HACKING THE ELECTORATE: A NON-INTERVENTION VIOLATION MAYBE, BUT NOT AN "ACT OF WAR"

Christopher T. Stein*

TABLE OF CONTENTS

* Major Christopher T. Stein (B.A., University of California, Los Angeles (2005); J.D., William S. Boyd School of Law (2008); LL.M., The United States Army Judge Advocate General's Legal Center & School (2018)) is an active duty United States Air Force Judge Advocate. He has served a variety of assignments both stateside and overseas, most recently as Staff Judge Advocate for the 8th Fighter Wing, Kunsan Air Base, Republic of Korea. The views expressed are his own and do not necessarily represent the views of the U.S. Air Force or Department of Defense.

What's the most resilient parasite? A bacteria? A virus? An intestinal worm? An idea. Resilient, highly contagious. Once an idea's taken hold in the brain it's almost impossible to eradicate.[1]

I. INTRODUCTION

Since voting machines went electronic, voters have worried elections would be hacked.[2] The media sensationalizes the ease with which electronic voting machines can be manipulated.[3] The U.S. government continually seeks to enhance the cybersecurity of its electronic election infrastructure.[4] To ensure their systems cannot be hacked, some U.S. states are even considering abandoning electronic voting technology altogether.[5] Electronic systems present a vulnerability, but the reality is, hacking systems can be difficult to do and even more difficult to conceal. Far neater is "hacking people"—getting voters to change their views without realizing they are doing so.[6]

While we fretted about a cyberattack on our machines, we missed the information attack on our minds. Russian hackers may or may not have successfully hacked American election systems, but they certainly hacked the electorate. Leading up to the 2016 U.S. presidential election, Russia orchestrated a sophisticated influence campaign, blending covert cyber intelligence operations with overt media operations.[7] Particularly innovative was Russia's leveraging of

---

[1] Christopher J. Nolan, INCEPTION: THE SHOOTING SCRIPT 2 (2010).

[2] *See* Brian Barrett, *America's Electronic Voting Machines are Scarily Easy Targets*, WIRED, Aug. 2, 2016, https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

[3] Ben Wofford, *How to Hack an Election in 7 Minutes*, POLITICO MAGAZINE, (Aug. 5, 2016) , https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.

[4] *See* DEP'T OF HOMELAND SEC., STATEMENT BY SECRETARY JEH JOHNSON ON THE DESIGNATION OF ELECTION INFRASTRUCTURE AS A CRITICAL INFRASTRUCTURE SUBSECTOR (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical (designating "election infrastructure" as "critical infrastructure" for asset prioritization purposes).

[5] Elizabeth Weise, *Paper Ballots are Back in Vogue Thanks to Russian Hacking Fears*, USA TODAY, Sept. 19, 2017, https://www.usatoday.com/story/tech/news/2017/09/19/russia-hacking-election-fears-prompts-states-to-switch-to-paper-ballots/666020001/.

[6] Molly K. McKew, *Forget Comey. The Real Story is Russia's War on America*, POLITICO, June 11, 2017, http://www.politico.com/magazine/story/2017/06/11/forget-comey-the-real-story-is-russias-war-on-america-215245.

[7] OFF. OF THE DIR. OF NAT'L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS 2 (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

social media capabilities to sway public opinion.[8] Now, American politicians—from sitting Senators, to a former Vice President, to the U.S. Ambassador to the United Nations—are decrying Russia's election meddling as an "act of war."[9]

This paper evaluates the legal implications of cyber-enabled information operations designed to influence an electorate. This is important to consider with respect to Russia's involvement in the 2016 election, because it implicates the United States' options in defense and its available remedies under international law. Furthermore, the standard by which we judge Russia today and the assertions we make about the international law related to cyber-enabled information operations will shape state approaches to such operations in the future. Part II describes Russian information operations during the 2016 U.S. presidential election. For the purposes of this paper, complex issues relating to attribution in cyber operations are ignored. The conclusions of the U.S. Intelligence Community and reports of reputable media organizations are accepted as true. Part III discusses cyber-enabled information operations in general and their significant rise in importance during the 21st century. Part IV explores the international law relating to the use of force and assesses whether Russia's operations specifically, and cyber-enabled information operations in general, could constitute a use of force. Finally, Part V assesses the same operations in light of the principle of non-intervention in the internal affairs of a state. Ultimately, this paper concludes that hacking the electorate through cyber-enabled information operations could violate the principle of non-intervention but does not constitute a use of force.

I. RUSSIAN INFORMATION OPERATIONS DURING THE 2016 U.S. PRESIDENTIAL ELECTION

In February 2017, Russia's Defense Minister revealed Russia had established an information operations force to bolster propaganda efforts.[10] However, The United States did not need this formal announcement to realize that Russia had "developed a sophisticated capability to influence the American political process."[11] The U.S. Intelligence Community had already concluded Russian

---

[8] JAMES M. LUDES & MARK R. JACOBSON, PELL CTR. FOR INT'L REL. & PUB. POL'Y, SHATTER THE HOUSE OF MIRRORS: A CONFERENCE REPORT ON RUSSIAN INFLUENCE OPERATIONS 5 (2017).

[9] Petra Cahill, *Dick Cheney: Russian Election Interference Possibly 'Act of War'*, NBC NEWS (Mar. 28, 2017), https://www.nbcnews.com/politics/white-house/dick-cheney-russian-election-interference-could-be-seen-act-war-n739391; John Haltiwanger, *Russia Committed Act of War with Election Interference, Nikki Haley Says*, NEWSWEEK (Oct. 19, 2017), http://www.newsweek.com/russia-committed-act-war-election-interference-nikki-haley-says-688518; Louis Nelson, *Cardin: Russia's Election Meddling is 'an Act of War'*, POLITICO (Nov. 1, 2017), https://www.politico.com/story/2017/11/01/russia-meddling-us-elections-ndi-event-244414.

[10] Ed Adamcyzk, *Russia Has a Cyber Army, Defense Ministry Acknowledges*, UPI (Feb. 23, 2017), http://tass.com/defense/932439.

[11] LUDES & JACOBSON, *supra* note 8, at 8.

President Vladimir Putin ordered an influence campaign in the 2016 presidential election.[12] The goals of this campaign were to undermine public faith in the democratic process, and harm the electoral chances and potential presidency of one of the candidates—Secretary Hillary Clinton.[13]

The investigation into, and effort to define the scope of, Russian operations continues. At a general level, it is clear that Russian information operations followed a three-pronged effort to: (1) hack the accounts of high-level officials and selectively disclose embarrassing information; (2) compromise state and local voter registration systems; and (3) disseminate propaganda and disinformation in the media.[14] Russian intelligence services collected information against political campaigns, think tanks, and lobbying groups, including gaining access to Democratic National Committee (DNC) networks.[15] After collecting this sensitive information, they leaked it to organizations, such as WikiLeaks, to push into the mainstream media.[16] Additionally, while there is no indication Russia changed vote counts, they were able to tamper with local election systems to create confusion on election day and cast doubt upon the legitimacy of the election results.[17] Perhaps most impactful was Russia's sophisticated influence operations on social media. Leveraging the significant information effect of these combined actions, Russia was able to undermine faith in the American democratic system for less than a "quarter the cost of building an F-35 jet."[18]

During the election, Facebook detected coordinated activity by inauthentic accounts manipulating political discussion, including the promotion and denigration of specific causes, sowing distrust in political institutions, and spreading confusion.[19] Russia used social media to spread hoaxes and conspiracies

---

[12] OFF. OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 7, at 1.

[13] *Id.*

[14] *Id.* at 2-4; *see also* Jack Corrigan, *Social Media is "First Tool" of 21st-Century Warfare, US Lawmaker Says*, DEFENSE ONE (Sept. 29, 2017), http://www.defenseone.com/technology/2017/09/social-media-first-tool-21st-century-warfare-lawmaker-says/141392/ (reporting that the Vice Chair of the Senate Intelligence Committee stated Russia hacked political parties, attacked voter registration systems, and used paid advertising and fake accounts on social media to disseminate misinformation).

[15] OFF. OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 7, at 2.

[16] *Id.* at 3. *See also* David E. Sanger & Charlie Savage, *U.S. Accuses Russia of Directing Hacks to Influence the Election*, N.Y. TIMES (Oct. 7, 2016), https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html, at A1.

[17] Nicole Perlroth, Michael Wines & Matthew Rosenberg, *Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny*, N.Y. TIMES (Sept. 1, 2017), https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

[18] Corrigan, *supra* note 14, (quoting Senator Mark Warner (D-VA), Vice Chair of the Senate Intelligence Committee, which is investigating Russian actions during the 2016 election).

[19] Jen Weedon et al., *Information Operations and Facebook*, FACEBOOK, (Apr. 27, 2017), https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

such as the assertions that Secretary Clinton had Parkinson's Disease, Pope Francis endorsed Trump, and that Clinton and her aides were running a pedophile ring in the basement of a pizza parlor ("Pizzagate").[20] The vast majority of inauthentic activity did not specifically reference the election, but rather amplified divisive social and political messages across the ideological spectrum.[21] This use of social media exploited a vulnerability because, while Facebook was prepared to defend against traditional cyberattacks, it failed to prepare for the use of its platform in a massive disinformation campaign.[22]

Twitter may have been used even more extensively than Facebook for "large-scale automated messaging, using 'bot' accounts to spread false stories and promote news articles."[23] A Twitter bot is a program that automatically posts or shares messages.[24] During the 2016 election, bots circulated links to conspiracy sites, promoted Secretary Clinton's email scandal[25] and role in the Benghazi tragedy,[26] and filled Twitter with pro-Trump hashtags.[27] They may have engaged in voter suppression efforts, such as encouraging Clinton supporters to vote online, by phone, or by text.[28] One study found an estimated 400,000 bots operating on Twitter, generating nearly 20% of all election-related messages.[29] These bots

---

[20] Massimo Calabresi, *Inside Russia's Social Media War on America*, TIME (May 18, 2017, 3:48 PM), http://time.com/4783932/inside-russia-social-media-war-america.

[21] Alex Stamos, *An Update on Information Operations on Facebook*, FACEBOOK (Sept. 6, 2017), https://newsroom.fb.com/news/2017/09/information-operations-update.

[22] Adam Entous, et al., *Obama Tried to Give Zuckerberg a Wake-up Call Over Fake News on Facebook*, WASH. POST (Sept. 24, 2017), https://www.washingtonpost.com/business/economy/obama-tried-to-give-zuckerberg-a-wake-up-call-over-fake-news-on-facebook/.

[23] Daisuke Wakabayashi & Scott Shane, *Twitter Seen as Key Battlefield in Russian Influence Campaign: [National Desk]*, N.Y. TIMES (Sept. 28, 2017), at A1.

[24] Caitlin Dewey, *One in Four Debate Tweets Comes from a Bot. Here's How to Spot Them*, WASH. POST (Oct. 19, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/10/19/one-in-four-debate-tweets-comes-from-a-bot-heres-how-to-spot-them.

[25] Michael S. Schmidt, *Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules*, N.Y. TIMES (Mar. 2, 2015), https://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html (discussing Secretary Clinton's use of personal email account to conduct official business).

[26] Elizabeth Chuck, *Benghazi 101: What You Need to Know Ahead of Clinton's Testimony*, NBC NEWS (Oct. 22, 2015, 12:45 AM), https://www.nbcnews.com/news/world/benghazi-101-what-you-need-know-ahead-clintons-testimony-n447996 (discussing the attack on the U.S. diplomatic compound in Benghazi, Libya, ahead of Sec. Clinton's testimony before Republican-led House committee).

[27] Dewey, *supra* note 24.

[28] *Social Media Influence in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 23 (2017) (statement of Sean J. Edgett, Acting Gen. Counsel of Twitter).

[29] Nanette Byrnes, *How the Bot-y Politic Influenced This Election*, MIT TECH. REV. (Nov. 8, 2016), https://www.technologyreview.com/s/602817

become influential because they are active and produce voluminous tweets, which are then retweeted, thereby spreading misinformation, rumors, and conspiracy theories.[30] Bots aggregate the sentiment in a polarized discussion—they create the illusion of grassroots support and momentum.[31] Russia's impressive use of new technology and social media platforms highlighted the rising importance of cyber-enabled information operations in pursuing foreign policy objectives.

II. THE RISING IMPORTANCE OF CYBER-ENABLED INFORMATION OPERATIONS

The "whole world is a hostage to information," explained Russian Press Secretary Dmitry Peskov in a recent interview.[32] With the great technological advances of the "Information Age," information is no longer a collateral effect of the use or threat of military force, but rather the effective force itself. U.S. military planners recognize that, "our conventional superiority creates a compelling logic for states and non-state actors to move out of the traditional mode of war" and use "some unexpected combination of technologies and tactics to gain an advantage."[33] These planners have suggested, accordingly, that our "most likely opponent in the future" is the enemy that accumulates gains by magnifying small tactical effects through the media and information warfare.[34]

Information operations, like those during the 2016 election, are nothing new. As Senator Mike Rounds (R-SD), chairman of the U.S. Senate Subcommittee on Cybersecurity explained: "[m]any nation-states, in one form or another, seek to shape outcomes, whether they be elections or public opinion."[35] Information is a powerful tool—an element of national power—and the United States is continually seeking new ways to leverage this tool to achieve its foreign policy goals.[36] Early 21st century efforts were as basic as dropping leaflets for civilians and sending

/how-the-bot-y-politic-influenced-this-election (citing research by Alessandro Bessi & Emilio Ferrar).

[30] *Id.*

[31] *Id.*

[32] Jill Dougherty, *How the Media Became One of Putin's Most Powerful Weapons*, ATLANTIC (Sept. 16, 2017), https://www.theatlantic.com /international/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062.

[33] James N. Mattis & Frank Hoffman, *Future Warfare: The Rise of Hybrid Wars*, PROCEEDINGS MAG., Nov. 2005, at 18.

[34] *Id.*

[35] *Cyber-Enabled Information Operations: Hearing Before the S. Subcomm. on Cybersecurity, S. Comm. on Armed Services*, 115th Cong. 2 (2017) (statement of Sen. Mike Rounds, Chairman, S. Subcomm. on Cybersecurity).

[36] DEP'T OF DEF., STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT (2016).

emails to military generals.[37] As of 2015, however, the United States had military information operations personnel deployed to 21 U.S. embassies using a variety of platforms, including the internet, to disseminate information intended to change perceptions and influence the behavior of target audiences.[38] According to media reports, the U.S. military has even attempted to develop software that would allow it to manipulate social media sites using fake online personas to influence internet conversations and spread propaganda.[39]

Whether it is through supporting truthful information, spreading propaganda and disinformation, stoking perceived divisions and disunity, or undermining trust in information streams, cyber-enabled information operations are a consequential weapon in 21st century warfare. This weapon presents a significant challenge, however, because of the way it evades traditional conceptions of war and the laws regulating the use of armed force. Information operations exist within the grey zone between peace and war and exploit states' lack of doctrine to understand them, lack of preparation to combat them, and lack of legal architecture to regulate them. As discussed in the next two sections, this ambiguity leads to disagreements about the legal implications of previously unimagined actions accomplished through emerging technology.

IV. THE INTERNATIONAL LAW OF FORCE

Although American politicians have complained about Russia's "act of war," that is not a recognized term of art in international law. For politicians, referring to an act of war is a rhetorical device that "merely serves to convey the gravity of the situation."[40] Lawyers attempt to be more precise. Classical definitions of war emphasize a conflict (1) between states, (2) using armed forces, (3) to overpower the enemy.[41] War means the use of military force—breaking off diplomatic relations, imposing an economic boycott, or exacting psychological pressure is not enough.[42] An act of war is, therefore, better expressed under international law as a "use of force" or an "armed attack." This section will look at the law relating to use of force and armed attack to evaluate whether cyber-enabled information

---

[37] Peter Ford, *Is it Too Late for a Popular Uprising Inside Iraq?,* CHRISTIAN SCIENCE MONITOR (Jan. 27, 2003), https://www.csmonitor.com/2003/0127/p14s01-usmi.html.

[38] *Countering Adversarial Propaganda: Hearing Before the H. Subcomm. on Emerging Threats & Capabilities, H. Comm. on Armed Services*, 114th Cong. 3 (Oct. 22, 2015) (statement of Brigadier General Charles Moore, Deputy Director for Global Operations, Joint Staff).

[39] Nick Fielding & Ian Cobain, *Revealed: US Spy Operation that Manipulates Social Media*, THE GUARDIAN (Mar. 17, 2011), https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks.

[40] YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 5 (6th ed. 2017).

[41] *Id.* at 7.

[42] *Id.* at 12-13.

operations, such as Russian operations during the 2016 U.S. presidential election, could reasonably be called an act of war.

A. *Jus ad Bellum*, Use of Force, and Armed Attack

While states employ the rhetorical power of war, international law speaks in terms of force.[43] The "starting point for any examination" of the law leading to the use of force—the *jus ad bellum*—is the United Nations (UN) Charter.[44] The UN Charter is the "authoritative statement of the law on the use of force."[45] Article 2(4) establishes that states "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[46] Article 51 ensures that this prohibition on using force does not "impair the inherent right of individual or collective self-defence if an armed attack occurs."[47]

The meaning of the UN Charter has been, and continues to be, "shaped by the actions and reactions of states and by the opinions of publicists and scholars."[48] The Charter provisions are dynamic and thus change over time through state practice.[49] There is not, therefore, perfect agreement on what constitutes a use of force.[50] An even more "fundamental disagreement" relates to that use of force which gives rise to the right of self-defense—the right to go to war.[51]

All states agree that an armed attack gives rise to the right to self-defense.[52] States disagree, however, as to what constitutes an armed attack.[53] The United States insists any use of force is an armed attack and claims the inherent right of self-defense potentially applies against any illegal use of force.[54] This position

---

[43] CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 6-7 (3rd ed. 2008).

[44] *Id.* at 2.

[45] Louis Henkin, *Use of Force: Law and U.S. Policy*, *in* RIGHT V. MIGHT: INTERNATIONAL LAW AND THE USE OF FORCE 38 (2d ed. 1991).

[46] U.N. Charter art. 2, ¶ 4.

[47] U.N. Charter art. 51.

[48] *See* Henkin, *supra* note 45, at 40.

[49] GRAY, *supra* note 43, at 30.

[50] *Id.*

[51] *Id.* at 114.

[52] *Id.* at 128.

[53] *See id*. at 128-29.

[54] OFF. OF GEN. COUNS. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL 47-48 n.230 (Dec. 2016), *citing* Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 92-93 (1989) ("The United States has long assumed that the inherent right of self defense potentially applies against any illegal use of force, and that it extends to any group or State that can properly be regarded as responsible for such activities. These assumptions are supported in customary practice."); *see also* William H. Taft IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE J. INT'L L. 295, 300-01 (2004) ("A requirement that an attack reach a certain level of gravity before triggering a right of self-defense would make the use of force more rather than less likely, because it

varies significantly from most other states and international law scholars, who endorse a "gap" between an Article 2(4) "use of force" and an Article 51 "armed attack."[55] For example, in the *Nicaragua* case, the International Court of Justice (ICJ) distinguished "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[56] The United States claimed it had a right of collective self-defense arising from Nicaragua's supply of arms to armed opposition forces in El Salvador. The court disagreed, concluding that while Nicaragua may have committed a wrongful use of force, supplying arms was not an armed attack and, therefore, did not give rise to an entitlement of self-defense.[57] Similarly, in the *Oil Platforms* case, the ICJ reiterated that the right of self-defense attaches only to an "armed attack" and that other uses of force may not be grave enough to rise to that level.[58]

Though the term "force" in Article 2(4) is not preceded by the adjective "armed," it nevertheless must denote violence.[59] Neither economic nor political coercion is a use of force.[60] The ICJ has found that even the funding of guerrillas engaged in operations in another state does not rise to a use of force.[61] Though arming *and* training them would.[62] The amount or intensity of the violence is irrelevant for determining a use of force, though it may be relevant for armed attack.[63] It is the violence itself that matters, not the type of weapons employed.[64]

Ultimately, in answering whether Russia's information operations constituted an act of war, it is not essential to resolve the debate between use of force and armed attack. Even if a state does not have the full right of self-defense against an action not rising to the level of an armed attack, it can employ proportionate countermeasures against a use of force.[65] Additionally, any use of force, even one falling short of an armed attack, would violate the UN Charter and disrupt the peace. Finally, for U.S. practitioners of information operations, because U.S. policy deems any use of force as equivalent to an armed attack, use of force will be the more

---

would encourage States to engage in a series of small-scale military attacks, in the hope that they could do so without being subject to defensive responses. Moreover, if States were required to wait until attacks reached a high level of gravity before responding with force, their eventual response would likely be much greater, making it more difficult to prevent disputes from escalating into full-scale military conflicts.").

[55] DINSTEIN, *supra* note 40, at 206-07; *see also* GRAY, *supra* note 43, at 147-48.

[56] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 191 (June 27, 1986).

[57] *Id.* ¶ 247.

[58] Oil Platforms (Iran v. U.S.), Judgement, 2003 I.C.J. 161, ¶ 64 (Nov. 6, 2003).

[59] DINSTEIN, *supra* note 40, at 90.

[60] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* 37 COLUM. J. TRANSNAT'L L. 885, 907-08 (1999).

[61] Nicaragua, *supra* note 56, ¶ 228.

[62] *Id.*

[63] DINSTEIN, *supra* note 40, at 90.

[64] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8, 1996).

[65] *Id.* ¶ 42.

consequential lens through which they must view their operations. The important analysis becomes, then, to what extent cyber-enabled information operations can constitute a use of force.

B. Cyber-Enabled Information Operations as a Use of Force

Cyberspace is a relatively new phenomenon and state practice within the domain is "only beginning to clarify the application to cyber operations of the *jus ad bellum*."[66] A cyber operation constitutes a use of force when its "scale and effects" are comparable to traditional uses of force.[67] "Scale and effects" is a shorthand designed to capture the quantitative and qualitative factors to be analyzed.[68] To guide such an assessment, the authors of the Tallinn Manual proposed an approach that considers: (1) severity, (2) immediacy, (3) directness, (4) invasiveness, (5) measurability of effects, (6) military character, (7) state involvement, and (8) presumptive legality.[69]

Cyber operations that cause effects which, if caused by traditional physical means would be regarded as a use of force, will likely be considered a use of force.[70] Such operations might include triggering a nuclear plant meltdown, opening a dam above a populated area causing destruction, or disabling air traffic control services resulting in airplane crashes.[71] Presumably, this would also include cyber interventions with less drastic consequences, such as the Stuxnet attack.[72]

Stuxnet was a computer worm introduced into an Iranian nuclear facility that caused the centrifuges to change the speed of their rotation, thereby breaking them and impeding the Iranian nuclear program.[73] Though this damage was caused remotely, through the use of nonviolent computer programming, it created real physical damage. The severity of this damage and the deleterious effect to the Iranian nuclear facility was indistinguishable from a physical attack and it would be difficult to argue it was anything less than a use of force.

Information manipulation and exploitation, on the other hand, is not a use of force. Article 41 of the UN Charter states explicitly that "interruption of . . . postal, telegraphic, radio, and other means of communication" are not considered to be a

---

[66] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 328 (Michael N. Schmitt et al. eds., 2nd ed. 2017) (The Tallinn Manual is the preeminent study on how international law applies in cyberspace. It records the opinions of 19 international law experts convened under the aegis of the NATO Cooperative Cyber Defence Centre of Excellence.).

[67] *Id.* at 330.

[68] *Id.* at 331.

[69] *Id.* at 333-36.

[70] OFF. OF GEN. COUNS. DEP'T OF DEF., *supra* note 54 ¶ 16.3.1.

[71] *Id.* (citing Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference* (Sept. 18, 2012), *reprinted in* 54 HAR. INT'L L. J. ONLINE 4 (2012).

[72] *See* David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 377 (2013).

[73] *Id.* at 376–77.

use of force.[74] The *jus ad bellum* is primarily concerned with bringing the level of interstate violence to zero. It is much less concerned with those activities that fall below the threat or use of force. As discussed in the previous section, it certainly does not purport to eliminate all forms of coercion between states. In fact, one might hypothesize that because interstate competition is inevitable, banning force is likely to increase other forms of conflict as the competition is channeled to nonviolent forums.

Mere economic or political pressure is not a use of force.[75] Cyber operations intended "to undermine confidence in a government or economy" are not a prohibited use of force.[76] On this point, the Tallinn experts agreed that "non-destructive cyber psychological operations intended solely to undermine confidence in a government" do not qualify as a use of force.[77] Thus, manipulating or changing the opinions and actions of the electorate, so far as it is accomplished through nonviolent means, is not a use of force. If not a use of force, then these information operations would not be properly referred to as acts of war and would not implicate a state's inherent right of self-defense.

C. Russia's 2016 Election Efforts as a Use of Force

Russia's 2016 presidential election efforts can be assessed at each of the three prongs of their operation: (1) the hacking of high-level officials' accounts and selective disclosure of embarrassing information; (2) the compromise of state and local voter registration systems; and (3) the dissemination of propaganda and disinformation in the media.

First, as outlined above, Russia stole and then disclosed emails from the DNC and other politically-connected individuals.[78] It did so with the intent to interfere with the election process, and its actions had very real consequences, such as causing the DNC Chair, Debbie Wasserman Schultz, to resign shortly before the election.[79] However, while these actions were undoubtedly consequential, they were nonviolent. Hacking servers to steal sensitive information is standard espionage.[80] Traditional espionage has long been accepted by the international legal

---

[74] U.N. Charter art. 41.

[75] Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 574 (2011).

[76] *Id.*

[77] TALLINN MANUAL 2.0, *supra* note 66, at 331.

[78] David E. Sanger & Charlie Savage, *U.S. Accuses Russia of Directing Hacks to Influence the Election*, N.Y. TIMES (Oct. 7, 2016), https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html?searchResultPosition=1, at A1.

[79] *Id.*

[80] *See* Gary Brown, *Economic Espionage: Spying and Fighting in Cyberspace: What is Which?*, 8 J. NAT'L SECURITY L. & POL'Y 621, 626 (2016).

system.[81] When applied to the cyber context, merely gaining access to a network or computer to gather information is neither a wrongful use of force nor an armed attack under international law.[82]

The 2014 Sony hack, and the U.S. government's reaction, provides an interesting point of comparison. In presumed retaliation for a Sony Pictures comedy about Kim Jong-un, the North Korean government hacked Sony's computer system, stealing and then releasing to the public massive amounts of personal data, emails, contracts, scripts, and movies.[83] In addition to extracting information, these cyber operations actually damaged Sony's network and rendered inoperable many of their computer systems.[84] While legal writers can debate whether this damage may have constituted a use of force short of an armed attack,[85] the U.S. president expressly denied it was an act of war, and instead termed it cyber vandalism.[86]

Had U.S. government computers been rendered similarly nonfunctional during the 2016 Russian hacking, the debate about just how destructive the effects were would be stronger. Parsing out the difference between physical destruction, like the Stuxnet attack, and interfering with the cataloging and retrieving of information, like the Sony hack, is paramount. The Sony attacks, however, like those against the DNC and political operatives, were carried out against private entities on commercial systems. According to one respected commentator, there is "considerable doubt" as to whether an attack on a commercial system, as compared to a military system, could constitute an attack on a state.[87] In the *Oil Platforms* case, the ICJ looked skeptically at the United States' claim that Iran had attacked it, noting the vessel destroyed, though it might have been American-owned, "was not flying a United States flag, so that an attack on the vessel is not in itself to be equated with an attack on that State."[88] Despite the economic importance of Sony and the political importance of the DNC, it would be troubling to deem actions against those private entities as attacks on a state.

Second, Russian hackers targeted the election systems of at least 21 U.S. states.[89] These efforts seem to have constituted "preparatory activity," such as

---

[81] *Id.* at 622.

[82] *Id.* at 625.

[83] Amanda Hess, *Inside the Sony Hack*, SLATE (Nov. 22, 2015, 8:25 PM), http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

[84] *Id.*

[85] *See* Tim McCormack, *The Sony and OPM Double Whammy: International Law and Cyber "Attacks,"* 18 SMU SCI. & TECH. L. REV. 379, 401 (2015).

[86] Steve Holland & Doina Chiacu, *Obama Says Sony Hack Not an Act of War*, REUTERS (Dec. 21, 2014, 7:55 PM), https://www.reuters.com/article/us-sony-cybersecurity-usa/obama-says-sony-hack-not-an-act-of-war-idUSKBN0JX1MH20141222.

[87] GRAY, *supra* note 43, at 151.

[88] Oil Platforms, *supra* note 58, ¶ 64.

[89] Geoff Mulvihill & Jake Pearson, *Federal Government Notifies 21 States of Election Hacking*, ASSOCIATED PRESS (Sept. 22, 2017), https://apnews.com/cb8a753a9b0948589cc372a3c037a567.

scanning computer systems and attempting to breach voter systems.[90] While no vote counts were changed directly, Russia may have tampered with voter rolls, such that some voters were turned away from the polls.[91] It is undeniable that even making people question whether tampering has occurred undermines faith in an election. However, as discussed above, this type of nonviolent psychological operation that undermines confidence in government—or even democracy as a whole—is not a use of force under international law. Even if Russia had changed vote counts, leading directly to the inauguration of the losing candidate, it is difficult to see this being equivalent to the physical violence required by the ICJ and international legal community.

Third, and finally, Russia masterfully manipulated social media to influence the electorate. In what will surely be of the most interest to social scientists and governments going forward, Russia exploited the democratization of information in social media and Western liberal values about free speech. As explained in detail above, it spread misinformation, stoked division, and sowed confusion. This was the most devastating aspect of Russian operations in the 2016 election and will be the most difficult to combat in the future, but it is the easiest prong to dismiss as a possible use of force. There is simply nothing about Russian social media operations that approximates physical force or violence. While unusual in its sophisticated use of new media, there is nothing unusual about states using propaganda to influence elections. Russia has long used propaganda in an attempt to undermine Western liberalism and call into question the feasibility of democracy.[92] The United States too has used information activities to influence foreign elections.[93] No matter how consequential the propaganda is to the outcome, if it does not hurt people or damage property it is not a use of force under international law.

That is not to say information activities could never constitute a use of force. During the 2016 election, Russia helped spread, among other hoaxes, a conspiracy that Secretary Clinton and her aides were running a pedophile ring in the basement of a Washington DC pizza parlor.[94] Someone taken in by this hoax showed up at

---

[90] *Id.*

[91] Nicole Perlroth, Michael Wines, & Matthew Rosenberg, *Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny*, NY TIMES (Sept. 1, 2017), https://www.nytimes.com/2017/09
/01/us/politics/russia-election-hacking.html.

[92] Michael Weiss, *The Making of a Russian Disinformation Campaign: What it Takes*, CNN (Oct. 11, 2017), https://www.cnn.com/2017/10/11/
opinions/the-making-of-a-russian-disinformation-campaign-opinion-weiss/index.html.

[93] Ishaan Tharoor, *The Long History of the U.S. Interfering with Elections Elsewhere*, WASH. POST (Oct. 13, 2016), https://www.Washington
post.com/news/worldviews/wp/2016/10/13/the-long-history-of-the-u-s-interfering-with-elections-elsewhere/?utm_term=.876daa71ccd5.

[94] Calabresi, *supra* note 20.

the pizza parlor with an assault rifle and fired it near an employee.[95] The man claimed he had come to investigate the abuse.[96] Though Russia did not invent this bizarre conspiracy theory, its release of hacked emails created the fodder and its social media actions helped propagate it. If the man had killed the employee instead of just scaring him, would Russia be responsible for this use of force (or armed attack)? Based on the sheer absurdity and unpredictability of the man's actions, one would assume not. However, one can imagine information manipulations that result in more causally linked harm. If a state were to manipulate the information environment, by changing programing code in a computer system so the screen displayed inaccurate information for example, such that a worker inadvertently triggered a nuclear plant meltdown, or a pilot could not land an airplane, these could be classified as uses of force. In the case of Russia's information operations during the 2016 election, nothing approximates such a use of force. That these operations did not constitute a use of force does not end the analysis, because they may have been illegal for other reasons.

V. NON-INTERVENTION IN INTERNAL POLITICAL AFFAIRS

That a cyber operation fails to rise to a use of force, "does not necessarily render it lawful under international law."[97] An operation might still constitute a violation of state sovereignty through a breach of the non-intervention principle.[98] Given the combined scope and scale of Russia's cyber-enabled information operations during the 2016 presidential election, and its clear intent to manipulate a democratic political outcome, Russia likely violated the principle of non-intervention. The opposing conclusion, however, would be defensible as well, because of the ambiguity of what constitutes coercive intervention, particularly with respect to a democratic election. This section describes the prohibition on coercive intervention, considers how this principle applies to influencing electorates, and then assesses Russia's 2016 U.S. election operations with respect to this non-intervention principle.

A. The Prohibition on Coercive Intervention

[95] Amy Davidson Sorkin, *The Age of Donald Trump and Pizzagate*, NEW YORKER (Dec. 5, 2016), https://www.newyorker.com/news/amy-davidson/the-age-of-donald-trump-and-pizzagate.

[96] *Id.*

[97] TALLINN MANUAL 2.0, *supra* note 66, at 330.

[98] Brian J. Egan, *International Law & Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 174 (2017) ("In certain circumstances, one State's non-consensual cyber operation in another State's territory *could* violate international law, even if it falls below the threshold of a use of force.").

"The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference."[99] While this principle is not specifically articulated within the U.N. Charter, it is widely accepted as a matter of customary international law and has been reflected in numerous international declarations.[100] For example, in 1981, the U.N. General Assembly, in the *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, reaffirmed the "sovereign and inalienable right of a State freely to determine its own political . . . system . . . in accordance with the will of its people, without outside intervention, interference, subversion, coercion or threat in any form whatsoever."[101] The same declaration recognized the "right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political . . .interests and aspirations."[102]

As articulated by the General Assembly, the non-intervention principle would seem to preclude essentially any involvement in another state's internal affairs. In that case, Russia's, as well as many other states', information operations would clearly violate the principle. However, just five years after the U.N. declaration, the ICJ found the non-intervention principle required more significant coercive involvement.[103] Intervention, they said, "is wrongful when it uses *methods of coercion* in regard to such choices, which must remain free ones."[104] Coercion, thus, "forms the very essence of" intervention.[105]

Coercion is "particularly obvious" in the use of force.[106] However, a coercive act is any act designed to compel another state to take action it would not otherwise take or refrain from action it would take.[107] While it need not rise to the level of force, coercion requires more than "mere influence."[108] It involves actions that "deprive the target State of choice."[109] Propaganda, even if intended to cause a state to act in a certain way, does not qualify as intervention because "the target state retains the ability to choose."[110] An ill-informed vote—even one shaped by the misinformation of an international competitor—is still a choice.

Coercive intervention remains a "grey zone" in international law—an area of significant legal ambiguity.[111] Between funding, training, and equipping forces to overthrow a government e.g., the *Nicaragua* case, and mere propaganda, there is

---

[99] Nicaragua, *supra* note 56, ¶ 202.
[100] *Id.* ¶ 202, 203.
[101] G.A. Res. 36/103 ¶ 2(I)(b) (Dec. 9, 1981).
[102] *Id.* ¶ 2(I)(c).
[103] Nicaragua, *supra* note 56, ¶ 205.
[104] *Id.* (emphasis added).
[105] *Id.*
[106] *Id.*
[107] TALLINN MANUAL 2.0, *supra* note 66, at 318-19.
[108] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L. L. ONLINE 1, 8 (2017).
[109] *Id.*
[110] *Id.*
[111] *Id.* at 8.

not a lot of guidance in international law. The sliding scale hinges on choice and when an action moves from information influence—fairly competing within the marketplace of ideas—to usurpation of free will. This becomes particularly relevant when applied to influencing electorates.

B. Elections, Electorates, and Political Independence

Protecting a state's self-determination with respect to its political system is at the core of the non-intervention principle.[112] States must remain free to decide on their own political systems.[113] The international community has been particularly concerned about interventions in the electoral process.[114] The whole point of democracy is that the government should reflect the will of the people.[115] Therefore, when it comes to undermining the political independence of a democracy, the electorate is the point of inflection.

Despite the sensitivity of electoral interventions, states have a long history of influencing elections.[116] States use political activity to help friends and impede foes—and this is to say nothing of efforts to violently overthrow leaders and establish regime change. One political scientist calculated that the United States and Russia/Soviet Union intervened in elections 117 times between 1946 and 2000.[117] These interventions spanned public threats and promises, provision of campaign funds, leaking of documents, and creation of campaign materials.[118] At one end of the spectrum, in the late 1940s, the U.S. "supplied scarce newsprint to centrist, anticommunist political parties in Italy and France during closely contested elections."[119] At the other end, Russia may have poisoned the main Ukrainian opposition candidate, Viktor Yushchenko, in 2004.[120]

Not all electoral involvement violates the non-intervention principle. That will depend, as discussed above, on whether the involvement is coercive—whether it

---

[112] G.A. Res. 36/103 (Dec. 9, 1981).

[113] Nicaragua, *supra* note 56, ¶ 205.

[114] Maziar Jamnejad, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 369 (2009) ("States are particularly concerned about this form of intervention, and nine General Assembly resolutions condemning interference in electoral processes were adopted between 1989 and 2001.").

[115] Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1595 (2017).

[116] *See* Dov H. Levin, *Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset*, CONFLICT MANAGEMENT & PEACE SCI. (2016).

[117] Dov H. Levin, *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results*, 60 INT'L STUDIES Q. 189 (2016).

[118] *Id.* at 192-93.

[119] MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 186 (5th ed. 2012).

[120] Levin, *supra* note 117, at 193; Elisabeth Rosenthal, *Liberal Leader from Ukraine was Poisoned*, N.Y. TIMES (Dec. 12, 2004), http://www.nytimes.com/2004/12/12/world/europe/liberal-leader-from-ukraine-was-poisoned.html.

deprives the electorate of free choice. That states repeatedly engage in certain behaviors suggests that they do not consider them to violate international law. Thus, while it may violate domestic law,[121] funding politicians, political parties, and political campaigns could hardly constitute impermissible intervention. Similarly, influencing the information environment, even through propaganda or disinformation, is permissible. By contrast, interfering with a state's ability to hold an election, or manipulating election results "would be a clear violation of the rule of non-intervention."[122] Whether Russia's involvement in the 2016 U.S. presidential election was prohibited, therefore, depends where along this spectrum its activity falls.

C. Russian Intervention in the 2016 Election

Scholars who have analyzed Russia's actions during the 2016 election are divided over whether they violated international law.[123] None of the standard rubrics for assessing such actions "clearly and unambiguously apply" to the facts.[124] Some have even argued that the standard framework under international law is insufficient to handle these technologically sophisticated cyberattacks.[125] They argue that Russia's actions did not violate the non-intervention principle as it currently exists, but they should.[126] Importantly, these opinions were formed on but one aspect of Russia's operations: the hacking and release of information. They did not assess the compromising of voter registration systems or the disinformation campaign in social media.

As detailed above, Russia deliberately interfered in the 2016 presidential election by (1) hacking and disclosing information from political operatives, (2) compromising voter registration systems, and (3) disseminating propaganda and disinformation. Any one of these might not constitute a prohibited intervention on

---

[121] *See*, *e.g.*, 52 U.S.C. § 30121 (prohibiting foreign nationals from donating money in connection with an election).

[122] Egan, *supra* note 98, at 175.

[123] Ohlin, *supra* note 115, at 1579 ("When it was revealed that the Russian government interfered in the 2016 U.S. presidential election…international lawyers were divided over whether the cyber attack violated international law."); Schmitt, *supra* note 108, at 8 ("Opinions vary as to whether the cyber operations were coercive in the intervention sense…[the] slightly sounder view is that the cyber operations manipulated the process of elections and therefore caused them to unfold in a way that they otherwise would not have. In this sense, they were coercive.").

[124] Ohlin, *supra* note 115, at 1579-80.

[125] Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT'L SEC. J. 146, 169 (2018).

[126] *Id.* ("[T]his Article calls for a reevaluation of non-intervention's application to technically non-coercive but highly disruptive cyber-attacks. In the context of cyber-attacks, I submit that the norm against non-intervention is violated when the attack causes 'disruption' rather than outdated notion of 'coercion.'").

its own. First, Russia hacked private email accounts and disclosed unaltered information. Though some of the emails likely shaped voter opinions, they remained free to use or not use this information as they pleased. It would be difficult to argue that giving the public more information—even if accomplished through illegal means—constitutes an impermissible intervention. Second, Russian computer hackers conducted preparatory steps on U.S. state election systems but may have done nothing more than scare election officials with the possibility of what could have been. Exposing the weakness of electronic voting infrastructure, without actually changing votes, is not coercive. Third, while Russia conducted an incredibly sophisticated social media propaganda campaign, exposing voters to lies and conspiracy theories, it essentially just magnified the discontent and discord that already existed. Arguably, thoughtful voters could ignore the absurd conspiracy theories and consider the issues that were important to them. Their free will was not overcome merely by social media ads.

As a whole, however, Russia's influence operation was: (1) intrusive along a core democratic political function, (2) unprecedented in scale, and (3) motivated by clear intent to interfere in an internal political matter. First, while the intensity of Russia's actions—in terms of the level of intrusiveness—fell far short of armed force, they were directed at democratic elections, an area the international community has been particularly sensitive about. Furthermore, Russian agents used criminal means—hacking both private and government computer systems—to carry out their ends, and certainly violated U.S. election laws. Additionally, the actual injury caused by Russia's actions was severe. At the most extreme, they may have determined the outcome of the election. Even at the least extreme, they have undermined confidence in the legitimacy of the election and the installed president. Finally, if Russia actually precluded people from voting, either by encouraging Clinton supporters to vote using invalid methods,[127] or by tampering with local poll books such that voters were turned away,[128] there is little doubt that preventing an electorate from expressing its will constitutes coercive intervention.

Second, the scale of Russia's information campaign was stunning. It constituted a multi-faceted effort to use cyber espionage, network disruption, covert misinformation, and overt propaganda. On social media alone, Facebook identified more than 80,000 fake ads and estimated 126 million people were exposed to Russia-linked content.[129] Twitter found nearly 3,000 Russian operative-controlled accounts and more than 36,000 bots that disseminated 1.4 million tweets during the election.[130] This is to say nothing of the fact that nearly every voter was exposed—through the news media or water cooler conversations about what had been reported—to hacked information and Russian-bolstered conspiracy theories.

---

[127] *Social Media Influence in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 6 (2017) (statement of Sean J. Edgett, acting general counsel of Twitter).

[128] Perlroth, Wines, & Rosenberg, *supra* note 91.

[129] Nicholas Fandos, Cecilia Kang, & Mike Isaac, *House Intelligence Committee Releases Incendiary Russian Social Media Ads*, N.Y. TIMES (Nov. 1, 2017), https://www.nytimes.com/2017/11/01/us/politics/russia-technology-facebook.html.

[130] *Id.*

The effects, of course, are much more difficult to disentangle. Some potential voters may have been turned away from the polls or did not go in the first place because they thought they had already voted, but those actions are the least capable of being attributed to Russia. The DNC changed leadership and feelings were hurt, but it is difficult to know how those hacks shaped the final outcome of the election. The most speculative part of the assessment is how the social media campaign impacted voters. It certainly fueled the flames of discord, but did it change any votes? There is no way of knowing.

Third, Russia acted with the intent to influence the election. The purpose or motivation of the intervening state is surely important in assessing the legality of its actions. Value promotion or image management—the type of activity Russia does through its Russia Today platform—will be looked upon much more favorably than regime change. Russia has refused to admit it was involved in 2016 election intervention efforts, let alone disclosed its true motives. But the U.S. Intelligence Community has declared that one of Russia's objectives was to harm the electoral chances and potential presidency of Secretary Clinton.[131] The content of much of the misinformation and the hacks of the DNC support that. It is also true that much of the content of the inauthentic activity on social media was not specifically about the election, but rather amplified a range of divisive political, social, and racial issues.[132] With this dual intent, Russia sought both to influence the outcome of a specific election, and to undermine faith in the liberal democratic system as a whole. Both of these objectives cut to the core of what the principle of non-intervention is intended to protect. Interfering for these objectives goes beyond permissible interstate competition.

Based on the specific facts of Russia's information operations during the 2016 U.S. presidential election, the stronger argument is that they violated the non-intervention principle. Through a multi-faceted operation that was intrusive, pervasive, and motivated by ill-intent, Russia interfered with the U.S. electorate's right to freely choose its political leadership in a fair contest. The international community has a strong interest in clearly delimiting impermissible intervention in democratic elections and should do so in this case. That being said, the extent to which cyber-enabled information operations implicate the non-intervention principle will remain highly fact dependent as states struggle to apply an old legal framework to innovative operations enabled by new technology.

VI. CONCLUSION

While we were consumed by the technological aspects of election hacking and cyber security, Russia orchestrated an incredibly successful effort to hack the electorate. Using both covert cyber intelligence operations and overt media operations, Russia implanted ideas—about a candidate, about an election, and about a democratic system—that continue to reverberate through the American psyche.

---

[131] OFF. OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 7, at 1.
[132] Stamos, *supra* note 21; Wakabayashi & Shane, *supra* note 23.

This interference undercut the legitimacy of the American democratic process and may have swayed the outcome of the 2016 presidential election. While complaints of an act of war are inaccurate under international law, American politicians are rightly concerned by this prohibited intervention into U.S. internal affairs. Cyber-enabled information operations have provided an array of powerful new weapons in the realm of interstate competition as states attempt to exert their will and achieve favorable international outcomes. While these weapons can be used within the scope of the law to influence decision-makers (including electorates), they can also cross the line into coercive intervention of state sovereignty. Understanding the way these new weapons fit into the old fabric of international law will help states respond to operations against them and lawfully carry out operations against their competitors.