FAKE NEWS: THE LEGALITY OF THE RUSSIAN 2016 FACEBOOK INFLUENCE CAMPAIGN

ALLISON DENTON

ABSTRACT

From the Internet Research Agency's office building in Saint Petersburg, Russia, a number of Russian hackers created fake Facebook profiles of American citizens and used these profiles to purchase and design politically divisive Facebook advertisements. Likely backed by the Russian government, Agency hackers intended to use the fake advertisements to promote the 2016 presidential election of Donald Trump, to cause political division in America, and to foster distrust of the American media. Using Facebook's Core Audience and Custom Audience tools exactly as they are supposed to be used, the Agency's fake advertisements reached 126 million Facebook users. This note will first paint a picture of Russia's motives and methodologies with respect to the 2016 influence campaign. It will then analyze the Facebook influence campaign as a violation of domestic law and of international law. Concluding that the influence campaign is a violation of domestic law but not international law, this note will finally discuss the policy implications of these conclusions.

INTRODUCTION

Behind the white glow of their computer screens, Russian hackers employed by the Internet Research Agency (the "Agency") conducted a multi-faceted campaign intended to influence the 2016 U.S. presidential election between Hillary Clinton and Donald Trump. A crucial aspect of this campaign was conducted over Facebook, a popular social media platform. Agency hackers first created fake Facebook profiles under seemingly American names and identities.[1] Next, Agency hackers used these fake profiles to purchase advertisements from Facebook, and designed inflammatory advertisements directed at hot-button political issues and the candidates themselves.[2] Finally, using Facebook's Core Audience and Custom Audience tools exactly as they are supposed to be used, Agency hackers directed these advertisements to target susceptible American voters by implementing specific demographic information into Facebook's advertising tools.[3] Algorithms generated by Facebook then used this demographic information to distribute the advertisements to the Agency's target audience.[4]

Much controversy has surrounded the legality of the Russian influence campaign in the 2016 election. This question has been difficult to answer given the multi-faceted nature of the campaign. In addition to the Facebook influence campaign, Russia has also been accused of other election-meddling activities, for example, the DNC Hack, alleged interference with electoral booths, and the staging of rallies or in-person protests.[5] Further, because the

[1] Adrian Chen, *The Agency*, N.Y. TIMES (June 2, 2015), https://www.nytimes.com/2015/06/07/magazine/the-agency.html. [http://perma.cc/9GML-HNGT]

[2] *Id.*

[3] Elizabeth Dwoskin, Craig Timberg & Adam Entous, *Russians Took a Page from Corporate America by Using Facebook Tool to ID and Influence Voters*, WASH. POST (Oct. 2, 2017), https://www.washingtonpost.com/business/economy/russians-took-a-page-from-corporate-america-by-using-facebook-tool-to-id-and-influence-voters/2017/10/02/681e40d8-a7c5-11e7-850e-2bdd1236be5d_story.html?utm_term=.b1abbe3b6ce7 [http://perma.cc/G8UE-UD48].

[4] Massimo Calabresi, *Inside Russia's Social Media War on America*, TIME (May 18, 2017), http://time.com/4783932/inside-russia-social-media-war-america/ [http://perma.cc/5AH5-RNVG].

[5] Chen, *supra* note 1.

Russians operated near the outskirts of the law (as opposed to blatantly over or under the line of legality), the actual harm resulting from the influence campaign is rather low. The Russians did not primarily attack vote-counting systems, but instead focused on more subliminal messaging through methods such as the Facebook influence campaign. Thus, the only concrete harms resulting from the campaign are the fostering of distrust in the media and the creation of political division. As explained herein, these harms are not considered substantial from a legal standpoint.

This paper will examine whether the Agency's creation of fake Facebook profiles, purchase of fake Facebook advertisements, and use of Facebook's targeted advertising tools for the purpose of influencing the 2016 election (the "Facebook influence campaign") violated domestic and international law. Part 1 will discuss the Russian motivations behind the influence campaign and will examine the specific methods used by the Russians over Facebook in conducting the campaign. Part 2 will analyze the various theories under which the Facebook influence campaign could be considered a violation of domestic and international law. This section will examine the violation of domestic law theories in the February 2018 indictment by Special Counsel Robert Mueller and will propose that the Facebook influence campaign could be a violation of the Computer Fraud and Abuse Act ("CFAA"). Next, this section will examine the various international law theories under which the Facebook influence campaign could be considered a violation, concluding that the Facebook influence campaign does not violate international law. Part 3 will analyze the policy implications of these conclusions. It will first suggest that domestic law enforcement is an insufficient means of handling remote cyber election meddling activities. It will similarly propose that foreign policy supports the fact that remote cyber election activities like the Facebook influence campaign should not be considered violations of international law. Finally, it will conclude that rather than criminalizing remote cyber election activities on the domestic or international law platforms, a policy framework is the most effective means of handling this pervasive issue.

I. RUSSIAN MOTIVATIONS AND METHODOLOGY BEHIND THE 2016 FACEBOOK INFLUENCE CAMPAIGN

In 2017, the CIA, FBI, and NSA released a Directorate of National Intelligence Report ("DNI Report") on the Russian activities and intentions in conducting the 2016 influence campaign. The DNI Report assessed with "high confidence" that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election,"[6] and

[6] DIR. OF NAT'L INTELLIGENCE, ICA 2017-01D, INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS: THE ANALYTIC

further, that "Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences."[7] With respect to Russia's goals, the DNI report stated with "high confidence" that the Russians intended the influence campaign to "undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."[8] In order to advance these goals, the Internet Research Agency created a sprawling, highly-sophisticated influence campaign over multiple social media platforms.

A. Russian Motivations Behind the 2016 Facebook Influence Campaign

The Russian influence campaign purported to destabilize American democracy and to promote the election of Donald Trump.[9] By sharing controversial articles and videos on platforms such as Facebook, Russia sought to "deepen the splits" between Clinton and Trump supporters, thus undermining faith in American democracy and the American media.[10] At the same time, the decidedly pro-Trump and anti-Clinton rhetoric in the postings aligned with Russia's goal of supporting Trump's candidacy.

Russia's preference for Trump over Clinton is unsurprising. To Russia, the election of Clinton would have presented obstacles to ending sanctions against "Putin's cronies after the annexation of Crimea and the invasion of eastern Ukraine";[11] destabilizing NATO;[12] advancing Russia's positions on Syria and Ukraine;[13] and achieving an international counterterrorism coalition against ISIL.[14] In addition to these foreign policy considerations, Putin may "hold a grudge" against Clinton for speaking out against the Putin

PROCESS AND CYBER INCIDENT ATTRITION ii (2017) [hereinafter DNI REPORT].

[7] *Id.* at iii.

[8] *Id.* at ii.

[9] *See id.* (noting that "Putin and the Russian government developed a clear preference for President-elect Trump").

[10] *See* Evan Osnos, David Remnick, & Joshua Yaffa, *Trump, Putin, and the New Cold War*, NEW YORKER (Mar. 6, 2017), https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war [https://perma.cc/6YTE-TC6N] (targeting groups by "demographics, geography, gender and interests").

[11] *Id.*

[12] *Id.* (noting the Kremlin views "the expansion of NATO to Russia's borders" as "provocation" and "against Russia's interests"). *See also* Lauren Carroll, *Russia and its Influence on the Presidential Election*, POLITIFACT (Dec. 1, 2016), http://www.politifact.com/truth-o-meter/article/2016/dec/01/russia-and-its-influence-presidential-election/ [https://perma.cc/JT9K-TV9G] (noting that in the third presidential debate, Clinton accused Trump of planning to "break up NATO" at Putin's request).

[13] DNI REPORT, *supra* note 6, at 4. *See also* Osnos et al., *supra* note 5 (noting that the Kremlin feared military action by Clinton in Syria).

[14] DNI REPORT, *supra* note 6, at 1.

regime by "inciting mass protests" during the 2011 Russian elections.[15] The Russian government favored Trump's election so powerfully that Vladimir Zhirinovskiy, the leader of the nationalist Liberal Democratic Party of Russia, even stated that the Russians would be "drinking champagne" if Trump won the presidency.[16] On November 8, 2016, their wish came true. At the end of a bitterly divisive election cycle, Donald Trump was elected President of the United States.[17]

Since the election, many have accused Trump of colluding with Russia in operating the 2016 influence campaign. In May 2017, the Department of Justice appointed Robert Mueller as Special Counsel "to oversee the investigation into ties between President Trump's campaign and Russian officials."[18] Trump has repeatedly denied these accusations, referring to the investigation as a "witch hunt" and a "hoax."[19] Trump has also rejected the suggestion that the influence campaign may have affected the outcome of the election, decided by an "extraordinarily close margin."[20]

Despite Trump's claims, as of October 2018, Mueller indicted or obtained guilty pleas from thirty-two people tied to the investigation. This number includes guilty pleas from four high-ranking Trump employees: George Papadopoulos, Trump's former foreign policy adviser; Paul Manafort, Trump's former campaign manager; Rick Gates, a former Trump campaign aide and Manafort's business partner; and Michael Flynn, Trump's former national security adviser.[21]

More relevantly, Mueller also indicted perpetrators of the Russian influence campaign in February 2018 and July 2018. In February, Mueller indicted "the [Agency], two other shell companies involved in financing the [A]gency, its alleged financier (Yevgeny Prigozhin), and 12 other Russian

---

[15] *Id. See also* Carroll, *supra* note 12 (discussing Putin's belief that Clinton incited protests surrounding 2011 Russian elections).

[16] DNI REPORT, *supra* note 6, at 4.

[17] *See* Harrison Smith, *Donald Trump is Elected President of the United States*, WASH. POST (Nov. 9, 2016), https://www.washingtonpost.com/lifestyle/kidspost/donald-trump-is-elected-president-of-the-united-states/2016/11/09/58046db4-a684-11e6-ba59-a7d93165c6d4_story.html?utm_term=.a3fb40c674aa [https://perma.cc/AMT8-3BT4] (discussing the controversy between Trump and Clinton prior to the election).

[18] Rebecca R. Ruiz & Mark Landler, *Robert Mueller, Former F.B.I. Director, Is Named Special Counsel for Russia Investigation*, N.Y. TIMES (May 17, 2017), https://www.nytimes.com/2017/05/17/us/politics/robert-mueller-special-counsel-russia-investigation.html [http://perma.cc/9HZD-9DJ7].

[19] Scott Shane & Mark Mazzetti, *The Plot to Subvert an Election: Unraveling the Russia Story So Far*, N.Y. TIMES (Sept. 20, 2018), https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html.

[20] *Id.*

[21] *Id.*

nationals who allegedly worked for it."[22] This indictment will be discussed in more detail in the domestic law analysis herein. In July, Mueller charged 12 officers of a Russian military agency with crimes related to "the high profile hacking and leaking of leading Democrats' emails during the 2016 campaign."[23] The Mueller investigation and indictments have contributed to the controversy surrounding the legality of the 2016 Russian influence campaign.

B. *Russian Methodology Behind the Influence Campaign*

The Russian influence campaign was multi-faceted and employed a variety of cyber-sleuthing techniques. For instance, Cozy Bear and Fancy Bear, two hacking groups working for the Russian government, facilitated the DNC Hack in June 2016.[24] The DNC hack involved a spear phishing attack[25] on John Podesta, compromising thousands of emails involving Clinton and the Clinton campaign.[26] The release of Podesta's emails revealed, among other things, that Clinton was given a "heads up" of the questions that would be asked during the primary debates.[27] In a more advanced attack, the Russians used "expertly tailored" messages to lure Defense Department employees into clicking on seemingly innocuous links posted to Twitter ("DoD Twitter Hack").[28] These messages contained malware that allowed hackers to "take

[22] Andrew Prokop, *All of Robert Mueller's Indictments and Plea Deals in the Russia Investigation So Far*, VOX (Oct. 10, 2018), https://www.vox.com/policy-and-politics/2018/2/20/17031772/mueller-indictments-grand-jury. [https://perma.cc/GG4B-6A9X]

[23] *Id.*

[24] Philip Bump, *Here's the Public Evidence that Supports the Idea that Russia Interfered in the 2016 Election*, WASH. POST (July 6, 2017), https://www.washingtonpost.com/news/politics/wp/2017/07/06/heres-the-public-evidence-that-supports-the-idea-that-russia-interfered-in-the-2016-election/?utm_term=.9d5825aa6572 [http://perma.cc/MTR4-YRKW].

[25] A phishing attack is when a hacker uses an "innocent-looking email to entice unwary recipients to click on a deceptive link, giving hackers access to their information or their network." Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?mcubz=0&_r=0 [http://perma.cc/MEV4-6VLC]. A spear-phishing attack occurs when this email is "tailored to fool a specific person." *Id.*

[26] Joe Uchill, *Typo Led to Podesta Email Hack: Report*, THE HILL (Dec. 13, 2016), http://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack [http://perma.cc/QW9F-8VXZ].

[27] *Id.*

[28] Calabresi, *supra* note 4 (noting that the "messages offered links to stories on recent sporting events or the Oscars, which had taken place the previous weekend").

control of the victim's phone or computer-and Twitter account."[29] The DoD Twitter Hack affected more than 10,000 Defense Department employees.[30] The DNC Hack and the DoD Twitter Hack illustrate the breadth and sophistication of the Russian influence campaign over social media.

This paper will focus specifically on the Facebook influence campaign. Though the influence campaign spanned a number of social media platforms, Facebook was the most popular for Russian hackers.[31] To facilitate the Facebook influence campaign, the Agency created at least 470 fake Facebook accounts[32] and employed "hundreds of Russians to post pro-Kremlin propaganda online under fake identities."[33] The Agency indictment accused Yevgeny Prigozhin, nicknamed "Putin's cook," and two companies that Prigozhin controlled of financing the influence campaign.[34] Prigozhin is a loyal Putin ally with a history of involvement in Russian government contracting and supporting senior Russian Federation officials.[35] With Prigozhin's contributions, the Agency used fake accounts to purchase more than $100,000 in Facebook advertisements.[36] Many of the advertisements were paid for using Qiwi, the Russian equivalent of Paypal.[37]

In addition to advertisements specific to Trump and Clinton, the Russian-sponsored posts included advertisements or messages exploiting "hot-button issues as illegal immigration, African American political activism and the

---

[29] *Id.*

[30] *Id.*

[31] *See* Sheera Frenkel & Katie Benner, *To Stir Discord in 2016, Russians Turned Most Often to Facebook*, N.Y. TIMES (Feb. 17, 2018), https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html [http://perma.cc/69UR-S9Z5] (noting that "[Facebook], more than any other technology tool" was singled out in the February 2018 Mueller indictment).

[32] Scott Shane & Vindu Goel, *Fake Russian Facebook Accounts Bought $100,000 in Political Ads*, N.Y. TIMES (Sept. 6, 2017), https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html?mcubz=3&_r=0 [http://perma.cc/Y7JN-899P].

[33] Chen, *supra* note 1.

[34] Indictment at 3, United States v. Internet Research Agency LLC et al., No. 1:18-cr-00032-DLF (D.C. Cir. filed Feb. 16, 2018). *See also* Neil MacFarquhar, *Yevgeny Prighozin, Russian Oligarch Indicted by U.S., Is Known As 'Putin's Cook'*, N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html [http://perma.cc/FM3G-5ENL].

[35] MacFarquhar, *supra* note 34.

[36] Shane & Goel, *supra* note 32.

[37] Craig Timberg, Elizabeth Dwoskin, Adam Entous & Karoun Demirjian, *Russian Ads, Now Publicly Released, Show Sophistication of Influence Campaign*, WASH. POST (Nov. 1, 2017), https://www.washingtonpost.com/business/technology/russian-ads-now-publicly-released-show-sophistication-of-influence-campaign/2017/11/01/d26aead2-bf1b-11e7-8444-a0d4f04b89eb_story.html?utm_term=.0a0fe0df0e82 [http://perma.cc/TS7V-LAEG].

rising prominence of Muslims in the United States."[38] While the majority of posts advanced conservative views, some contained liberal and anti-Trump rhetoric on controversial topics.[39] Though Russia hoped to advance Trump's candidacy, it also sought to cause political division and controversy in America. As such, it is not surprising that a minority of posts supported liberal causes.

Congress and independent researchers have made public a sampling of the Agency's posts.[40] One post depicts Jesus arm-wrestling with Satan.[41] Its caption declares Clinton "a Satan" while comparing Trump to a saint.[42] Another post contains a photo of women wearing the traditional Muslim Burqa with text suggesting that Muslims are terrorists.[43] Yet another post calls for the disqualification of Clinton from the presidential race, implying that her candidacy ran contrary to the values of the Founding Fathers.[44] Additional posts expressed anti-Black Lives Matter and pro-police views; support for closed borders; and allegations of corruption against the Clinton Foundation.[45]

Although the underlying accounts were fake, the Agency used Facebook's advertising service exactly as the platform is supposed to be used. Even Facebook did not initially notice the influence campaign as the "accounts, pages, and ads appeared to be legitimate."[46] Facebook's advertising service allows users to input information regarding its target audience, and then follows an algorithm to reach that target audience.[47] Algorithms are formulas designed to "segment huge populations into thousands of subgroups according to defining characteristics" to target certain demographics.[48] After the algorithm is generated, propagandists (people or automated computer programs known as bots) craft messages intending to influence followers' behavior. In other words, the algorithm allows propagandists to identify people who will be most responsive to the advertisements' content, and then ensures that the advertisements will reach the target audience.

Many companies and political campaigns use Facebook-generated

---

[38] Dwoskin et al., *supra* note 3.

[39] Scott Shane, *These Are the Ads Russia Bought on Facebook in 2016*, N.Y. TIMES (Nov. 1, 2017), https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html?_r=0 [http://perma.cc/7LTA-MV76].

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] Dwoskin et al., *supra* note 3.

[47] Calabresi, *supra* note 4.

[48] *Id.*

algorithms to reach potential customers or supporters.[49] The Facebook influence campaign, for example, did so using Facebook's advertising services exactly as they are supposed to be used. Nevertheless, in March 2018, Trump's election campaign was accused of impermissibly exploiting Facebook's advertising service by hiring the political data firm Cambridge Analytica to use "tools that could identify the personalities of American voters and influence their behavior."[50] The data "included details on users' identities, friend networks, and 'likes.' The idea was to map personality traits based on what people had liked on Facebook, and then use that information to target audiences with digital ads."[51] Facebook as the advertising service of choice showcases its effectiveness in reaching the advertiser's target goals.

Facebook's advertising service contains a number of tools allowing users to tailor advertisements to their specific needs. Facebook's most basic advertising service, the Core Audience tool, allows advertisers to identify and reach a susceptible target audience. The Core Audience tool gives users the ability to "find people" based on location, demographics, interests, behavior, and connections.[52] It also allows users to set specific preferences related to the ad, including the ad's objective and the target audience.[53] Once the Core Audience tool sends the advertisement to the target audience, the more advanced Custom Audience tool focuses in on the most susceptible users by allowing advertisers to retarget those who already accessed pages promoted by the advertisers' accounts.[54] In addition to retargeting, the Custom Audience tool allows for more specific targeting of people by location, age, gender, and interests, among other factors.[55] Facebook can generate this expertly directed advertising campaign in as little as thirty minutes.[56]

The Agency likely first used the Core Audience tool to direct its advertisements toward a susceptible target audience. Once users clicked on the Agency's advertisements, the Agency then employed the Custom

---

[49] Dwoskin et al., *supra* note 3.

[50] Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/M6LT-YVZ3].

[51] *Id.*

[52] *Core Audiences*, FACEBOOK, https://www.facebook.com/business/learn/facebook-ads-choose-audience (last visited Nov. 6, 2017) [http://perma.cc/5T7R-6MRK].

[53] *Id.*

[54] Dwoskin et al., *supra* note 3.

[55] *Custom Audiences*, FACEBOOK, https://www.facebook.com/business/a/custom-audiences?ref=sem_smb&campaign_id=1398023950488031&placement=broad&creative=68255646852&keyword=+targeted++facebook++ads&extra_1=481d506a-7450-457b-9e5d-945c397aa33f (last visited Nov. 6, 2017) [http://perma.cc/K4WQ-RUW8].

[56] *Id.*

Audience tool to retarget these users.[57] The Custom Audience feature sent "specific ads and messages to voters" who visited sites contained in the Agency's advertisements.[58] Clicking on a site contained in an Agency advertisement would bring the user to a platform outside Facebook, "where they would be tracked with more-aggressive forms of tracking software."[59] Additionally, many Russian sites outside of Facebook contained cookies that allowed the Agency to "follow any visitor across the Web and onto Facebook."[60] The Agency could then use the Custom Audience tool to feed that information into Facebook's systems, matching propagandists with specific Facebook accounts.[61] By "liking" or "sharing" the Agency's posts, users further spread the advertisements to their family and friends.[62] While the Agency's advertisements reached 29 million Facebook users, the total number of users who viewed the Agency's content is at least 126 million, due to users "liking" and "sharing" the content on their own pages.[63]

To this day, it is unknown whether, or how, the influence campaign affected voters and the outcome of the election. Although 126 million may seem like a significant number, the reach of the Russian influence campaign was actually rather small. Between January 2015 and August 2017, Facebook identified "80,000 pieces of divisive content" on Facebook, as well as "120,000 pieces of Russian-linked content" on Facebook-owned Instagram.[64] Nevertheless, when compared with the "11 trillion posts from Pages on Facebook" viewed by users in this same time period, 126 million seems rather inconsequential.[65] In addition, the majority of the Agency's advertisements were viewed after the 2016 election.[66] The DNI Report declined to assess how the influence campaign may have affected the outcome of the election, stating that the intelligence community does not "analyze US political processes or US public opinion."[67]

---

[57] *See* Dwoskin et al., *supra* note 3. (". . .very successful click gives them more data that they can use to retarget. It feeds on itself it spends up the influence dramatically").

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] Mike Isaac & Daisuke Wakabayashi, *Russian Influence Reached 126 Million Through Facebook Alone*, N.Y. TIMES (Oct. 30, 2017), https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html [http://perma.cc/9GL7-4JXH].

[64] *Id.*

[65] *Id.*

[66] Dwoskin et al., *supra* note 3.

[67] DNI REPORT, *supra* note 6, at i.

II. RUSSIAN INFLUENCE CAMPAIGN AS A VIOLATION OF DOMESTIC AND INTERNATIONAL LAW

The Facebook influence campaign can be analyzed under both domestic and international law theories. As explained below, the Facebook influence campaign likely violated U.S. domestic law, but failed to violate international law.

A. Domestic Legal Framework

The influence campaign can plausibly be considered a violation of a number of U.S. laws. Mueller's February 2018 indictment charged the Agency and Agency employees with Conspiracy to Defraud the United States ("Count 1") and Conspiracy to Commit Wire Fraud and Bank Fraud ("Count 2") based on the defendants' involvement in the influence campaign.[68] Additionally, the Facebook influence campaign likely violated the Federal Election Campaign Act ("FECA"), the Foreign Agent Registration Act ("FARA"), and the U.S. anti-hacking statute, the Computer Fraud and Abuse Act ("CFAA"). The basis for the FECA, FARA, and CFAA violations are discussed herein.

Mueller's February 2018 indictment accused the Agency, Agency financier Prigozhin, Prigozhin's two companies that funded the Agency, and 12 Agency employees with "carrying out a massive fraud against the American government and conspiring to obstruct enforcement of federal laws."[69] Facebook is mentioned more than any other social media platform in the indictment.[70] The indictment specifically references the Facebook influence campaign by the Agency's name for it: the "translator project."[71] Specific to the influence campaign over social media, the indictment alleges:

> From at least April 2016 through November 2016, Defendants and their co-conspirators, while concealing their Russian identities and Internet Research Agency affiliation through false personas, began to produce, purchase, and post advertisements on U.S. social media and other online sites expressly advocating for the election of then-candidate Trump or

[68] Indictment at 6, United States v. Internet Research Agency LLC et al., No. 1:18-cr-00032-DLF (D.C. Cir. filed Feb. 16, 2018).

[69] Matt Apuzzo & Sharon LaFraniere, *13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign*, N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html [http://perma.cc/3XK4-DBZN].

[70] Frenkel & Benner, *supra* note 31 (noting that Facebook and Facebook-owned Instagram were mentioned in the indictment 41 times, while "Twitter was referred to nine times, Youtube once and . . . PayPal 11 times").

[71] Indictment at 4, 30, United States v. Internet Research Agency LLC et al., No. 1:18-cr-00032-DLF (D.C. Cir. filed Feb. 16, 2018).

> expressly opposing Clinton. Defendants and their co-conspirators did not report their expenditures to the Federal Election Commission, or register as foreign agents with the U.S. Department of Justice.[72]

Thus, though the indictment expressly charges Conspiracy to Defraud the United States and Conspiracy to Commit Wire Fraud and Bank Fraud,[73] it also suggests that defendants' involvement with the Facebook influence campaign could constitute violations of FECA and FARA.

FECA "prohibits foreign nationals from making any contributions, expenditures, independent expenditures, or disbursements for electioneering communications."[74] Further, FECA "requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission [('FEC')]."[75] Thus, the Agency's purchase of advertisements likely qualifies as a violation of FECA because the purchased advertisements "expressly advocated" for then-candidate Trump and the expenses were never reported to the FEC.

FARA requires that "agents of foreign principals (which includes foreign non-government individuals and entities). . .submit periodic registration statements containing truthful information about their activities and the income earned from them."[76] FARA keeps the U.S. government and U.S. citizens informed of "the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law."[77] Given that the Agency and Agency employees failed to disclose their operations, the Facebook influence campaign likely constitutes as a violation of FARA.

Though not mentioned in the indictment, the influence campaign could plausibly violate the U.S. anti-hacking statute, the Computer Fraud and Abuse Act ("CFAA"). Under 18 U.S.C. §1030(a)(2)(C), the Facebook influence campaign "exceeded authorized access" to a protected computer.[78] To exceed the permissible scope of access and violate the CFAA, the Agency had to breach Facebook's user agreement. In a blog post on Facebook's website, Elliot Schrage, the Vice President of Policy and Communications for Facebook, stated that many of the Agency's advertisements "did not violate" Facebook's "content policies."[79] Nevertheless, the underlying fake accounts used to purchase these otherwise legitimate advertisements

---

[72] *Id.* at 19.

[73] *Id.* at 4, 30.

[74] *Id.* at 11.

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] Computer Fraud and Abuse Act, 18 U.S.C. §1030(a)(2)(C) (2018).

[79] Elliot Schrage, *Hard Questions: Russian Ads Delivered to Congress*, FACEBOOK NEWSROOM (Oct. 2, 2017), https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress/ [http://perma.cc/ZT5Q-RZVH].

represent a violation of Facebook's user agreement at the time of the influence campaign, the Statement of Rights and Responsibilities ("the Statement").[80]

Facebook users agreed to the Statement by "using or accessing Facebook services."[81] The fourth provision of the Statement governed Registration and Account Security. Under this provision, the Statement dictated: "You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission."[82] By creating fake accounts, the Agency clearly violated this provision. An additional sub-provision under Registration and Account Security prohibited "creating more than one personal account."[83] Since Agency employees each managed more than one fake account, the influence campaign likely violated this provision as well.

The Agency's conduct also violated provision three, Safety. Under Safety, the Statement required that advertisers did not "collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without prior permission."[84] By using cookies to track users' conduct outside of Facebook, and then employing that information in targeting these users on the Custom Audience feature, the Agency violated this provision. The Agency clearly violated another sub-provision under Safety: "You will not facilitate or encourage any violations of this Statement or our policies."[85] By controlling the creation of thousands of advertisements spread over hundreds of fake accounts, the Agency clearly facilitated violations of the aforementioned sub-provisions under Registration and Account Security.

The indictment of the Agency and Agency employees strongly suggests that the Facebook influence campaign violated U.S. domestic laws; namely conspiracy laws, FECA, and FARA. Analysis of the CFAA further indicates that the Facebook influence campaign could also qualify as violation of this statute.

B. International Legal Framework

Although the Facebook influence campaign constitutes a violation of domestic law, it nonetheless fails to breach international law. The Facebook influence campaign cannot be considered an armed attack, primarily because

[80] *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms. The Statement has since changed and is now called the Facebook Terms of Service [http://perma.cc/9ME2-C8TN].

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

the physical harm was minimal and the cyberattack failed to produce any physical consequences. The influence campaign was not a use of force under the U.S. definition because it did not involve military attacks or armed violence. Further, the influence campaign did not violate the norm of nonintervention because it was not sufficiently coercive. Finally, the influence campaign did not infringe on U.S. sovereignty because it failed to interfere with or usurp an inherent government function.

1. Armed Attack and Use of Force

There is little basis for characterizing the influence campaign as an armed attack or a use of force. To qualify the Russian influence campaign as an armed attack would be inconsistent with the traditional understanding of an armed attack as the "most grave form of the use of force."[86] An effects-based approach is generally used to determine whether an armed attack has occurred.[87] There are two effects-based tests to evaluate whether a cyber-attack rises to the level of an armed attack: the Schmitt test and the Silver test.

Schmitt's test contains six factors used to assess the effects of a cyberattack in determining whether it qualifies as an armed attack:

> (1) severity: the type and scale of the harm; (2) immediacy: how quickly the harm materializes after the attack; (3) directness: the length of the causal chain between the attack and the harm; (4) invasiveness: the degree to which the attack penetrates the victim state's territory; (5) measurability: the degree to which the harm can be quantified; and (6) presumptive legitimacy: the weight given to the fact that, in the field of cyber-activities as a whole, cyber-attacks constituting an armed attack are the exception rather than the rule.[88]

Using Schmitt's test, it is evident that the influence campaign does not qualify as an armed attack. The influence campaign was not especially severe because it did not result in any physical harm or physical consequences.[89] Because it has not been proven that the influence campaign affected the outcome of the election, the only harm that resulted from the campaign was the spread of divisive content over social media. The most severe element of the harm stems from the fact that the content was promoted by a foreign state with ill intentions: to usurp the American democratic process, spread division, and foster mistrust. Nevertheless, Facebook users viewing and

---

[86] Oona Hathaway & Rebecca Crootof, *The Law of Cyberattack*, 100 CALIF. L. REV. 817, 847 (2012) (quoting Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 191 (June 27)).

[87] *Id.*

[88] *Id.*

[89] *Id.* (interpreting severity according to the "type and scale of the harm").

sharing the content were unaware of the content's sponsor and the poster's intentions. As such, the content of the postings themselves and the division they caused amongst Facebook users represents the harm at issue here, especially considering that the majority of content was posted after the election. Given that America is a country that values the freedom of speech, divisive political content is posted on social media regularly and argued over by those with differing political views. Thus, assuming that the influence campaign did not affect the outcome of the election, the harm was rather small.

The remaining five factors similarly fail to support the conclusion that the influence campaign qualifies as an armed attack. The harm was not immediate: the influence campaign lasted over a period of two years. There is a strong causal link between the attack (posting of divisive content on Facebook with the intent to influence the election and cause conflict) and the harm that divisive content over social media creates. But, as discussed, this harm was not severe. If one argues that the harm is distrust in the media resulting from the campaign, the causal link is very weak. The attack was also minimally invasive: it had no physical effects on U.S. territory and did not significantly alter the U.S. electoral process. The influence campaign was conducted entirely over social media and, though directed at U.S. citizens, could have reached Facebook users around the world. The harm resulting from the influence campaign is extremely difficult to quantify. On a personal level, it is nearly impossible to know how viewing the sponsored content affected individual voters. On a larger scale, it is similarly difficult to assess how the divisive content affected America's perception of the candidates, social issues, and the media itself. The final factor notes that armed attacks are the "exception and not the rule." Given the minimal effects of the influence campaign as indicated by the first five factors, the Facebook influence campaign does not qualify as an armed attack.

Daniel Silver, the former General Counsel of the CIA and the NSA, has dictated another effects-based test for evaluating whether a cyberattack constitutes an armed attack. The Silver test is two-fold: it assesses the severity of the cyberattack and the foreseeability of the consequences.[90] Under Silver's test, a cyberattack is only sufficiently severe if it causes physical injury or property damage.[91] The second prong, foreseeability, is met only if the foreseeable consequence of the cyberattack is "to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion."[92] Because no physical injury or harm to property resulted from the influence campaign, neither the first nor the

[90] *Id.* at 848.

[91] *Id.*

[92] *Id.*

second prong is met. Thus, the influence campaign also fails to qualify as an armed attack under Silver's test.

The Facebook influence campaign similarly fails to qualify as a use of force under Article 2(4) of the UN Charter. Article 2(4) states, "All Members 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."[93] The U.S. considers "use of force" as "military attacks or armed violence."[94] Thus, under the U.S. view, the Facebook influence campaign clearly fails to qualify as a use of force. Additionally, Harold Koh, the former legal adviser for the Department of State, noted that "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[95] Because the Facebook influence campaign did not cause any of these consequences, the Department of State would not characterize it as a use of force.

To this day, "no state has claimed that a cyber-attack constitutes an 'armed attack. Nor has any state argued that cyber-attacks generally constitute a prohibited use of force."[96] Given the relatively minimal physical harm resulting from the Facebook influence campaign, it would be unprecedented to consider it an armed attack or a use of force under generally accepted definitions.

2. Norm of Nonintervention

The Facebook influence campaign similarly fails to qualify as a violation of the norm of nonintervention. Rule 66, Intervention by States, of the Tallinn Manual 2.0 ("Tallinn 2.0") notes that "[a] state may not intervene, including by cyber means, in the internal or external affairs of another State."[97] A violation of the norm of nonintervention constitutes a breach of international law, and allows the injured state to take countermeasures against the attacker.

To qualify as unlawful, the intervention must be "coercive" and must bear "on matters in which each State is permitted, by the principle of sovereignty,

---

[93] U.N. Charter art. 2, ¶ 4.

[94] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 427 (2011).

[95] Harold Koh, Speech at the U.S. Cyber Command InterAgency Legal Conference (Sept. 18, 2012) (transcript available at Chris Borgen, *Harold Koh on International Law in Cyberspace*, OPINIO JURIS) (Sept. 19, 2012, 10:01 AM), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/ [http://perma.cc/72AH-WF4Y].

[96] Hathaway & Crootof, *supra* note 86, at 840.

[97] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE LAW APPLICABLE TO CYBER OPERATIONS 312 (2d ed., Cambridge Univ. Press 2017) [hereinafter TALLINN MANUAL 2.0].

to decide freely."[98] Sufficient coercion is an affirmative act "designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State."[99] Unlawful intervention on matters reserved to the target state include "coercive cyber acts by a State that are intended to eliminate or limit"[100] another state's "choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[101] Further, "cyber means that are coercive in nature may not be used to alter or suborn modification of another State's governmental or social structure."[102]

Under this definition, the influence campaign seemingly could qualify as a violation of nonintervention. The Agency, backed by Russia, created fake Facebook accounts and purchased politically charged advertisements intending to influence the outcome of a U.S. election. The electoral process is certainly a matter reserved to the United States. The issue thus lies with whether the influence campaign was sufficiently coercive.

The majority of Tallinn experts agree that propaganda does not satisfy coercion for the purposes of nonintervention.[103] The Facebook influence campaign constitutes "propaganda" within the meaning of the Tallinn Manual. Tallinn experts find that propaganda does not rise to the level of coercion because there is a difference between "influencing" and "factually compelling" the target actions of the State.[104] Tallinn 2.0 gives the specific example that "a State-sponsored public information campaign via the Internet designed to persuade another State of the logic of ratifying a particular treaty would not amount to a violation of the prohibition of intervention."[105] There are obvious parallels to this hypothetical and the Russian influence campaign over Facebook. As such, it seems unlikely that a State-sponsored information campaign via the internet designed to persuade another State to support a particular presidential candidate or political views would amount to a violation of nonintervention.

Nevertheless, a few experts argued that in situations involving propaganda, "the context and consequences of a particular act that would not normally qualify as coercive could raise it to that level."[106] This view promotes an effects-based test to suggest that if the consequences of a cyber operation are sufficiently intrusive and harmful, it could be considered a violation of

[98] *Id.* at 315. *See also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 205 (June 27).

[99] TALLINN MANUAL 2.0, *supra* note 97, at 318.

[100] *Id.* at 318-19.

[101] Nicar. v. U.S., 1986 I.C.J. at 108, ¶ 205.

[102] TALLINN MANUAL 2.0, *supra* note 97, at 315.

[103] *Id.* at 318-19.

[104] *Id.*

[105] *Id.* at 319.

[106] *Id.*

international law. Applying this logic to the influence campaign, we then turn again to the harm caused.

As previously discussed, the harm resulting from the influence campaign was minimal. If there existed concrete evidence that the influence campaign affected the outcome of the 2016 U.S. election, the analysis would look quite different. Barring this evidence, the only real harms that resulted from the influence campaign were the spread of "fake news," the potential increase in political division, and increased distrust in the American democratic system. Consequently, the harms are likely not severe enough to qualify as a violation of nonintervention.

Scholar Michael Schmitt, one of the leading authors of the Tallinn Manual and an expert in cybercrime, previously suggested that the Russian "hacking campaign" constituted a violation of the norm of nonintervention.[107] Schmitt rolled back this assertion in a recent article on the topic, wherein he concluded that the Russian influence campaign likely did not violate nonintervention.[108] Nevertheless, Schmitt suggested herein that the most compelling base for a nonintervention violation rests in the "covert nature of the troll operation" that constrained Americans' freedom of choice because voters could not accurately evaluate where the information came from – "[t]he deceptive nature of the trolling is what distinguishes it from a mere influence operation."[109] This theory falls within the minority view of the Tallinn experts, essentially alleging that the covert nature of the Facebook influence campaign allows it to "rise to the level" of coercion, when coercion would otherwise not be present.[110] Schmitt admitted, however, that this conclusion is "by no means unassailable" because it is unclear whether the Facebook influence campaign actually caused a difference in election results.[111]

3. Violation of U.S. Sovereignty

The final possibility is to consider the influence campaign as a violation of US sovereignty. Tallinn 2.0 supports the prevailing definition of sovereignty, qualifying it as a norm of international law from which derogation is not permitted.[112] As such, a violation of sovereignty is considered on par with

[107] Morgan Chalfant, *Democrats Step Up Calls that Russian Hack was Act of War*, THE HILL (Mar. 26, 2017), https://thehill.com/policy/cybersecurity/325606-democrats-step-up-calls-that-russian-hack-was-act-of-war [https://perma.cc/Q4MV-H95P].

[108] *See* Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHICAGO J. INT'L L. 30, 50 (2018).

[109] *Id.* at 51.

[110] *Id.*

[111] *Id.* at 51-52.

[112] *See* Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AM. J. INT'L L. UNBOUND 213, 214 (2017).

violations of other norms of international law, such as non-intervention. Tallinn 2.0 states that remote cyber operations can violate a state's sovereignty based on the "degree of infringement upon the state's territorial integrity" and whether the infringement interferes with or usurps an inherent governmental function.[113] Remote cyber operations causing physical damage or resulting in a sufficient loss of functionality to an inherent governmental function constitute a violation of sovereignty under the Tallinn view.[114] There is no precise threshold defining a "sufficient" loss of functionality in assessing whether a remote cyber operation constitutes a violation of sovereignty.[115]

As the Facebook influence campaign did not cause physical damage, whether the campaign can be considered a violation of sovereignty rests on if it caused a sufficient loss of functionality. First, it is unclear whether the Facebook influence campaign even caused a loss of functionality. Though promulgated using fake Facebook accounts, the Facebook influence campaign employed Facebook's advertising service exactly as it was intended to be used. The divisive content was posted in users' Facebook feeds along with other legitimate advertisements and posts. The content of the posts themselves do not violate Facebook's user agreement. The potential loss of functionality comes from the tracking software implemented on users' computers prior to accessing Facebook or after clicking on one of the Agency's advertisements and being directed to an outside platform. As such, with respect to Facebook specifically, it is questionable whether a loss of functionality, let alone a sufficient loss of functionality, occurred.

Even assuming there was a loss of functionality, the influence campaign likely did not interfere with or usurp an inherent government function. Usurpation "involves performing an inherently governmental function on another State's territory without its consent."[116] Interference includes actions "that disturb the territorial State's ability to perform the functions as it wishes."[117] The U.S. electoral process unquestionably counts as an inherent government function.[118]

An interference theory is most plausible here. The Facebook influence campaign could be considered an action that disturbed the U.S.'s ability to run its electoral process as it wished. Nevertheless, "merely engaging in election propaganda does not amount to election interference, at least as a

---

[113] *Id.* at 215.

[114] *See id.*

[115] Ahmed Ghappour, *Tallinn, Hacking, and Customary International Law*, 111 AM. J. INT'L L. UNBOUND 224, 225 (2017).

[116] Schmitt, *supra* note 108, at 45.

[117] *Id.* at 45-46.

[118] *Id.* at 45.

matter of law."[119] Thus, the Facebook influence campaign likely does not constitute a violation of sovereignty.

Schmitt opined that the Facebook influence campaign could potentially be considered a violation of sovereignty because the Agency hackers "created fake identities in which they masqueraded as Americans," thus feigning the true source of the disinformation.[120] Again, Schmitt focused on the covert nature of the Facebook influence campaign in suggesting that it could qualify as a breach of international law. In Schmitt's opinion, an "open propaganda campaign, even one involving disinformation" would not constitute a violation of international law, whereas the Facebook influence campaign could.[121] Nevertheless, Schmitt again qualified that this conclusion is "far from unassailable" mainly because the Russians avoided taking actions that would plainly constitute interference.[122]

While the Facebook influence campaign violated U.S. domestic laws, it failed to breach international law. The Facebook influence campaign fails to qualify as an armed attack or use of force, and likely does not constitute a violation of nonintervention or of sovereignty. On the nonintervention front, the Facebook influence campaign was not coercive. With respect to sovereignty, the campaign did not cause a loss of functionality or an interference with an inherent governmental function. Though Schmitt presents theories under which the Facebook influence campaign could be considered violations of nonintervention and sovereignty, he recognized that these theories do not concretely show breaches of international law.

III. POLICY IMPLICATIONS OF THE LEGALITY OF THE FACEBOOK INFLUENCE CAMPAIGN

The legality of the Facebook influence campaign has policy implications on both domestic and international law platforms. While the Facebook influence campaign likely qualifies as a violation of domestic law, domestic enforcement is ultimately ineffective and has created intra-branch and inter-branch institutional conflict within the U.S. government. On the other hand, the fact that the influence campaign likely does not qualify as an international law violation leaves us wondering how to handle remote cyber election meddling as a pervasive issue of foreign policy.

This section will first contend that domestic enforcement is an ineffective means of dealing with remote cyber election meddling activities. It will further highlight the problems with criminalizing remote cyber election meddling activities on the international platform. It will finally suggest that

[119] *Id.* at 46.

[120] *Id.* at 46-47.

[121] *Id.* at 46.

[122] *Id.* at 47.

the most effective means of handling remote cyber election meddling activities would be to create an effective international policy framework.

A. Domestic Criminalization

The Mueller investigation is important and has been extremely beneficial in many respects. The February 2018 indictment in particular was very positive in the sense that it credibly "educate[d] the American public about the reality and scale of the Russian threat to the American political process."[123] Nevertheless, domestic criminalization alone is not sufficient to prevent remote cyber election meddling activities and may actually create adverse results.

The Mueller indictment, or any domestic criminalization of the influence campaign, may in fact educate and embolden Russian hackers.[124] While the indictment could create a "small deterrent effect" for prospective hackers, "naming names" will not adequately deter future Russian attacks.[125] Regardless of whether the influence campaign actually changed the outcome of the election, it was wildly successful in many respects. The Russians succeeded in sowing discord and spreading distrust. Consequently, a "rational Russia would see the tiny costs imposed by the Mueller indictment as very much worth the benefits it reaped in American politics."[126]

While the indictment clearly attributed the influence campaign to Russia, the United States has failed to publicly respond to that claim.[127] The lack of a U.S. response to the indictment's attribution charge shows weakness and vulnerability, potentially inviting future attacks.[128] Again, a "rational Russian" may view the U.S.'s failure to respond as an indication that the United States "is more exposed, and [has] weaker tools of retaliation, than previously thought."[129]

Further, Mueller's indictment may glorify the scope and effect of the influence campaign for Russia. A central element of the success of the influence campaign is that Russia ran the campaign.[130] By credibly describing the influence campaign and its effects and publicly attributing that claim to Russia, the indictment may actually enhance the campaign's impact.

---

[123] Jack Goldsmith, *The Downsides of Mueller's Russia Indictment*, LAWFARE (Feb. 19, 2018), https://www.lawfareblog.com/downsides-muellers-russia-indictment [https://perma.cc/B8CJ-B8TU].

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] *Id.* ("A large part of the operation's success, a central element of its discordant impact, is the fact that *the Russians* did it.")

The Mueller indictment may also reveal U.S. forensic tactics used in gathering the information in the indictment, which "might reveal something about U.S. intelligence collection methods" thereby educating future Russian hackers.[131]

In addition to educating and emboldening Russian hackers, the Mueller indictment could have the same effect on other adversaries.[132] The indictment describes in details the methods used by Russian hackers to "wreak enormous harm on the [United States] at a relatively small cost."[133] This could provide specific inspiration and ideas to other prospective hackers, and could assist adversaries in evading detection by the U.S. government.[134]

The Mueller indictment has also adversely affected the U.S. democratic and political landscape, namely due to Trump's refusal to credit the investigation. Trump has consistently criticized the Mueller investigation, only "rarely" and "begrudgingly" acknowledging Russian hacking – "and when he does, he hastens to emphasize its triviality, meaninglessness."[135] In fact, Trump reflected upon a conversation with Russian President Vladimir Putin regarding the allegations of Russian meddling in the 2016 U.S. election, saying "Every time [Putin] sees me, he says 'I didn't do that.' And I believe, I really believe, that when he tells me that, he means it."[136] Just two days after the February 2018 indictment, Trump tweeted, "I never said Russia did not meddle in the election, I said 'it may be Russia, or China or another country or group, or it may be a 400 pound genius sitting in bed and playing with his computer.' The Russian 'hoax' was that the Trump campaign colluded with Russia – it never did!"[137]

Trump's repeated attempts to undermine the Mueller investigation have created intra-branch institutional conflict between the Department of Justice and the President, as well as inter-branch institutional conflict between the President, who is in charge of foreign policy, and Congress, the organization in charge of enacting domestic laws – including U.S. criminal laws. In a semi-illuminating tweet, Trump noted, "If it was the GOAL of Russia to create discord, disruption and chaos within the U.S. then, with all of the Committee Hearings, Investigations and Party hatred, they have succeeded beyond their

---

131 *Id.*

132 *Id.*

133 *Id.*

134 *Id.*

135 David Remnick, *Mueller's Indictment Ends Trump Myth of the Russia 'Hoax'*, NEW YORKER (Feb. 16, 2018), https://www.newyorker.com/sections/news/muellers-indictments-end-trumps-myth-of-the-russia-hoax [https://perma.cc/EXX8-XAZW].

136 *Id.*

137 Donald J. Trump (@realdonaldtrump), TWITTER (Feb. 18 2018, 4:33 AM), https://twitter.com/realdonaldtrump/status/965202556204003328 [https://perma.cc/2KWW-PF2N].

wildest dreams. They are laughing their asses off in Moscow. Get smart America!"[138] Here, Trump fails to recognize his own contributions to the discord created by his comments on the Mueller investigation and the influence campaign itself. Nevertheless, he is correct in recognizing that the various responses within the U.S. government have served to increase the controversy surrounding the 2016 U.S. election.

B. International Criminalization

Criminalizing remote cyber election meddling activities under international law is similarly ineffective in handling activities such as the Facebook influence campaign. While this paper contends that the Facebook influence campaign did not violate international law, Schmitt indicated that there could be valid bases to consider the campaign as a violation of nonintervention and sovereignty. This section will examine the issues with that proposition.

1. Increased International Conflict

Remote cyber activities will rarely rise to the level of an armed attack,[139] but do have the capacity to fall under other categories of unlawfulness that international law provides for. For example, countermeasures are "acts that would be unlawful if not done in response to a prior international law violation."[140] As such, an injured state could employ countermeasures to counter a use of force, violation of nonintervention, and possibly a violation of sovereignty. Theoretically, in response to a cyberattack that does not meet the armed attack threshold but does meet a different violation threshold, the injured state can respond with non-forceful countermeasures subject to necessity and proportionality.[141] While Tallinn 2.0 offers the prevailing definition of sovereignty—that it constitutes a norm of international law from which derogation is not permitted—a minority view suggests that sovereignty is an underlying principle of international law.[142] Under the Tallinn 2.0 view, a state may employ countermeasures in response to a violation of sovereignty, as a violation of sovereignty is considered an international wrongful act.[143]

Absent urgent situations, an injured state is generally warranted to take

---

[138] Donald J. Trump (@realdonaldtrump), TWITTER (Feb. 18 2018, 5:11 AM), https://twitter.com/realdonaldtrump/status/965212168449941505 [https://perma.cc/5AXH-WEX6].

[139] Hathaway & Crootof, *supra* note 86, at 840.

[140] *Id.* at n.109.

[141] Hathaway & Crootof, *supra* note 86, at 845.

[142] Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207, 208 (2017).

[143] Schmitt & Vihul, *supra* note 112, at 214.

countermeasures only after asking the attacking state to comply with the law, notifying the state of its intention to use countermeasures, and proposing settlement negotiations.[144] If countermeasures are permitted, they "must be targeted at the state responsible for the prior wrongful act and must be temporary and instrumentally directed to induce the responsible state to cease its violation."[145] Countermeasures are not allowed after the international wrongful act has ceased.[146]

In addition, the injured state must accurately attribute the cyberattack in order to engage in countermeasures.[147] Given the complexity of cyberattacks and the widespread use of anonymizing servers, the danger of misattribution is always high. While there is no "explicit" burden of proof for attribution, "international law generally requires that States act reasonably under the circumstances when they gather information and draw conclusions based on that information."[148]

The self-help measures permitted though countermeasures create many opportunities to conduct counter-attacks in response to violations of international law. If remote cyber election meddling activities such as the Facebook influence campaign were considered violations of international law, the number of international law violations would inevitably increase.[149] This increase could exacerbate foreign conflict, warranting states to employ countermeasures against one another on a broader scale. Remote cyber election meddling activities, however, generally fall into the "grey zone" of international law, and many actors likely operate under the assumption that their conduct will not be criminalized. At this time, the law is simply not mature enough to clearly indicate whether these types of attacks fall into a specific violation of international law. As the norms progress and the law advances, it is likely that some type of remote cyber activities will breach international law. Nevertheless, using the Facebook influence campaign as a framework, it is evident that considering this objectively wrong and condemnable conduct as an international law violation is a stretch. To begin doing so could merely increase the number of violations warranting injured states to engage in counter-attacks against attacking states. This could escalate foreign conflicts and result in a never-ending stream of attacks and

144 Hathaway & Crootof, *supra* note 86, at 858.

145 *Id.* at 857.

146 *Id.* at 857-58.

147 *Id.* at 858.

148 Brian Egan, Legal Adviser, U.S. Dep't of State, Remarks on International Law and Stability in Cyberspace 19 (Nov. 10, 2016).

149 Steve Ranger, *Did Russia's Election Hacking Break International Law? Even the Experts Aren't Sure*, ZDNET (Mar. 6, 2017), http://www.zdnet.com/article/did-russias-election-hacking-break-international-law-even-the-experts-arent-sure/ [http://perma.cc/535P-6X72].

counterattacks between states.

However, states likely would not employ countermeasures every time they face an opposing state's breach of a domestic law with the intent to influence an election. The uncertainties associated with attribution may dissuade states from publicly attributing the attack and from employing countermeasures.[150] States risk attribution sounding illegitimate, "especially when faced with denial by the accused country."[151] Though states are not required to reveal evidence underlying attribution, they often face political pressure to do so.[152] An injured state may not want to reveal the tools used to discover the alleged infringement, as doing so could give away details about the injured state's own cybersecurity mechanisms. As such, public attribution and taking countermeasures may not be a wise policy choice for many states.

Additionally, countermeasures are not warranted after the cyberattack has ceased.[153] In cases of cyber election meddling, the injured state may not be able to discover the violation, conduct a full-fledged investigation, and attribute the attack while it is ongoing. Assuming the injured state is unable to do so, the injured state would not be warranted to take countermeasures against the adversary state.

2. Change in U.S. Foreign Policy

Despite the fact that states may not always choose to engage in countermeasures, the risk of increasing the number of international conflicts could be particularly disadvantageous for the United States. The United States may hesitate to take countermeasures in the face of a cyberattack. Our democratic framework would likely result in high political pressure to back up public attribution. Other countries—Russia likely included—may not face the same policy implications. Thus, other countries may not hesitate to take countermeasures against the United States, though we may refrain from engaging in countermeasures in similar situations. Consequently, increasing the number of cyberattacks that count as international law violations may have an adverse impact on U.S. foreign policy, while presenting a golden opportunity for other countries.

Additionally, Russia is not the only country engaged in foreign election hacking. The United States is guilty of election meddling as well.[154] If remote cyber election activities such as the Facebook influence campaign constituted a breach of international law, the United States would have to refrain from

---

150 Ghappour, *supra* note 115, at 227.

151 *Id.*

152 *Id.*

153 Hathaway & Crootof, *supra* note 86, at 858.

154 Scott Shane, *Russia Isn't the Only One Meddling in Elections. We Do It, Too.*, N.Y. TIMES (Feb. 17, 2018), https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html [http://perma.cc/AFP6-ULJY].

employing its own techniques to interfere with foreign elections, or at least would face greater consequences for doing so. Though Russia used technologically advanced means to influence the 2016 election, the United States has used classic intelligence tactics to intervene in foreign elections going back as far as 1946.[155] Despite the controversy surrounding the Russian intervention, Steven L. Hall, the former chief of Russian operations at the C.I.A., stated: "If you ask an intelligence officer, did the Russians break the rules or do something bizarre, the answer is no, not at all."[156] Further, Loch K. Johnson, an American intelligence scholar, noted that "Russia's 2016 operation was simply the cyber-age version of standard United States practice for decades, whenever American officials were worried about a foreign vote."[157]

Though American interference is generally motivated by purer motivations than Russian interference,[158] America's history of election meddling is well-settled.[159] Thus, the American intelligence community would have to change many of its practices if remote cyber election meddling activities such as the Facebook influence campaign breached international law. In doing so, the United States could lose valuable intelligence opportunities, or might refrain from making a positive change in a foreign country fearing international sanctions.

C. Necessity of an Effective Policy Framework

Neither domestic nor international criminalization provide an effective means of handling remote cyber election meddling activities from a policy perspective. Nevertheless, the effects of these activities cannot be taken lightly. Instead, an international policy framework would provide the best way forward for dealing with this pervasive issue.

The results of the Russian influence campaign may never be adequately measured, but it is fair to say that the campaign caused public controversy, distrust in politics, the democratic system, and the media. While this paper focused specifically on the Facebook influence campaign, the influence campaign conducted for the 2016 U.S. election also spanned social networks such as Instagram, Twitter, and Google.[160] Furthermore, Russia's interference was not limited to the influence campaign alone. Russia is also

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.* (noting that American election interference is normally motivated by "helping non-authoritarian candidates challenge dictators or otherwise promoting democracy," while Russia "has more often intervened to disrupt democracy or promote authoritarian rule").

[159] Shane, supra note 154.

[160] Isaac & Wakabayashi, *supra* note 63.

charged with facilitating the DNC Hack using spear phishing techniques[161] and currently faces allegations of collusion with top American political leaders—including President Trump himself.[162] Despite the ongoing controversy surrounding Russia's interference in the 2016 election, Russia is also faced with allegations of running an influence campaign to interfere in the 2018 U.S .midterm elections.[163]

Additionally, the U.S. is not the only country that has been targeted by Russian influence campaigns. Russia has been accused of conducting another influence campaign prior to the 2017 French election between Marine Le Pen (Russia's pick) and Emmanuel Macron.[164] Before the election, Kremlin-controlled news sources Russia Today (RT) and Sputnik reported that Macron was secretly gay, and that he was backed by a "very rich gay lobby."[165] Sputnik also accused Macron of being a "U.S. agent lobbying banks' interests."[166]

Russia also faces allegations of cyber election interference in Ukraine, Germany, Bulgaria, and the Vienna-based Organization for Security and Cooperation in Europe.[167] A few days before the 2014 parliamentary elections in Ukraine, hackers conducted a denial of service attack and against Ukraine's Central Election Commission and attempted to fake the election results.[168] In 2015, Germany accused Russia of hacking and stealing data from computers belonging to House of Parliament members.[169] German intelligence identified the hacker as Sofacy, a group associated with

---

[161] Bump, *supra* note 24.

[162] Philip Bump, *Trump and the White House Have Denied Russian Collusion More than 140 Times*, WASH. POST (Jan. 11, 2018), https://www.washingtonpost.com/news/politics/wp/2018/01/11/trump-and-the-white-house-have-denied-russian-collusion-more-than-140-times/?utm_term=.eac08a632949 [http://perma.cc/GED2-TALC].

[163] DANIEL R. COATS, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 11 (2018) ("The 2018 US mid-term elections are a potential target for Russian influence operations. . . We assess that the Russian intelligence services will continue their efforts to disseminate false information via Russian state-controlled media and covert online personas about US activities to encourage anti-US political views").

[164] Andrew Higgins, *It's France's Turn to Worry About Election Meddling by Russia*, N.Y. TIMES (Apr. 17, 2017), https://www.nytimes.com/2017/04/17/world/europe/french-election-russia.html?mcubz=3 [http://perma.cc/NV6U-BT8A].

[165] *Id*.

[166] *Id*.

[167] Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA TODAY (Jan. 9, 2017), https://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/ [https://perma.cc/4KV7-SBYB].

[168] *Id*.

[169] *Id*.

Russia.[170] The German chancellor Angela Merkel said she "could not rule out Russian interference in Germany's 2017 federal election through internet attacks and disinformation campaigns."[171] Also in 2015, Bulgaria's Central Election Commission experienced a hack "almost certainly linked to Russia."[172] In November 2016, the OSCE, an organization that monitors European elections, experienced a "major security information incident" that "compromised [] confidentiality."[173] This cyberattack was attributed to the Russian hacking groups Fancy Bear and Sofacy.[174]

This paper considers various domestic and international law theories to assess the legality of the Facebook influence campaign, concluding that the Facebook influence campaign likely violated domestic law but not international law. Nevertheless, domestic law enforcement is not sufficient to prevent remote cyber election meddling activities in the future because it may cause conflict and glorify the adversary's actions. Similarly, international criminalization would not effectively handle the foreign policy issues of remote cyber election meddling activities. If, for example, the Facebook influence campaign did qualify as a breach of international law, the risk of conflict escalation between states would be severe. U.S. foreign policy would be negatively impacted because states would not face the same restraints that would prevent the United States from combatting influence campaigns. At the same time, however, this paper illustrates the pervasive problem of cyberattacks with the intent to influence elections. Rather than outlawing this behavior outright, it would be more helpful to develop a policy framework to deal with these infractions on the international law platform.

170 *Id.*

171 *Id.*

172 *Id.*

173 *Id.*

174 *Id.*