thousands of examples of cyber attacks aimed at impacting the social, economic, military, and political outcome in a victim country. Recent mistrust between Russia and the West originates from alleged Russian interference in U.S. and European elections, which directly violates the noninterventionist principle.[67]

## Foreign Intervention by Major Powers

Ever since legal scholars like Grotius and Suarez introduced the principles of foreign intervention in the fifteenth century, the methods used to intervene in foreign countries have become more complex.[68] From clandestine operations by the U.S. in Nicaragua (1984) and Spain (1930),[69] to Russian military support given to rebels in Georgia and Ukraine, major powers—and regional powers like Iran, India and the United Kingdom—in violation of the customary international law, have tried to interfere in the political processes of other countries. The frequency of such actions has increased significantly due to competitive elections worldwide. Cornell University's post-doctoral fellow Dov Levin states: "Attempts by a great power to meddle in an election of an-other

---

[66] Kim Zetter, "An unprecedented look at Stuxnet, the world's first digital weapon," *Wired*, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. (Accessed 15 November 2018.)

[67] In this thesis, I keep the scope of my focus on pre-election interventions by foreign countries, and have chosen not to extend the scope further to include military intervention and economic coercion.

[68] William Mattessich, "Digital destruction: Applying the principle of non-intervention to distributed denial of service attacks manifesting no physical damage," *Columbia Journal of Transitional Law* 54, no. 3 (September 4, 2016): 873-896.

[69] Thomas Jackamo, "From the Cold War to the new multilateral world order: The evolution of covert operations and the customary international law of non-intervention," *Virginia Journal of International Law* 32, no. 4 (1992): 930.

country in favor of a particular candidate or a specific party may shape electoral outcomes."[70] Some examples of intervention by major powers are given below.

In 1948, U.S. intervention in Italian elections was a bold attempt to steer election results to favor the Christian Democrat candidate, which resulted in their win against the Communist party. The U.S. poured more than $65 million into psychological warfare on behalf of the Christian Democrats between 1948 to 1968, with the U.S. threatening to withdraw economic and military assistance if the Communists were elected.[71] Since that time, the Christian Democrat Party remains as one of the major political powers in Italy.[72]

The U.S. government established a close relationship with Thailand's government during the Vietnam war, launching almost 80% of U.S. strikes and covert operations in Vietnam from the U.S. base in Thailand. In return, the Thai military and government officials received millions of dollars in funding between 1950 and 1975.[73] During the 1969 Thai elections, the U.S. government heavily favored the UTPT party by spending millions of dollars before the elections to improve the party's chances of winning.[74]

U.S. intervention in Thailand's election process did not end with the Vietnam war. According to the Center for Research on Globalization, while many conversations have been held about Russian meddling in the 2016 U.S. elections, the U.S. is today trying to influence Thailand by funding their media organizations to call for protests in

---

[70] Levin, *When the Great Power Gets the Vote*.

[71] Deborah Kisatsky, *The United States and the European Right, 1945-1955* (Columbus: Ohio State University Press, 2005), 113.

[72] Laurence Whitehead, *The International Dimensions of Democratization Europe and the Americas* (Oxford: Oxford University Press, 2004), 52.

[73] Arne Kislenko, "A not so silent partner: Thailand's role in covert operations, counter insurgency, and the wars in Indochina," *Journal of Conflict Studies* 24, no. 1 (Summer 2004). https://journals.lib.unb.ca/index.php/jcs/article/view/292/465. (Accessed 15 November 2018.)

[74] Levin, "Partisan Electoral Interventions," 3.

the favor of earlier elections. With direct funding through National Endowment for Democracy (NED), U.S. hopes to get its proxy, Thaksin Shinawatra, and his Pheu Thai Party (PTP) in power.[75]

Latin America has also seen a fair amount of overt and covert U.S. interventions. Consider the U.S. intervention in the Dominican Republic in 1965;[76] the U.S. invasion of Grenada, ordered by President Ronald Reagan in 1983;[77] and Operation Just Cause in Panama at the end of 1989;[78] in each instance, the U.S. openly brought its allies to political power in these countries.

Russia has used a mix of military and economic power to influence elections in the former Soviet republics of Ukraine, Georgia, and Crimea. In early 2014, while hiding behind the Ukrainian parliamentary decision to repeal the official status of the Russian language, Russia took military steps to annex Crimea from Ukraine. Also, to support the Russian population residing in Ukraine, the Kremlin poured military might into its border with Ukraine.[79] In August 2008, the pro-West government of Georgia sent troops to its breakaway region of South Ossetia. To support South Ossetia and Abkhazia, Russia took military action against Georgia, resulting in the independence of both regions. According

---

[75] Joseph Thomas, "Confirmed US meddling in Thailand's Upcoming Elections," *New Eastern Outlook*, February 21, 2018. https://journal-neo.org/2018/02/21/confirmed-us-meddling-in-thailands-upcoming-elections/. (Accessed 15 November 2018.)

[76] Russell Crandall, *Gunboat Democracy: U.S. Interventions in the Dominican Republic, Grenada, and Panama* (Lanham, Md: Rowman & Littlefield, 2006).

[77] Stephen Zunes, "The U.S. Invasion of Grenada," Global Policy Forum, October 2003. https://www.globalpolicy.org/component/content/article/155/25966.html. (Accessed 15 November 2018.)

[78] Independent Commission of Inquiry on the US Invasion of Panama,*The U.S. Invasion of Panama: The Truth Behind Operation "Just Cause"* (Boston: South End Press, 1992), 3-8.

[79] Michael Kofman et al., "Lessons from Russia's Operations in Ukraine," RAND Corporation , xii. https://www.rand.org/pubs/research_reports/RR1498.html. (Accessed 15 November 2018.)

to Dov Levin, the U.S. and Russia have both interfered in the electoral processes on every continent except the countries of Oceania (see Figure 4).

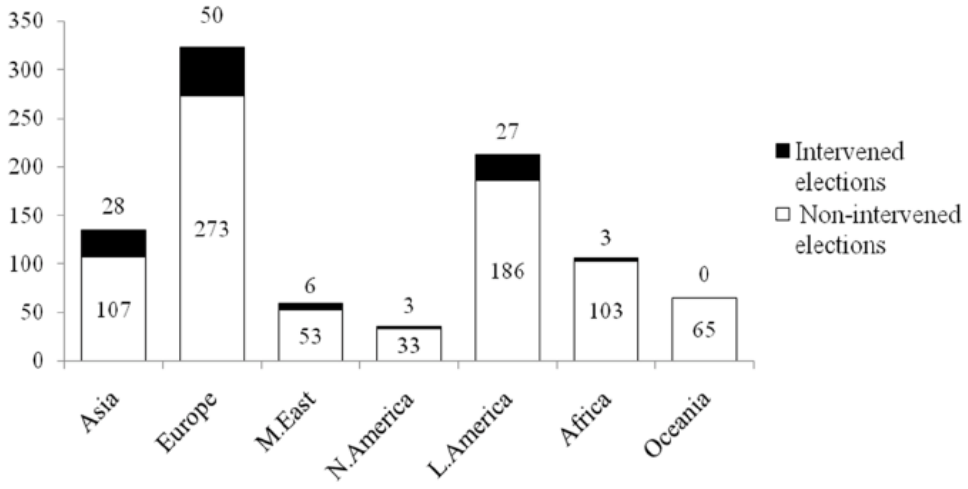


Figure 4. Intervention by the US and USSR/Russia in Foreign Countries.

Source: Levin, 2016.

In the past, countries like United States and Russia may have used traditional coercive techniques to interfere in the internal affairs of foreign countries. But with the expansion of cyberspace, well-equipped countries now use coercive cyber attacks and digital media campaigns to influence the political outcome in other countries which may be in direct violation of customary international law.[80]

[80] Schmitt, *Tallinn Manual 2.0*, 80.

## Risks of Cyberspace

Sony Pictures released a movie named "The Interview," a story about two young Americans going to interview a North Korean leader, but in fact they were hired by the CIA to assassinate President Kim Jong Un. Soon before the was movie released, alleged North Korean operatives hacked into Sony Pictures servers and threatened to release their internal emails. In retaliation, the U.S. government is alleged to have taken down internet access for all computers in North Korea.[81] The moves were a blatant violation of customary international law, and once again highlighted the dangers of cyber warfare, especially cyber espionage.

Cyber interference does not stop with private corporations. In new threats to the principles of sovereignty and nonintervention, countries have tried to extend their influence through a variety of powerful tools including digital media, denial of service, and hacking. Scholars generally believe that cyber espionage or attacks violate international laws; however, it is a challenge to associate such actions with exact law in the international arena.[82]

The advent of digital media in cyber sphere has pushed pre-election conversations among citizens and communities outside the realm of traditional media by providing opinion platforms capable of spreading the message without any barriers. World powers view platforms like Google, Facebook, Twitter, and Instagram as powerful tools for spreading the message of democracy and helping to bring social change across the

---

[81] David Sanger, David Kirkpatrick, and Nicole Perlroth, "The world once laughed at North Korean cyberpower. No More," *New York Times*. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

[82] Jens D. Ohlin, "Did Russian cyber interference in the 2016 election violate international law? *Texas Law Review* 95, no. 7 (2017): 1579-1598. https://ssrn.com/abstract=2934321. (Accessed 16 November 2018.)

borders without government restrictions. Social media-powered political activism has been hailed as a major power behind confronting social conformity,[83] achieving democratic development and political change,[84] and a powerful agent for driving out corruption,[85] bigotry, and lies. It seems clear that countries with higher public penetration into digital infrastructure and access to open internet, pose greater challenges for information security.[86]

According to Pew Research, more than 79% of American adults now use social networking sites, up from 7% in 2015,[87] with more than 1.8 billion active monthly users worldwide on Facebook.[88] Users spend an average of at least 50 minutes[89] each day on social media platforms. The proliferation of social media platforms among millenials has encouraged political activists to gravitate toward these platforms as another successful method for spreading their message. On one hand, Western countries like the United States have promoted the use of social media platforms and supported adoption of the internet in countries with oppressive regimes, thus igniting public uprisings like the

---

[83] Glenn W. Richardson, *Social Media and Politics: A New Way to Participate in the Political Process* (Santa Barbara: Praeger, 2017), 8.

[84] Nhamo A. Mhiripiri, and Tendai Chari, *Media Law, Ethics, and Policy in the Digital Age* (Hershey, PA: IGI Global, 2017), 168.

[85] Rania Fakhoury, "Can social media, loud and inclusive, fix world politics?," *The Conversation.* https://theconversation.com/can-social-media-loud-and-inclusive-fix-world-politics-74287.

[86] Kelly M. Greenhill, and Robert J. Krause. *Coercion: The Power to Hurt in International Politics* (Oxford: Oxford University Press, 2018), 179.

[87] Shannon Greenwood, Andrew Perrin, and Maeve Duggan, "Social Media Update 2016," Pew Research Center. http://www.pewinternet.org/2016/11/11/social-media-update-2016/.

[88] Rosamond Hutt, "The world's most popular social networks, mapped," World Economic Forum. https://www.weforum.org/agenda/2017/03/most-popular-social-networks-mapped/.

[89] James Stewart, "Facebook has 50 minutes of your time each day. it wants more," *New York Times.* https://www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html.

Orange Revolution in Ukraine (2014)[90] and the so-called "Arab Spring" in several Middle East countries (2011).[91] On the other hand, open digital platforms in Western countries have exposed those countries to foreign coercive campaigns while frequently violating customary international law.[92]

[90] Cecily Hilleary. "Ukraine's social media revolution years in the making," *Voice of America News,* March 14, 2014. https://www.voanews.com/a/ukraines-protest-movement-fueled-by-social-media/1871457.html.

[91] Heather Brown, Emily Guskin, and Amy Mitchell, "The role of social media in the Arab uprisings," Pew Research Center, November 28, 2012. http://www.journalism.org/2012/11/28/ role-social-media-arab-uprisings/.

[92] Steven R. Swanson, "Forcing Facebook on foreign dictators: A violation of international law," *Tennessee Law Review* 79, no. 4 (2012): 851.

# Chapter VI

## Methods of Digital Intervention

U.S. presidential elections in 2016 revealed the alleged involvement of a major foreign power in the country's national elections. This may not be the first time a foreign power became involved in the pre-election process of another country, but it surely highlighted new tactics, using social media with brazen sophistication. Hillary Rodham Clinton, 2016 Democratic presidential candidate, argued:

> The real news, however, was that the Russian intervention had gone far beyond hacking email accounts and releasing files. Moscow had waged sophisticated information warfare at a massive scale, manipulating social media and flooding it with propaganda and fake news.[93]

The candidate choices available to the American populace was not usual. As voters sought to identify difference between the two candidates, they were influenced (overtly and alleged covertly) by a series of social media campaigns specifically focused on undermining the Democratic candidate, Hillary Clinton. Media has always taken center stage in every national political campaign as a way to expand ideological influence and control.[94] However, digital media has blurred the boundaries behind the spread of some ideological messages.

---

[93] Hillary Rodham Clinton, *What Happened* (NY: Simon & Schuster, 2018), 352.

[94] Edward S. Herman, Noam Chomsky, and John Pruden, *Manufacturing Consent: The Political Economy of the Mass Media* (Old Saybrook, CT: Tantor Audio, 2017).

Special Counsel Robert Mueller, in his February 2018 indictment of 13 Russian individuals and organizations stated:

> Defendants, posing as U.S. persons and creating false U.S. personas, operated social media pages and groups designed to attract U.S. audiences. These groups and pages, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by Defendants. Defendants also used the stolen identities of real U.S. persons to post on organization-controlled social media accounts. Over time, these social media accounts became Defendants' means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the presidential election of 2016.[95]

Rival countries have used several tools to infiltrate each other's digital infrastructure. From stealing commercial secrets, intellectual property, and trade secrets to gaining insight into government operations, adversary countries often focus their direct and indirect attacks on each other. The rapid adoption of digital platforms to manage daily lives, communication, dialogue, and information storage (48% of these services are delivered via cloud[96]) also provides ample opportunity for cyber hackers to steal or alter information for their benefit. According to an IRTC data breach report, 177,866,236 individual records were exposed due to hacking activities in 2015.[97]

A great many digital threats come from individual cyber hackers and groups. But due to the ambiguous nature of these groups, some states have leveraged their capabilities to extend their strategic goals. Groups like Anonymous, Computer Chaos Club, OurMine,

---

[95] U.S. Department of Justice, "The Grand Jury for the District of Columbia" Charges," Case 1:18-cr-00032-DLF Document 1, filed 02/16/18. https://www.justice.gov/file/1035477/download. (Accessed 16 November 2018.)

[96] PriceWaterhouse Coopers, "How businesses are embracing a modern approach to threat management and information sharing," *Global State of Information Society Survey*, 2017. http://www.pwc.com/gsiss. (Accessed 16 November 2018.)

[97] Identity Theft Resource Center (ITRC), "Data Breach Reports," December 29, 2015. http://www.idtheftcenter.org/images/breach/DataBreachReports_201. (Accessed 16 November 2018.)

Syrian Electronic Army, and LuizSec[98] are just few of many that are testing the world's digital infrastructure every day.

## Distributed Denial of Service Attacks

Distributed Denial-of-Service (DDoS) attacks occur when multiple connected online devices (usually known as 'bots" try to generate so much fake traffic that it overwhelms the server of the target site, causing it to shut down. DoS is not only one of the easier ways to disrupt services in a foreign country, it is also difficult to link a foreign administration as the source of such attacks, particularly when that government may hide behind individuals or pseudo organizations. According to Verisign, a leading internet security company, DDoS attacks have rapidly increased and are becoming more sophisticated (see Figure 5).

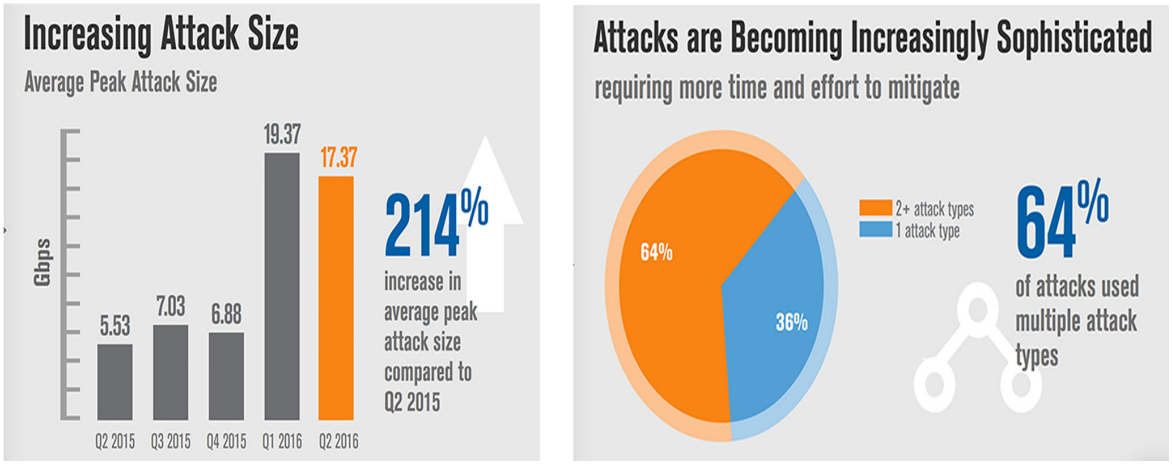


Figure 5. Increasing Size and Sophistication of DDoS Attacks.

Source: Verisign, 2016.

[98] David Z. Morris, "How hackers make money from DDoS attacks," *Fortune*, October 22, 2016. http://fortune.com/2016/10/22/ddos-attack-hacker-profit/.

DDoS attacks are not new to cyber attackers who use machines or network not available to users to flood a site with fake requests. This tactic has been used by every web-enabled nation against its adversaries' digital infrastructure. For instance, Russian servers have been linked to DDoS attacks on the financial networks of Netherland, Crimea, Malaysia, and Kazakhstan,[99] as well as the government and business infrastructures of its former republics of Estonia, Georgia, and Ukraine.[100] The governments of China and the U.S. have also accused each other for similar attacks on their respective infrastructures.

## DDoS Attacks During Elections

During the 2016 U.S. presidential elections, cybersecurity firm Flashpoint reported: "Between 16:20 UTC on November 6, 2016 and 8:19 UTC on November 7, 2016, four 30-second HTTP Layer 7 attacks targeted the campaign websites of presidential candidates Donald Trump and Hillary Clinton."[101] Although the unsuccessful attacks seemed to be carried out by an individual, they appeared to be a part of a larger plan to influence the elections. Hackers like Jono Gaukster went open with their intentions (see Figure 6). During the election campaign, many private companies like Twitter, PayPal, and Spotify were attacked, and users complained they could not reach news organization like CNN, *New York Times*, Yelp, and *Wall Street Journal*. In 2017, the French media experienced a

---

[99] Robert Windrem, "Timeline: Ten years of Russian cyber attacks on other countries," *NBC News,* December 18, 2016. https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111. (Accessed 16 November 2018.)

[100] Christian Czosseck, and Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: IOS Press, 2009), 163-179

[101] Allison Nixon, John Costello, and Robbie Tokazowski, "Flashpoint monitoring of Mirai shows attempted DDoS of Trump and Clinton websites," *Flashpoint,* November 7, 2016. https://www.flashpoint-intel.com/blog/trending/attempted-ddos-trump-and-clinton-websites/.


Figure 6. Twitter Feed from Possible Cyber Attacker

Source: Twitter

DDoS attack that caused a brief shutdown of French newspaper sites including Le Monde, Le Figaro, L'Equipe, Le Nouvel Observateur.[102] In 2011, Russian media experienced a series of DDoS attacks against its opposition media and blog sites.[103]

Since then, countries have used DDoS attacks to affect other digital infrastructure as well. A successful DDoS attack can take down online voting machines, which are used by five U.S. states. Such attacks can also disrupt the voting process by targeting the voter registration system.

## Server Hacks

Since the advent of the digital age in the twentieth century, malicious individuals and entities have continuously attacked servers to gain illegal access to user data. In the

[102] Yohai Einav, "The DDoS Attack on French Media," *Akamai Security Intelligence and Threat Research Blog*, Intelligent Platform, Spring 2018. https://www.nominum.com/tech-blog/ddos-attack-french-media/.

[103] Hal Roberts and Bruce Etling, "Coordinated DDoS attack during Russian Duma elections," Internet and Democracy Blog, Weblogs at Harvard, December 8, 2011. http://blogs.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/.

beginning, business and public secrets were subject to hacking, but more recently hacked information has been used to influence public opinion in a major election, with a cyber attack happening every 39 seconds.[104] By hacking into servers or data storage devices through web floods, phishing, SQL injections, and social engineering (among others), hackers illegally gain access to sensitive private information and use that information to either blackmail or influence the subject.

Fears of cyber espionage have recently increased as China and Russia have improved their cyber-intrusion capabilities. Chinese hackers, backed by the Chinese military, allegedly gained entry into U.S. power systems and left behind software capable of sabotaging the infrastructure.[105]

Hacking During U.S. Elections

March 19, 2016: John Podesta, then-chairman of Democratic presidential candidate Hillary Clinton's campaign, received an email from "Gmail Team" asking him to reset his password. Podesta, on the advice of his technology team, resets his password through the provided link in what turned out to be a phishing email. With Podesta's click, the Democratic campaign was revealed, laying out the foundation of their defeat in the 2016 presidential election. U.S. intelligence later concluded that a typo-laden email was part of an elaborate hacking campaign designed by the Russians.[106]

---

[104] Michael Cukier, "Study: Hackers attack every 39 seconds," February 9, 2007. University of Maryland. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (Accessed 16 November 2018.)

[105] Lansing Gordon, *Rise of the Cybergens* (NJ: Bookbaby, 2015), Chapter 5.

[106] Jim Sciutto, "How one typo helped let Russian hackers in," *CNN*, June 27, 2017. https://www.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html.

Three months later, WikiLeaks founder Julian Assange admitted that he planned to publish Hillary Clinton's emails. Security experts were later able to link these attacks with the notorious Russian backed group 'Cozy Bear' or 'APT28' and hackers at Dutch intelligence agency AIVD were successfully able to infiltrate the computer network of 'Cozy Bear' in Moscow to get evidence of their hacking of DNC systems[107]. AIVD later deducted the relationship between 'Cozy Bear' and Kremlin.

## Hacking During European Elections

Borrowing from the successful playbook of meddling in the 2016 U.S. presidential elections, in 2017 the Kremlin allegedly tried to influence the outcome of French and German national elections. U.S. intelligence is confident that Russians tried to sway the French presidential election by hacking into and leaking emails belonging to the centrist candidate, Emmanuel Macron.[108]

Using hacking as an effective tool to gain access to sensitive information, Russians also tried to sway German elections in 2017 by placing malware in the German government network. German security experts blamed the Kremlin-linked group "APT28" or the "Cozy Bear" group for hacking into the defense and foreign ministries.[109] In another instance, the United Kingdom GCHQ's Cyber Security Center warned of

---

[107] Huib Modderkolk, "Dutch agencies provide crucial intel about Russia's interference in US elections," *Volkskrant*, January 25, 2018. https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/. (Accessed 16 November 2018.)

[108] Mark Hosenball, "U.S. increasingly convinced that Russia hacked French election, *Reuters*, May 9, 2017. https://www.reuters.com/article/us-france-election-russia/u-s-increasingly-convinced-that-russia-hacked-french-election-sources-idUSKBN1852KO. (Accessed 16 November 2018.) See also: Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (New Haven, CT: Yale University Press, 2017).

[109] Deutsche Welle, "Germany admits hackers infiltrated federal ministries, Russian group suspected," February 28, 2018. http://www.dw.com/en/germany-admits-hackers-infiltrated-federal-ministries-russian-group-suspected/a-42775517.

possible state-sponsored malicious cyber activity that sought to impact UK energy, manufacturing, and water services sectors.[110]

## Fake News

Misinformation or propaganda campaigns have long been part of the political landscape. George Orwell's novel *1984,*[111] although published in 1949, predicted a political future run by misinformation. People in the 21st century can relate to Orwell's vision of society, especially after the 2016 U.S. presidential election. An unrestricted information flow, unhampered by geographical boundaries and helped by digital media platforms, has amplified the possibility of an Orwellian society. Effective propaganda campaigns have been used by almost every country in the world as part of the information warfare strategy. During the Cold War era, traditional misinformation campaigns generally originated from within physical borders, making them easier to identify.

During the 2016 elections, a new/old phrase began to appear: *fake news*, which is viewed by the World Economic Forum as one of the top perils to open societies.[112] Fake news generally spreads via digital media as people and bots post deceptive or incorrect information on social media under the guise of legitimate news, hoping to influence public opinion. In the Summer of 2016, Republican presidential candidate Donald J.

---

[110] Oscar Williams-Grut, "Report: Russia Hacked UK Energy Companies on Election Day," *Business Insider-UK*, November 14, 2017. http://www.businessinsider.com/russia-hacked-uk-energy-companies-election-day-2017-7?r=UK&IR=T. (Accessed 16 November 2018.)

[111] George Orwell, *1984* (Boston: Houghton Mifflin, (1949) 2018.

[112] Farida Vis, "The Rapid Spread of Misinformation," *World Economic Forum*, 2014. http://reports.weforum.org/outlook-14/wp-content/blogs.dir/30/mp/files/pages/files/trend-10.pdf.

Trump used the term "fake news" to describe any news from media sources that he considered unfriendly.

While Trump was labeling opposition media as fake, Kremlin-backed groups and companies orchestrated a powerful disinformation campaign as part of their efforts to influence the electoral outcome of the 2016 election. Stories about Pope Francis endorsing Donald Trump, or Hillary Clinton supplying weapons to terrorist organizations went viral through various social media platforms like Facebook.[113]

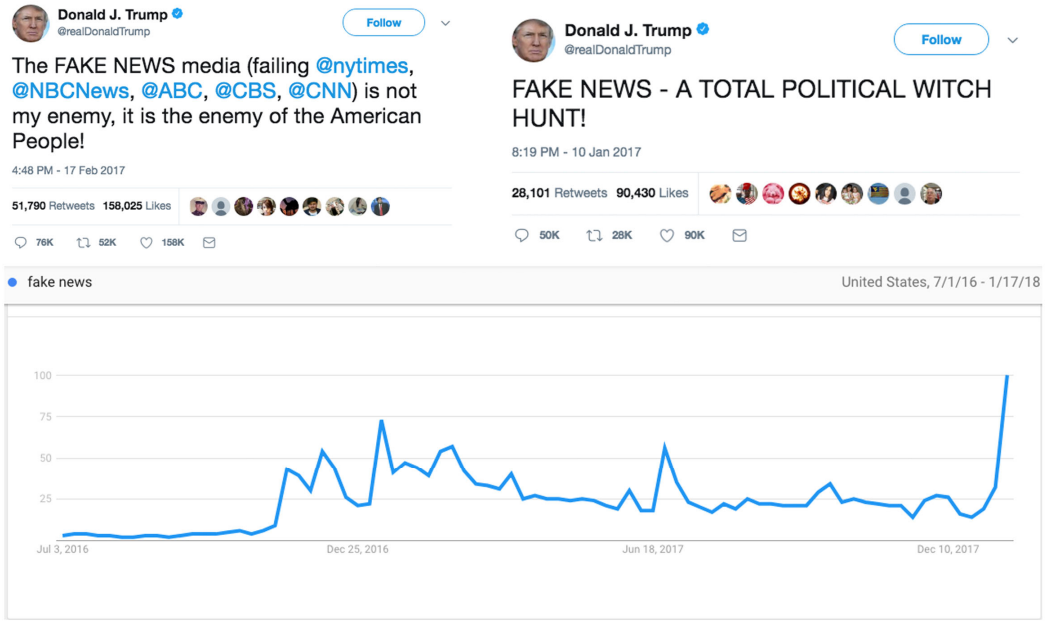


Figure 7. Examples of Fake News Chatter.

Source: Twitter

[113] Lucia Graves, "How Trump weaponized 'Fake News' for his own political ends," *Pacific Standard,* February 26, 2018. https://psmag.com/social-justice/how-trump-weaponized-fake-news-for-his-own-political-ends. (Accessed 16 November 2018.)

Fake News and U.S. Presidential Elections

U.S. intelligence chiefs have alleged Russian interference in the 2016 U.S. presidential elections on multiple occasions. A report from the Director of National Intelligence revealed Russia's role in disseminating fake news through Russian Television and a network of state-sponsored trolls resulted in strong penetration of social media platforms in the US. The report states:

> Russia's state-run propaganda machine—comprised of its domestic media apparatus, outlets targeting global audiences such as RT and Sputnik, and a network of quasi-government trolls—contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences. State-owned Russian media made increasingly favorable comments about President-elect Trump as the 2016 US general and primary election campaigns progressed while consistently offering negative coverage of Secretary Clinton.[114]

A Russia-backed group coordinated its efforts with Kremlin-sponsored mainstream media outlets like RT (formerly *Russia Today*). RT editors also aligned themselves with WikiLeaks, and boasted of their special relationship with WikiLeaks founder, Julian Assange.[115] WikiLeaks was later influential in accessing and leaking emails relate to the Democratic National Committee and Hillary Clinton's campaign.

Russia-backed trolls made liberal use of various social media platforms like Facebook to promote sponsored fake news under the guise of real information. According to an indictment from the current (2018) investigation by Special Counsel Robert Mueller, Russians spent more than $1.25 million every month on Facebook campaigns in

[114] Director of National Intelligence, "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," January 6, 2017: 3. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[115] DNI, "Intelligence Community Assessment."

support of Project Lakhta.[116] The *Washington Post* analyzed some of the Russia-sponsored fake news that became popular during the 2016 U.S. election. Although most of the ads were in fact sponsored, they were designed to look like they originated from authentic U.S. groups or individuals. Majority of the ads were promoted to inflate negative public sentiment against then Democratic candidate, Hillary Clinton.

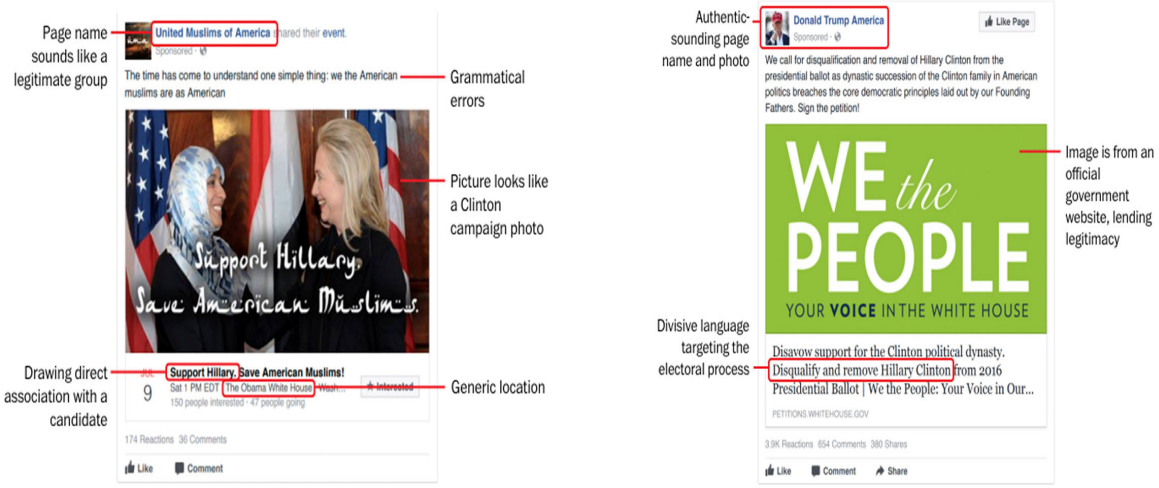


Figure 8. Examples of Fake News on Social Media

Source: Keating et al., 2017.

[116] Charlie Osborne, "Project Lakhta: Russian national charged with US election meddling," *Zero Day*, October 22, 2018. https://www.zdnet.com/article/russian-national-charged-with-us-election-meddling/. (Accessed 16 November 2018.)

During the campaign season, many Americans saw Russia-sponsored free and paid posts directed against Hillary Clinton. Metadata released by U.S. Congressional Democrats offered a glimpse into the Russian fake news machine. A sample of some of the popular posts is shared by the Washington Post.


Figure 9. Fake News

Source: https://www.google.com/search?q=https://www.washingtonpost.com/graphics/+2017/business/russian-ads-facebook-targeting/?utm_term%3D.2f683fc95449&tbm=isch&tbo=u&source=univ&sa=X&ved=2ahUKEwjorsqO8dneAhUM3FMKHeeBD3gQsAR6BAgDEAE&biw=1680&bih=889#imgrc=3RrAaRXl7p_nCM:

According to Facebook, more than 3,000 Facebook ads that were purchased by 470 accounts associated with International Research Agency, a Russian troll farm, have been shut down by the company.[117] Facebook CEO, Mark Zuckerberg, admitted:

> The integrity of our elections is fundamental to democracy around the world. That's why we've built teams dedicated to working on election integrity and preventing governments from interfering in the elections of other nations. And as we've shared before, our teams have found and shut down thousands of fake accounts that could be attempting to influence elections in many countries, including recently in the French elections.[118]

In addition to social media, Russians also made full use of its state-sponsored media network RT. With $190 million in annual funding from the Kremlin, the channel reached 550 million people worldwide.[119] Although the Kremlin denies any involvement in the U.S. presidential election, Robert Mueller's probe into foreign interference is still ongoing and has indicted more than a dozen Russian individuals and firms.

## Fake News and European National Elections

After the 2016 U.S. presidential election, U.S. and European intelligence agencies became concerned about possible Russian meddling in the French and German national elections of 2017. Despite cautionary steps taken by the French security infrastructure, fake news began surfacing against presidential candidate Emmanuel Macron, calling him

---

[117] Dylan Byers, "Facebook says it sold ads to Russian 'troll farm' during 2016 campaign," *CNNMoney,* September 7, 2017. http://money.cnn.com/2017/09/06/media/facebook-russia-ads-2016-election/index.html.

[118] Mark Zuckerberg Facebook post, September 21, 2017. https://www.facebook.com/zuck/posts/10104052907253171.

[119] DNI, "Intelligence Community Assessment."

a supporter of Muslim *sharia* law, alleging that Al-Qaida supported him,[120] and that Macron had a secret fund in an offshore account in the Bahamas.[121] Russian state-sponsored media *Sputnik* reported that the candidate might have been acting in the interests of U.S. financial markets,[122] while other fake news claimed that Macron's campaign was funded by Saudi Arabia.[123] While it might be true that fake news did not have the same impact in the French elections as it did in the U.S. presidential election, Russian efforts to sway the French elections resulted in pre-election opinion polls that divided the far-right candidate Marine La Pen, the left-wing candidate Jean-Luc Melenchon, and the pro-Europe candidate Emmanuel Macron.[124]

In Germany, Europe's most powerful leader, Chancellor Angela Merkel, geared up to confront tactics similar to those faced by the U.S. and French election processes. In 2015, a large number of emails were stolen from her political allies during several hacks by "Cozy Bear," and Merkel was afraid that, during the election period, information might make its way through human and bot-managed fake news.[125] As a preemptive strike on fake news, the German parliament passed a law imposing fines of up to $50

---

[120] Wais Bashir, "Fake News in the French Election," *BBC News*, April 5, 2017. http://www.bbc.com/news/world-europe-39495635.

[121] Eric Maurice, "Fake news takes centre stage in French election," *EU Observer*, May 4, 2014. https://euobserver.com/elections/137781.

[122] "Ex-French Economy Minister Macron Could Be 'US Agent' lobbying banks' interests," *Sputnik*, April 2, 2017. https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/.

[123] *CrossCheck*, "Was Macron's campaign for the French presidency financed by Saudi Arabia?," March 2, 2017. https://crosscheck.firstdraftnews.org/checked-french/macrons-campaign-french-presidency-financed-saudi-arabia/.

[124] David Gilbert, "Russia's fake news machine is now targeting the French election," *VICE News,* April 21, 2017. https://news.vice.com/en_ca/article/paz4vg/russias-fake-news-machine-is-now-targeting-the-french-election.

[125] Patrick Beuth, et al., "Cyberattack on the Bundestag: Merkel and the Fancy Bear," *Zeit Online*, May 12, 2017. http://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia.

million against Facebook and other social media outlets that do not promptly remove "illegal content."[126] Similar to the German Network Enforcement Act,[127] the European Union also took measures to reduce the impact of fake news. Due to upfront aggressive actions by Germany, fake news did not yield similar results in their national elections.

[126] Simon Shuster, "Inside the Next Fake News War," Time, last modified August 9, 2017, http://time.com/4889471/germany-election-russia-fake-news-angela-merkel/.

[127] Jenny Gesley, "Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under "Facebook Act" | Global Legal Monitor," Home | Library of Congress, last modified July 11, 2017, http://www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/.

# Chapter VII

## Analysis

Dov Levin has extensively covered the empirical evidence and traditional methods used by the world's leading powers, the United States and Russia, to interfere in foreign elections. However, his research study only covers up to 2000.[128] Thereafter, actions in cyberspace took over when it came to infrastructure, information sharing, public dialogue, and international relations.

Under international law, meddling by a foreign power with voter counts or voting machines amounts to intervention in the domestic affairs of a state, thus providing the basis for being charged with a violation of the international principles of sovereignty and nonintervention.[129] Cyberspace provides not only potential new domains for state and non-state interaction,[130] but also the possibility of cyber threats against the principles of sovereignty by providing an efficient but opaque mode of possible intervention. Since states frequently engage in peacetime espionage and coercive activities as part of their statecraft, experts are divided between the legality and illegality of such activities[131] when conducted as a one-off campaign. The Tallinn Manual states: "Although peacetime

---

[128] Levin, "Partisan Electoral Interventions."

[129] U.S. Department of State, Office of the Historian, "Monroe Doctrine," 1823. https://history.state.gov/milestones/1801-1829/monroe. Also, Organization of American States (OAS), Charter, Article 3. http://www.oas.org/en/sla/dil/inter_american_treaties_A-41_charter_OAS.asp; and U.N. General Assembly, Resolution A/RES/20/2131.

[130] Raynova. "Toward a Common Understanding, 7.

[131] Darien Pun, "Rethinking espionage in the modern era," *Chicago Journal of International Law* 18, no. 1 (July 2017): 360.

cyber espionage by states does not per se violate international law, the method by which it is carried out might do so."[132]

Cyberspace has dramatically altered global practice of the principles of nonintervention by accelerating an aggressor's efforts and making it difficult to clearly attribute individual actions with a specific state. Before analyzing the legality of current international practice, it is important to understand the legal status of tactics used by major world powers especially in case of Russian practices that sought to influence the 2016 U.S. elections, which is the focus of this thesis.

The birth of the digital age introduced the world to cyber espionage, but it is important to understand that the concept of sovereignty reigns over the cyber infrastructure situated within the geographical boundaries of a State and espionage activities against such infrastructure are considered violation of the State's sovereignty.[133] Tallinn Manual states: "A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[134] Therefore, a State can protect its cyber infrastructure through internal laws and measures. However, if all states are engaging in espionage during peacetime, it is difficult to single out one state's efforts to utilize a particular form of espionage.[135]

When analyzing Russia's intervention in the US and European pre-election processes, it should be understood that Russian actions were not isolated events but were

---

[132] Schmitt, *Tallinn Manual 2.0*, 168.

[133] Schmitt, *Tallinn Manual 2.0*, 11.

[134] Schmitt, *Tallinn Manual 2.0*, 13.

[135] Quincy Wright, *Essays on Espionage and International Law* (Leopold Classic Library, 2015), 21. (Accessed 17 November 2018.)

part of a carefully orchestrated campaign intended to influence the outcomes of the respective processes. Hacking of Democratic National Committee servers (DNC) was cyber espionage undertaken by Russian actors, which some scholars may believe is legal.[136] However, most legal scholars viewed those Russian actions as a violation of U.S. sovereignty—not because cyber espionage is involved, but because the responsible actors were conducted the interference from another state's territory without the knowledge or consent of the target state.[137]

It is also important to note that computer hacking is usually prosecuted under a country's domestic civil or criminal legal structures. Most scholars would consider Russian hacking of the DNC servers as a form of sabotage and therefore be found in violation of the ICJ's ruling in Nicaragua v. United States.[138] Hacking of the DNC servers sought to leak damaging emails with the intent of negatively impacting Hillary Clinton's political campaign.[139] This was not just a standalone action of cyber espionage that mattered in this case; it also brought into perspective the Russian objective of hoping to alter the outcome of the 2016 presidential election through a series of alleged meetings and alleged possible coordination with the Trump campaign.

The Russian also mounted DDoS attacks on the DNC, which were part of the campaign to influence the U.S. elections. Although much of the conversation about the

---

[136] Ohlin, "Russian Cyber Interference." Ohlin noted: "The Russian interference could simply be viewed as an act of espionage, but it has long been understood (at least until recent controversies in human rights law) that spying violates domestic—but not international--law." 1579-1598.

[137] Schmitt, *Tallinn Manual 2.0*, 168.

[138] International Court of Justice, "Military and Paramilitary Activities."

[139] Leonid Bershidsky, "Why some U.S. ex-spies don't buy the Russia story," *Bloomberg.com*, August 10, 2017. https://www.bloomberg.com/view/articles/2017-08-10/why-some-u-s-ex-spies-don-t-buy-the-russia-story.

legality of these DDoS attacks falls under domestic law,[140] the larger and more sinister intent behind the DDoS attacks was to undermine public confidence in the Western democratic process.

Fake news was another tool used by the Russians. Through Facebook and other social media platforms, trolls tried to direct traffic toward websites run by alleged Russian operatives. Fake news, such as a story about Hillary Clinton and other Democrats running a child sex ring at a pizza shop,[141] attempted to sway voter turnout in favor of the Republican nominee, Donald Trump. Research by Hunt Allcott and Matthew Gentzkow showed that fake news tilted heavily in favor of Trump. There were some 115 pro-Trump fake stories shared 30 million times on Facebook, compared to 41 pro-Clinton fake stories shared 7.6 million times,[152] and 38 million Facebook shared stories translated into 760 million user views. Special Counsel Robert Mueller's recent indictment[142] of 13 Russian nationals and three companies corroborates the findings by Allcott and Gentzkow.

As noted earlier, propaganda has been part of state and military operations for centuries.[143] States recognize the role of state-sponsored media in disseminating false

---

[140] Jerry Wegman and Alexander Korzyk, "Internet denial of service attacks: Legal, technical and regulatory issues," *Journal of Legal, Ethical and Regulatory Issues* 7, no. 1/2 (2004): 46-51.

[141] Jason Le Miere. "Hillary Clinton, pedophilia and ankle bracelets: New Trump support conspiracy theory in Pizzagate on steroids," *Newsweek,* Nov. 20, 2017. http://www.newsweek.com/hillary-clinton-conspiracy-theory-trump-717398.

[152] Hunt Allcott and Matthew Gentzkow, "Social media and fake news in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (2017): 211-236.

[142] U.S. Department of Justice, Grand Jury for the District of Columbia, Case 1:18-cr-00032-DLF Document 1, February 16, 2018. https://www.justice.gov/ file/1035477/download. (Accessed 16 November 2018.)

[143] Bryant Wedge, "International Propaganda and Statecraft," *Annals of the American Academy of Political and Social Science* 398, no. 1 (1971).

information that may affect public dialogue. Accelerated global communication through digital media has loosened government controls on communication channels—but this has also provided opportunities for groups or governments to weaponize such channels.[144] U.S. domestic law makes it challenging to effectively combat fake news.[145] However, even with disagreements regarding the extent the U.S. government has pledged to observe global norms while operating in cyberspace, destructive use of information can still violate Article 2(4) of the UN Charter.[146] Analyses of fake news campaigns seeking to alter the outcome of an election is part of a larger effort to benefit an aggressor and demonstrates a clear violation of customary international law and treaties.

Since the alleged Russian intervention in U.S. domestic affairs in 2016, it has proven challenging to clearly attribute the actions of so-called non-state actors with the Russian government. The *Tallinn Manual* states that the actions of non-state actors are attributable to a state if they are either directed by the state or if the state has "effective control" over them.[147] Similarly, the International Law Commission requires direct instructions or influence from a state in order to make attributions of violations to a specific state.[148] Since it is crucial to identify instructions, directions, and control by a

---

[144] Alan Rosenblatt, "Weaponizing social media," *HuffPost*, April 28, 2017 https://www.huffingtonpost.com/entry/weaponizing-social-media_us_58ebad34e4b0145a227cb6f1. See also: Eric Westervelt, "How Russia weaponized social media with 'social bots,'" *NPR.org*, November 5, 2017. https://www.npr.org/2017/11/05/562058208/how-russia-weaponized-social-media-with-social-bots.

[145] U.S. Courts, "U.S. Constitution First Amendment," http://www.uscourts.gov/about-federal-courts/educational-resources/educational-activities/first-amendment-activities. (Accessed May 28, 2018.)

[146] James Mooney, "Weaponizing Information Conference," Yale Law School, February 06, 2017. https://law.yale.edu/yls-today/news/weaponizing-information-conference-watch-panel-videos.

[147] Schmitt, *Tallinn Manual 2.0*, 81.

[148] United Nations International Law Commission (ILC), "Responsibility of States for Internationally Wrongful Acts," 2001, Article 8. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

state regarding violations by non-state actors, the U.S. Department of Justice is diligently collecting evidence of possible coordination or collusion between the Russian government and the Trump campaign. While Mueller conducts his investigation, a declassified version of a classified report prepared by the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA) and the National Security Agency (NSA) claims direct involvement of Russian government in the 2016 U.S. elections.[149]

Traditional international legal norms require a period of deliberation between member of international institutions like ICJ and the UN before deciding on possible judgment or retaliation, which in any case may not apply in cases of cyberspace intervention. Currently, a typical response from a victim state is immediate retaliation without undertaking the proper attribution process. For example, the U.S. retaliated almost immediately when North Korea attacked Sony pictures, and the Obama administration took a number of steps after finding probable Russian interference in the 2016 U.S. elections.[150]

The bar for determining a *bona fide* violation is set very high under current international customary and treaty laws; however, despite deficiencies in the current international legal framework, it remains challenging to reach a consensus among states in a world that is highly polarized. It is therefore recommended that the international community either accepts current practice as part of its framework of customary law, or

[149] Office of the Director of National Intelligence, "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections." January 2017. https://www.dni.gov/files/ documents/ ICA_2017_01.pdf.

[150] Tami Abdollah, "US punishes Russia for hacking presidential campaign," *Boston.com*, December 30, 2016. https://www.boston.com/news/politics/2016/12/29/us-senators-russia-should-be-sanctioned-for-election-hacks.

reconvene to determine a better and more effective legal structure for ensuring global adherence to the principles of nonintervention and state sovereignty.

# Chapter VIII

## Conclusion

Pre-election intervention in a foreign election is a violation of current international treaties, customary international law, and judgments passed by the International Court of Justice. Although both Russia and U.S. have interfered in foreign elections through coercion and espionage since World War II, cyberspace and digital media have become extensions to statecraft for influencing the domestic affairs of a foreign country. Due to today's interconnected world, current practice between countries seems to have outgrown established international law and customs, blurring the boundaries of the principles of sovereignty and nonintervention.

From my discussion of alleged Russian intervention in U.S. elections and other examples of cyber espionage, it is evident that without a means of determining clear attribution, the international legal framework is unable to associate cyber aggression against a state's domestic affairs, and therefore it is unable to provide remedies under the current framework. Pre-electoral intervention by powerful foreign countries is not a new concept, as many entities and nations have tried to extend their strategic goals by influencing political outcomes in other countries.

Cyberspace, especially digital media, has proven to be one of the most prolific and powerful tools for extending the capabilities of states to deploy efficient but obscure efforts to expand their reach. Although cyber espionage and coercion through digital media pose a major challenge when attempting to make direct attribution, similar

challenges have been faced by the traditional methods of espionage and coercion. Levin's outline of foreign intervention activities since World War II[151] (refer back to Figure 1) shows a stark similarity to activities conducted today by major national powers.

The advent of cyberspace introduced the elements of speed and obscurity of execution. While the principles of sovereignty and foreign nonintervention are globally understood and accepted, traditional practices of statecraft that violate these global norms and laws have increased and accelerated. Customary international law and treaties were agreed in the twentieth century with the expectation of coordinating behaviors between states that would observe traditional scenarios. But the introduction of cyberspace, social media, and other digital platforms now demands a second look at today's current legal framework.

More advanced countries have rapidly transitioned their traditional commerce, social infrastructure, and military structures as a result of cyberspace. Deliberate attacks on these platforms can have far-reaching effects on a victim country (e.g., my examples of North Korea's attack on Sony Pictures, the Stuxnet attack on Iranian nuclear sites, Chinese attacks on U.S. commercial infrastructure, and the 2016 Russian attacks on DNC servers). The current laws governing clear attribution must be revisited in order to comply with the U.N. Charter that has set a high bar for identifying a threat and its potential remedy. For now, customary international law is proving to be insufficient, leaving much to a state's interpretation which in turn may result in global disorder.

Finally, it is important to reiterate that every nation has a responsibility to protect its citizens and to ensure that national elections are fair and unaffected by overt or covert interventions from foreign elements. But with the introduction of cloud-based digital

[151] Levin, "When the Great Power Get a Vote," 189-202.

platforms, citizens can become part of a network that exists outside the geographic boundaries of a state. The introduction of barriers to free speech or attempts to control the flow of information by regulating cyberspace in some defined geographic boundary may adversely affect existing international treaties and customary international laws of free speech and freedom of information, thereby proving counterproductive and compromising trust.

References


Abdollah, Tami. “US Punishes Russia for Hacking Presidential Campaign.” *Boston.com.* https://www.boston.com/news/politics/2016/12/29/us-senators-russia-should-be-sanctioned-for-election-hacks.

Allcott, Hunt, and Matthew Gentzkow. “Social Media and Fake News in the 2016 Election.” *Journal of Economic Perspectives* 31, no. 2 (2017): 211-236.

Auchard, Eric. “Macron campaign was target of cyber attacks by spy-linked group.” *Reuters World News*. April 24, 2017. https://www.reuters.com/article/us-france-election-macron-cyber/macron-campaign-was-target-of-cyber-attacks-by-spy-linked-group-idUSKBN17Q200.

Baheri, Zahra, and Ali S. Fard. “Status of espionage from the perspective of international laws with emphasis on countries’ diplomatic and consular relations.” *Journal of Scientific Research and Development* 2, no. 1 (2015): 41-45.

Bashir, Wais. “Fake News in the French Election.” *BBC News.* http://www.bbc.com/news/world-europe-39495635.

BBC News. “How the US Spy Scandal Unravelled.” http://www.bbc.com/news/world-us-canada-23123964.

Bershidsky, Leonid. “Why Some U.S. Ex-Spies Don’t Buy the Russia Story.” *Bloomberg.com*. https://www.bloomberg.com/view/articles/2017-08-10/why-some-u-s-ex-spies-don-t-buy-the-russia-story.

Beuth, Patrick, Kai Biermann, Martin Klingst, and Holger Stark. “Cyberattack on the Bundestag: Merkel and the Fancy Bear.” *Zeit Online*. http://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia.

Boon, Kristin E. “Are Control Tests Fit for the Future? The Slippage Problem in Attribution Doctrines.” *Melbourne Journal of International Law* 15, no. 2 (2014).

Brown, Heather, Emily Guskin, and Amy Mitchell. “The Role of Social Media in the Arab Uprisings.” Pew Research Center, November 28, 2012. http://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/.

Byers, Dylan. “Facebook Says It Sold Ads to Russian ‘troll Farm’ During 2016 Campaign.” *CNNMoney*. http://money.cnn.com/2017/09/06/media/facebook-russia-ads-2016-election/index.html.

Clinton, Hillary Rodham. *What Happened*. New York: Simon & Schuster, 2018.

Crandall, Russell. *Gunboat Democracy: U.S. Interventions in the Dominican Republic, Grenada, and Panama*. Lanham, MD: Rowman & Littlefield, 2006.

CrossCheck. “Was Macron’s Campaign for the French Presidency Financed by Saudi Arabia?” https://crosscheck.firstdraftnews.org/checked-french/macrons-campaign-french-presidency-financed-saudi-arabia/.

Crowley, Michael. “Trump Urges Russia to Hack Clinton’s Email.” *Politico*. https://www.politico.com/story/2016/07/trump-putin-no-relationship-226282.

Cukier, Michael. “Study: Hackers attack every 39 seconds.” February 9, 2007. University of Maryland. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (Accessed 16 November 2018.)

Czosseck, Christian, and Kenneth Geers. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, 2009.

D’Amato, Anthony. “New Approaches to Customary International Law.” *American Journal of International Law* 105, no. 2 (January 2011): 163-167.

“Data Breach Reports: Identity Theft Resource Center.” ID Theft Resource Center. http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

Deeks, Ashley. “The Increasing State Practice and Opinio Juris on Spying.” *Lawfare Blog*. https://www.lawfareblog.com/increasing-state-practice-and-opinio-juris-spying.

Deutsche Welle. “Germany Admits Hackers Infiltrated Federal Ministries, Russian Group Suspected.” http://www.dw.com/en/germany-admits-hackers-infiltrated-federal-ministries-russian-group-suspected/a-42775517.

Einav, Yohai. “The (DDoS) Attack on French Media. Akamai Security Intelligence and Threat Research Blog. *Intelligent Platform*, Spring 2018 https://www.nominum.com/ tech-blog/ddos-attack-french-media/.

Eisenhower, Dwight D. Quoted in: Central Intelligence Agency, “Our first line of defense: Presidential reflections on U.S. intelligence.” https://www.cia.gov/library/ center-for-the-study-of-intelligence/csi-publications/books-and-monographs/our-first-line-of-defense-presidential-reflections-on-us-intelligence/eisenhower.html. (Accessed May 31, 2018.)

Eisenstadt, Michael, Michael Knights, and Ahmed Ali. “Iran’s Influence in Iraq.” Washington Institute for Near East Policy. http://www.washingtoninstitute.org/policy-analysis/view/irans-influence-in-iraq-countering-tehrans-whole-of-government-approach.

“Ex-French Economy Minister Macron Could Be ‘US Agent’ Lobbying Banks’ Interests.” *Sputnik News*. https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/.

Fakhoury, Rania. “Can Social Media, Loud and Inclusive, Fix World Politics?” *The Conversation*. https://theconversation.com/can-social-media-loud-and-inclusive-fix-world-politics-74287.

Farer, Tom J. “Political and Economic Coercion in Contemporary International Law.” *American Journal of International Law* 79, no. 2 (1985): 405-413.

Federal Trade Commission. “Phishing.” https://www.consumer.ftc.gov/articles/0003-phishing.

Franco, Chiara. Report of the International Conference on Coercive Diplomacy, Sanctions and International Law. Istituto Affari Internazionali (IAI). Rome. 13 February 2015. http://www.iai.it/sites/default/files/iai1505.pdf. (Accessed 15 November 2018.)

Gesley, Jenny. “Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under “Facebook Act.” *Global Legal Monitor*. http://www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/.

Gilbert, David. “Russia’s Fake News Machine is Now Targeting the French Election.” *VICE News*. https://news.vice.com/en_ca/article/paz4vg/russias-fake-news-machine-is-now-targeting-the-french-election.

Goodrich, Leland M. “From League of Nations to United Nations.” *International Organization* 1, no. 01 (1947): 3-21.

Gordon, Lansing. *Rise of the Cybergens*. NJ: Bookbaby, 2015.

Graves, Lucia. “How Trump Weaponized ‘Fake News’ for His Own Political Ends.” *Pacific Standard Magazine*. https://psmag.com/social-justice/how-trump-weaponized-fake-news-for-his-own-political-ends.

Greenhill, Kelly M., and Robert J. Krause. *Coercion: The Power to Hurt in International Politics*. Oxford: Oxford University Press, 2018.

Greenwood, Shannon, Andrew Perrin, and Maeve Duggan. "Social Media Update 2016." Pew Research Center: Internet, Science & Tech. http://www.pewinternet.org/ 2016/11/11/ social-media-update-2016/.

Grewal, David Singh. "The Domestic Analogy Revisited: Hobbes on International Order." *Yale Law Journal* 125, no. 3 (January 2016): 560-795. Accessed 14 November 2018.

Guzmán, Andrew T. *How International Law Works: A Rational Choice Theory*. New York: Oxford University Press, 2010.

Hadnagy, Christopher, and Paul Wilson. *Social Engineering: The Art of Human Hacking*. Hoboken, N.J.: Wiley, 2013.

(The) Hague Convention of 1907. "Convention Respecting the Laws and Customs of War on Land," Article 3, 1910. Library of Congress. http://www.loc.gov/law/ help/us-treaties/bevans/m-ust000001-0631.pdf.

Handeyside, Hugh. "The Lotus Principle in ICJ Jurisprudence: Was the Ship Ever Afloat?" *Michigan Journal of International Law* 29, no. 1 (2007), 71-94. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1145&context=mjil.

Herman, Edward S., Noam Chomsky, and John Pruden. *Manufacturing Consent: The Political Economy of the Mass Media*. Old Saybrook, CT: Tantor Audio Recorded Books, 2017.

Hilleary, Cecily. "Ukraine's Social Media Revolution Years in the Making." VOA. https://www.voanews.com/a/ukraines-protest-movement-fueled-by-social-media/1871457.html.

Hosenball, Mark. "U.S. Increasingly Convinced That Russia Hacked French Election." https://www.reuters.com/article/us-france-election-russia/u-s-increasingly-convinced-that-russia-hacked-french-election-sources-idUSKBN1852KO.

Hutt, Rosamond. "The World's Most Popular Social Networks, Mapped." World Economic Forum. https://www.weforum.org/agenda/2017/03/most-popular-social-networks-mapped/.

Identity Theft Resource Center (ITRC). "Data Breach Reports." December 29, 2015. http://www.idtheftcenter.org/images/breach/DataBreachReports_201. (Accessed 16 November 2018.)

International Coalition for the Responsibility to Protect (ICRtoP). Chapter 2, Sec. 2: 8, 12. http://responsibilitytoprotect.org/ICISS%20Report.pdf.

International Court of Justice. “Case Concerning Military And Paramilitary Activities In And Against Nicaragua.” http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

International Court of Justice. “Military and Paramilitary Activities in and Against Nicaragua.” Nicaragua v. United States of America. *I.C.J. Reports,* 1986. http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf. (Accessed 15 November 2018.)

Jackamo, Thomas. “From the Cold War to the new multilateral world order: The evolution of covert operations and the customary international law of non-intervention.” *Virginia Journal of International Law* 32, no. 4 (1992), 929-977.

Jackson, John H. “Sovereignty—Modern: A New Approach to an Outdated Concept.” *Georgetown Law Faculty Publications and Other Works* (2003), 110. https://scholarship.law.georgetown.edu/facpub/110. (Accessed 17 November 2018.)

Jared, Beim. “Enforcing a Prohibition on International Espionage.” *Chicago Journal of International Law* 18, no. 2 (2018), 647-672.

Jeyanthi, N., and R. Thandeeswaran. *Security Breaches and Threat Prevention in the Internet of Things*. Hershey, PA: IGI Global, 2017.

Keating, Dan, Kevin Shaul, and Leslie Shapiro. “The Facebook Ads Russians Showed to Different Groups.” *Washington Post.* https://www.washingtonpost.com/graphics/2017/business/russian-ads-facebook-targeting/?utm_term=.2f683fc95449.

Kelley, Michael B. “The Stuxnet attack on Iran’s nuclear plant was far more dangerous than previously thought.” *Business Insider*. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

Kisatsky, Deborah. *The United States and the European Right, 1945-1955*. Columbus: Ohio State University Press, 2005.

Kislenko, Arne. “A not so silent partner: Thailand’s role in covert operations, counter insurgency, and the wars in Indochina.” *Journal of Conflict Studies* 24, no. 1 (Summer 2004): 189-202.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. “Lessons from Russia's Operations in Crimea and Eastern Ukraine.” Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1498.html (Accessed 17 November 2018.)

Kohen, Marcelo. "The Principle of Non-Intervention 25 Years after the Nicaragua Judgment." *Leiden Journal of International Law* 25, no. 01 (2012), 157-164.

Kolb, Robert. "Attribution." *The International Law of State Responsibility: An Introduction.* 2017: 70-108. https://doi-org.ezp-prod1.hul.harvard.edu/10.4337/9781786434715.00008.

Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press, 2001.

Lamont, James, and Prateek Pradhan. "Nepal Hits Back at Foreign Intervention." *Financial Times*. May 16, 2010. https://www.ft.com/content/2c2ee906-610a-11df-9bf0-00144feab49a.

Landau, Susan. *Listening in: Cybersecurity in an insecure age*. New Haven, CT: Yale University Press, 2017.

Le Miere, Jason. "Hillary Clinton, pedophilia and ankle bracelets: New Trump-supporter conspiracy theory is Pizzagate on steroids." *Newsweek.* http://www.newsweek.com/hillary-clinton-conspiracy-theory-trump-717398.

Levin, Dov H. "Partisan electoral interventions by the great powers: Introducing the PEIG Dataset," *SAGE Journals.* September 9, 2016. https://journals.sagepub.com/doi/abs/10.1177/0738894216661190 (Accessed 15 November 2018.)

Levin, Dov H. "When the Great Power gets a vote: The effects of Great Power electoral interventions on election results." *International Studies Quarterly* 60, no. 2 (2016): 189-202.

Maldre, Patrik. "The Russian Cyber Threat: Views from Estonia." Center for European Policy Analysis, May 18, 2016. https://cepa.ecms.pl/The-Russian-Cyber-Threat-Views-from-Estonia.

Mattessich, William. "Digital destruction: Applying the principle of non-intervention to distributed denial of service attacks manifesting no physical damage." *Columbia Journal of Transitional Law* 54, no. 3 (September 4, 2016): 873-896.

Maurice, Eric. "Fake News Takes Centre Stage in French Election." *EUObserver*. https://euobserver.com/elections/137781.

Mhiripiri, Nhamo A., and Tendai Chari. *Media Law, Ethics, and Policy in the Digital Age*. Hershey, PA: IGI Global, 2017.

Modderkolk, Huib. “Dutch agencies provide crucial intel about Russia’s interference in US-elections.” *de Volkskrant*. January 25, 2018. https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/.

Mooney, James. “Weaponizing Information Conference: Watch Panel Videos and Read Summaries.” Yale Law School. February 5, 2017. https://law.yale.edu/yls-today/news/weaponizing-information-conference-watch-panel-videos.

Morris, David Z. “How Hackers Make Money from DDoS Attacks.” *Fortune*. October 22, 2016. http://fortune.com/2016/10/22/ddos-attack-hacker-profit/.

Nathan, James A. *Soldiers, Statecraft, and History: Coercive Diplomacy and International Order*. NY: Praeger, 2002.

National Security Act of 1947. House Office of the Legislative Counsel. https://legcounsel.house.gov/Comps/National%20Security%20Act%20Of%201947.pdf.

Nixon, Allison, John Costello, and Robbie Tokazowski. “Flashpoint Monitoring of Mirai Shows Attempted DDoS of Trump and Clinton Websites.” *Flashpoint*. https://www.flashpoint-intel.com/blog/trending/attempted-ddos-trump-and-clinton-websites/.

O’Neill, Daniel P. “When to Intervene: The Haitian Dilemma.” *SAIS Review* 24, no. 2 (2004), 163-174.

O’Toole, Gavin. *Politics Latin America*. Pearson, 2018.

Office of the Director of National Intelligence. “Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections.” https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Ohlin, Jens D. “Did Russian cyber interference in the 2016 election violate international law? *Texas Law Review* 95, no. 7 (2017), 1579-1598. https://ssrn.com/abstract=2934321. (Accessed 16 November 2018.)

Organization of American States (OAS), Charter, Article 3. http://www.oas.org/en/sla/dil/inter_american_treaties_A-41_charter_OAS.asp

Orwell, George. *1984*. (1949). Boston: Houghton Mifflin Harcourt, 2016.

Payne, Stanley G. *The Spanish Civil War*. Cambridge: Cambridge University Press, 2012.

Pew Research Center. "Social Media Fact Sheet." Survey conducted Sept. 29 – Nov. 6, 2016. http://www.pewinternet.org/fact-sheet/social-media/. (Accessed 15 November 2018.)

Porotsky, Richard D. "Economic coercion and the General Assembly: A post-Cold War assessment of the legality and utility of the thirty-five-year old embargo against Cuba." *Vanderbilt Journal of Transitional Law* 28, no. 4 (1995), 901-957.

Poushter, Jacob. "Not everyone in advanced economies is using social media." Pew Research Center. April 20, 2017. http://www.pewresearch.org/fact-tank/2017/04/20/not-everyone-in-advanced-economies-is-using-social-media/.

PriceWaterhouse Coopers. "Toward new possibilities in threat management: How businesses are embracing a modern approach to threat management and information sharing." 2017/ https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf.

Pun, Darien. "Rethinking Espionage in the Modern Era." *Chicago Journal of International Law* 18, no. 1 (July 2017), 353-391.

Raynova, Denista. "Toward a common understanding of the nonintervention principle." *European Leadership Network*. October 2017. https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/170929-ELN-Workshop-Report-Non-Intervention.pdf.

"The Real Story of 'Fake News.'" Merriam-Webster Dictionary. https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news. (Accessed May 28, 2018.)

Richardson, Glenn W. *Social Media and Politics: A New Way to Participate in the Political Process*. Santa Barbara: Praeger, 2017.

Roberts, Hal, and Bruce Etling. "Coordinated DDoS attack during Russian Duma elections." Weblogs at Harvard. December 8, 2011. http://blogs.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/.

Rosenblatt, Alan. "Weaponizing Social Media." *HuffPost*. https://www.huffingtonpost.com/entry/weaponizing-social-media_us_58ebad34e4b0145a227cb6f1.

Rushkoff, David. *Coercion: Why We Listen to What "They" Say?* New York: Riverhead, 2000.

Sanger, David, David Kirkpatrick, and Nicole Perlroth. “The world once laughed at North Korean cyberpower. No more.” *New York Times*. October 15, 2017. https://www.nytimes.com/ 2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

Schlütter, Birgit. *Developments in Customary International Law Theory and the Practice of the International Court of Justice and the International Ad Hoc Criminal Tribunals for Rwanda and Yugoslavia.* Dordrecht, Netherlands: Brill, 2010.

Schmitt, Michael N. (Ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. Accessed 17 November 2018.

Sciutto, Jim. “How one typo helped let Russian hackers in.” *CNN.* June 27, 2017. https://www.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html.

Shapiro, Leslie. “Anatomy of a Russian Facebook ad.” *Washington Post*. November 1, 2017. https://www.washingtonpost.com/graphics/2017/business/russian-ads-facebook-anatomy/?utm_term=.68f14866e364. Accessed 17 November 2018.

Sharf, Michael P. “Accelerated Formation of Customary International Law.” *ILSA Journal of International and Comparative Law* 20, no. 2 (Spring 2014): 309.

Shuster, Simon. “Russia has launched a fake news war on Europe. Now Germany is fighting back.” *Time*. August 9, 2017. http://time.com/4889471/germany-election-russia-fake-news-angela-merkel/. Accessed 14 November 2018.

St. J. Macdonald, R. “Book Review: The World Court. What it is and how it works.” *International Journal* 18, no. 4 (December 1963): 549-50. Accessed 14 November 2018.

Stewart, James. “Facebook has 50 Minutes of your time each day. It wants more.” *New York Times*. May 6, 2016. https://www.nytimes.com/2016/05/06/business/ facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html.

Swanson, Steven R. “Forcing Facebook on foreign dictators: A Violation of international law.” *Tennessee Law Review* 79, no. 4 (2012): 851-937.

Terry, Patrick. “‘Absolute Friends’: United States espionage against Germany and public international law.” *Revue québécoise de droit international* 28, no. 2 (2015): 173-203.

Thomas, Joseph. “Confirmed US meddling in Thailand’s upcoming elections.” Centre for Research on Globalization. February 22, 2018. https://www.globalresearch.ca/ confirmed-us-meddling-in-thailands-upcoming-elections/5629887. Accessed 17 November 2018.

United Nations General Assembly. “International Law Commission, Articles on State Responsibility.” https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility.

United Nations General Assembly. A/RES/20/2131. “Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty.” http://www.un-documents.net/a20r2131.htm. Accessed 14 November 2018.

United Nations General Assembly. A/RES/47/130. **“**Recognizing that the principles of national sovereignty and non-interference in the internal affairs of any State should be respected in the holding of elections.” 1992. http://www.un.org/documents/ga/res/47/ a47r130.htm.

United Nations International Law Commission. “Responsibility of States for Internationally Wrongful Acts.” Office of Legal Affairs. http://legal.un.org/ilc/texts/ instruments/english/commentaries/9_6_2001.pdf.

United Nations Office at Geneva (UNOG). “History of the League of Nations (1919-1946).” https://www.unog.ch/80256EDD006B8954/(httpAssets)/ 36BC4F83BD9E4443C1257AF3004FC0AE/$file/Historical_overview_of_the_League_ of_Nations.pdf. (Accessed May 28, 2018.)

United Nations. Charter. “Welcome to the United Nations.” Chapter I. http://www.un.org/en/sections/un-charter/chapter-i/index.html.

United Nations. Charter. “Welcome to the United Nations.” Chapter VII. http://www.un.org/en/sections/un-charter/chapter-vii/.

United Nations. Charter. “Welcome to the United Nations.” Chapter XXXIX. http://www.un.org/en/sections/un-charter/chapter-xxxix/.

U.S. Computer Emergency Readiness Team (US-CERT). “Avoiding Social Engineering and Phishing Attacks.” https://www.us-cert.gov/ncas/tips/ST04-014.

U.S. Courts. “U.S. Constitution, First Amendment.” http://www.uscourts.gov/ about-federal-courts/educational-resources/educational-activities/first-amendment-activities.

U.S. Courts. Constitution of the United States. First Amendment. http://www.uscourts.gov/about-federal-courts/educational-resources/educational-activities/first-amendment-activities. Accessed May 28, 2018.

U.S. Courts. New York Times v. Sullivan. Podcast. http://www.uscourts.gov/about-federal-courts/educational-resources/supreme-court-landmarks/new-york-times-v-sullivan-podcast.

U.S. Department of Justice. Grand Jury for the District of Columbia. Charges: Case 1:18-cr-00032-DLF Document 1. Filed February 16, 2018. https://www.justice.gov/file/1035477/download. (Accessed 16 November 2018.)

U.S. Department of State. Office of the Historian. "Monroe Doctrine," 1823. https://history.state.gov/milestones/1801-1829/monroe.

U.S. Department of State. Office of the Historian. Monroe Doctrine. 1823. https://history.state.gov/milestones/1801-1829/monroe.

Van der Linden, Harry. Digital Commons @ Butler University. https://digitalcommons.butler.edu/cgi/viewcontent.cgi?article=1041&context=facsch_papers.

"Verisign Q2 2016 DDoS Trends: Layer 7 DDoS Attacks a Growing Trend." Verisign Blog. 2016. https://blog.verisign.com/security/verisign-q2-2016-ddos-trends-layer-7-ddos-attacks-a-growing-trend/.

Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations. "Preamble." March 21, 1986. http://legal.un.org/ilc/texts/instruments/english/conventions/1_2_1986.pdf

Vis, Farida. "The Rapid Spread of Misinformation." World Economic Forum. http://reports.weforum.org/outlook-14/wp-content/blogs.dir/30/mp/files/pages/files/trend-10.pdf.

Wedge, Bryant. "International Propaganda and Statecraft." *Annals of the American Academy of Political and Social Science* 398, no. 1 (1971): 36-43.

Wegman, Jerry, and Alexander Korzyk. "Internet Denial of Service Attacks: Legal, Technical And Regulatory Issues." *Journal of Legal, Ethical and Regulatory Issues* 7, no. 1/2 (2004): 43-59.

Westervelt, Eric. "How Russia weaponized social media with 'social bots'." NPR.org. November 5, 2017. https://www.npr.org/2017/11/05/562058208/how-russia-weaponized-social-media-with-social-bots.

Whitehead, Laurence. *The International Dimensions of Democratization Europe and the Americas*. Oxford: Oxford University Press, 2004.

Williams-Grut, Oscar. "Report: Russia Hacked UK Energy Companies on Election Day." *Business Insider*. http://www.businessinsider.com/russia-hacked-uk-energy-companies-election-day-2017-7?r=UK&IR=T.

Windrem, Robert. “Timeline: Ten years of Russian cyber attacks on other countries.” NBC News. https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

Wood, Michael. “Second Report on Identification of Customary International Law.” United Nations. May 22, 2014. http://dag.un.org/handle/11176/307174. Accessed 17 November 2018.

Wright, Quincy. *Essays on Espionage and International Law*. Leopold Classic Library, 2015.

Zetter, Kim. “An unprecedented look at Stuxnet, the world’s first digital weapon.” *Wired*, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zuckerberg, Mark. Facebook, September 21, 2017. https://www.facebook.com/zuck/posts/10104052907253171.

Zunes, Stephen. “The US Invasion of Grenada.” *Global Policy*. October 25, 2003. https://www.globalpolicy.org/component/content/article/155/25966.html.