ELECTION INTERFERENCE UNDER INTERNATIONAL LAW

JULIA BROOKS*

I. INTRODUCTION

"The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion," wrote Special Counsel Robert S. Mueller, III in his report on Russian interference in the 2016 U.S. presidential election (Mueller Report).[1] As the report outlines, this assertion was based on two principal facts. First, the Internet Research Agency (IRA), a Russian government-linked organization, "carried out a social media campaign that favored presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton."[2] These operations were "designed to provoke and amplify political and social discord in the United States," in what the IRA termed "information warfare."[3] Second, the Russian intelligence service carried out "cyber intrusions (hacking) and releases of hacked materials damaging to the Clinton Campaign."[4] Russian intelligence units also targeted U.S. election systems themselves, separately hacking "computers belonging to state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections."[5] Similarly, according to a report from the U.S. Senate Intelligence Committee, Russia targeted election systems in all fifty states,[6] clearly violating U.S. law.[7] Important for the purposes of this annotation, however, is determining international law's applicability. This annotation, therefore, will analyze Russia's interference through the lens of international law and seek to answer whether its actions in the 2016 U.S. election fall under international law prohibitions against the use of force as applied to cyber operations, as well as whether these actions constitute infringements of state sovereignty and the principle of non-intervention.

* This online annotation was written in the course of the author's tenure as a Staff Editor on the *N.Y.U. Journal of International Law & Politics*.

1 1 ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION, at 1 (2019) [hereinafter MUELLER REPORT].

2 *Id.* at 1, 4.

3 *Id.* at 4.

4 *Id.*

5 *Id.* at 37.

6 1 S. COMM. ON INTELLIGENCE, REP. ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, S. DOC. NO. 116-XX, at 12 (1st Sess. 2019) [hereinafter SENATE INTELLIGENCE REPORT]; *see also* David E. Sanger & Catie Edmondson, *Russia Targeted Election Systems in All 50 States, Report Finds*, N.Y. TIMES (July 25, 2019), https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html (reporting and analyzing the Senate Intelligence Committee report).

7 Indictment at 2–3, United States v. Internet Research Agency LLC, et al., No. 1:18-cr-00032-DLF, 2018 WL 914777 (D.D.C. Feb. 16, 2018) [hereinafter IRA Indictment].

II. AN ACT OF (CYBER) WAR?

As more details of the Russian interference in the 2016 election came to light, a bipartisan array of U.S. political officials publicly referred to it as an "act of war."[8] Although perhaps pure political theater, as election interference of this type is a far cry from the traditional notion of war as armed conflict—or physical violence involving the use of armed force between states—it nevertheless raises the question of whether and how emerging concepts of *cyberwarfare* apply.

Traditional international law regulating the resort to war by states (*jus ad bellum*) centers around the general prohibition on the use of force enshrined in Article 2(4) of the U.N. Charter. Article 2(4) stipulates that all member 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."[9] Election interference could be considered an infraction against a nation's *political independence*, considering the integral role of elections to the political functioning of a democracy, but this would be a novel interpretation.

Even assuming election interference did constitute a breach of a nation's political independence, the question of what constitutes *force* in the cyber context still remains. The *Tallinn Manual 2.0*—a nonbinding, though useful, study on the applicability of international law to cyber operations—concludes that cyber operations could constitute uses of force in violation of the prohibition, provided that their "scale and effects are comparable to non-cyber operations rising to the level of a use of force."[10] Given the lack of an authoritative definition of "use of force" under international law, there is no easy answer here, but the *Tallinn Manual 2.0* points to a number of factors that states are likely to consider in assessing whether force was used, including the action's severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[11]

Taking into account these factors and definitional ambiguities, there is no absolute consensus on whether Russia's actions constituted an act of

8 *E.g.*, Morgan Chalfant, *Democrats Step up Calls that Russian Hack Was Act of War*, HILL (Mar. 26, 2017), https://thehill.com/policy/cybersecurity/325606-democrats-step-up-calls-that-russian-hack-was-act-of-war; John Haltiwanger, *Russia Committed Act of War with Election Interference, Nikki Haley Says*, NEWSWEEK (Oct. 19, 2017), https://www.newsweek.com/russia-committed-act-war-election-interference-nikki-haley-says-688518.

9 U.N. Charter art. 2, ¶ 4.

10 TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 330 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0]. The *Tallinn Manual 2.0* updates and expands the 2013 Tallinn Manual, and was written by an International Group of Experts under the direction of Professor Michael N. Schmitt, and facilitated and led by the NATO Cooperative Cyber Defense Centre of Excellence. *Id.* at xii, 1. It does not have the force of law, though is a leading interpretative guide on the applicability of international law to cyber operations. *Id.* at 2–3.

11 *Id.* at 331, 333–37.

war under international law. Former Central Intelligence Agency Director Michael Hayden has cautioned against labeling Russian election interference as an "act of war."[12] Michael Schmitt, director of the *Tallinn Manual* project, has also rejected the notion that this interference constitutes warfare, labeling it instead as "asymmetrical lawfare" in a "grey zone" of international law.[13] Indeed, the *Tallinn Manual 2.0* itself concludes that "cyber psychological operations intended solely to undermine confidence in a government . . . [do not] qualify as uses of force," since the scale and effects of such operations are unlikely to be comparable to non-cyber operations rising to the level of a use of force.[14]

III. STATE SOVEREIGNTY AND NON-INTERVENTION

Given some of the difficulties of applying the use of force framework to cyber operations, many commentators have preferred to focus on election interference as a violation of state sovereignty and the principle of non-intervention, foundational principles that undergird the general prohibition on the use of force. The U.N. General Assembly reaffirmed the principle of non-intervention in 1965, declaring that "[n]o State has the right to intervene, directly or indirectly, for any reason whatever, in the internal . . . affairs of any other State," and that "[e]very State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State."[15] The International Court of Justice (ICJ) also weighed in when it explained in *Nicaragua v. United States of America* that the principle of non-intervention "is part and parcel of customary international law,"[16] and "forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States."[17]

Similarly, the *Tallinn Manual 2.0* also concludes that interference may occur by cyber means, "for example, by using cyber operations to remotely alter electronic ballots and thereby manipulate an election."[18] While Russian actions involving the 2016 U.S. election appear to have stopped short of actually altering ballots, they undoubtedly had a significant impact: The Mueller Report concluded that Russian military units hacked "computers belonging to state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections."[19] Indeed, the U.S. Senate Intelligence

12 Morgan Chalfant, *Former CIA Director: Don't Call Russian Election Hacking 'Act of War,'* HILL (Apr. 11, 2017), https://thehill.com/policy/cybersecurity/328344-former-cia-director-dont-call-russian-election-hacking-act-of-war.

13 Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. 1, 3 (2017).

14 TALLINN MANUAL 2.0, *supra* note 10, at 331.

15 G.A. Res. 2131 (XX), at 2 (Dec. 21, 1965).

16 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27).

17 *Id.* at ¶ 205.

18 TALLINN MANUAL 2.0, *supra* note 10, at 313.

19 MUELLER REPORT, *supra* note 1, at 37.

Committee reported that Russia targeted election systems in all fifty states, and "may have been probing vulnerabilities in voting systems to exploit later."[20]

While the drafters of the *Tallinn Manual 2.0* do not speak directly to the type of social media influence campaigns or hacking and release of damaging materials employed in Russia's 2016 hacking, such actions may still constitute unlawful interference. Under *Nicaragua*, an intervention is unlawful when it falls within another State's *domaine réservé* (reserved domain, i.e., strictly internal affairs) and uses methods of *coercion*.[21] Considering that the ICJ recognizes that a state should decide freely its political system,[22] the more difficult question is what constitutes *coercion*. Here, views are divided. Jens David Ohlin argues, for instance, that the 2016 election interference was not necessarily coercive, given the difficultly of defining clear targets of coercion or directly compelled acts.[23] However, others point to the cumulative effect of the intrusions in potentially altering the course of the election, as well as the vital nature of state interests at stake, to argue that the interference was indeed coercive.[24] As Steven J. Barela writes, "'coercion' . . . revolves around understanding the potentially paralyzing effects of targeting and eroding [the] legitimacy" of U.S. democracy and elections.[25] This argument draws upon the large scale and reach of the Russian "social media campaign that

20 SENATE INTELLIGENCE REPORT, *supra* note 6, at 4, 12; *see also* Sanger & Edmondson, *supra* note 6 (reporting and analyzing the Senate Intelligence Committee report).

21 *See Nicaragua*, 1986 I.C.J. 14, ¶ 205 ("A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.").

22 *Id.*

23 For the argument that the Russian inference did not necessarily constitute coercion, see, e.g., Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1592, 1594 (2017) ("A legal finding of coercion would depend on identifying some individual or group as the target of the coercion. Was it the American voters? Were they coerced into voting for Trump and not for Clinton? If so, what were the threatened consequences? . . . While the Russian hacking was certainly corrosive, it is genuinely unclear whether it should count as coercive.").

24 For different formulations of the argument that the Russian inference did constitute coercion, see, e.g., Steven J. Barela, *Zero Shades of Grey: Russian-Ops Violate International Law*, JUST SECURITY (Mar. 29, 2018), https://www.justsecurity.org/54340/shades-grey-russian-ops-violate-international-law ("My own interpretation of 'coercion,' the pivotal legal term under discussion, revolves around understanding the potentially paralyzing effects of targeting and eroding legitimacy. With this core interest in jeopardy, and all that we have learned and watched over the last 15 months, the case has only become stronger for labelling what happened, and continues to occur, as *coercion*."); Schmitt, *supra* note 13, at 2, 8 (noting that "[i]t is unclear whether facilitating the release of actual e-mails—as distinct from, for example, using cyber means to alter election returns—amounts to coercion as a matter of law," though cyber operations could be considered coercive in the sense that they "manipulated the process of elections and therefore caused them to unfold in a way that they otherwise would not have").

25 Barela, *supra* note 24.

favored . . . Donald J. Trump and disparaged . . . Hillary Clinton," as the Mueller Report documented.[26] While the administration under President Barack Obama did not necessarily interpret Russian interference as a violation of international law, it articulated a similar understanding, noting that "Russia's cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government."[27] Thus, if the election interference is viewed as an effort to "provoke and amplify political and social discord in the United States," as the Mueller report describes it,[28] and not merely as a propaganda campaign, it may constitute unlawful intervention.[29]

Another aspect of Russia's actions that may also bring them within the scope of unlawful intervention in state sovereignty would require the actions to be considered an "interference with or usurpation of inherently governmental functions."[30] Without providing a definitive definition, the drafters of the *Tallinn Manual 2.0* note that "[e]xamples include changing or deleting data such that it interferes with . . . the conduct of elections."[31] Again, this is not exactly what happened in 2016, but the reference to election interference is instructive, in light of the evidence that Russian actors already targeted U.S. election systems in what may have been a step towards directly manipulating such data in the future.[32]

Based on the foregoing, it appears one may make a strong case that Russia's acts in the 2016 U.S. elections constituted at the very least unlawful interference of the United States' sovereignty, if not an outright act of war.

IV. RESPONDING TO VIOLATIONS

26 MUELLER REPORT, *supra* note 1, at 1.

27 Press Release, White House, Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and.

28 MUELLER REPORT, *supra* note 1, at 4.

29 *See* TALLINN MANUAL 2.0, *supra* note 10, at 26 ("With regard to propaganda, the International Group of Experts agreed that its transmission into other States is generally not a violation of sovereignty. However, the transmission of propaganda, depending on its nature, might violate other rules of international law. For instance, propaganda designed to incite civil unrest in another State would likely violate the prohibition of intervention (Rule 66).").

30 *Id.* at 20. According to the *Tallinn Manual 2.0*:

> The second basis upon which the Experts determined a violation of sovereignty occurs is when one State's cyber operation interferes with or usurps the inherently governmental functions of another State. This is because the target State enjoys the exclusive right to perform them, or to decide upon their performance. It matters not whether physical damage, injury, or loss of functionality has resulted or whether the operation qualifies in accordance with the various differing positions outlined above for operations that do not result in a loss of functionality.

Id. at 21–22.

31 *Id.* at 22.

32 *See supra* note 20 and accompanying text.

Russian actions in relation to the 2016 U.S. election raise a number of questions about the applicability and limits of international law. Even assuming Russia's actions constituted breaches of international law, as argued above, a more fundamental question remains: How can the United States respond to such a violation?

To be sure, the United States has already taken a number of measures to respond to the election interference. The U.S. Congress is currently considering measures to enhance election security, including funding fortification of U.S. election systems against future outside interference.[33] While such measures may be insufficient to address the scale of the vulnerabilities,[34] they are a start. The U.S. Department of Justice has also indicted thirteen Russian individuals and companies on federal criminal charges related to the election interference.[35] The United States has also instituted a variety of sanctions against certain Russian individuals and entities linked to the 2016 election interference, expelled suspected Russian intelligence operatives from the country, and shuttered compounds used for Russian intelligence activities in the United States[36] These measures, which can be considered retorsions, are all within the United States' legal prerogative, irrespective of whether Russia violated international law.

The Obama administration, however, stopped short of clearly calling the Russian operations a violation of international law, [37] and the administration under President Donald Trump has taken a much more ingratiating tone vis-à-vis Russia; neither administration has openly invoked the right under international law to take so-called countermeasures or reprisals (limited acts that would otherwise violate international law but may be lawfully taken in response to a violation).[38]

33 *E.g.*, Carl Hulse, *After Resisting, McConnell and Senate G.O.P. Back Election Security Funding*, N.Y. TIMES (Sept. 19, 2019), https://www.nytimes.com/2019/09/19/us/politics/mcconnell-election-security.html?module=inline; Michael Wines, *$250 Million To Keep Votes Safe? Experts Say Billions Are Needed*, N.Y. TIMES (Sept. 26, 2019), https://www.nytimes.com/2019/09/25/us/mitch-mcconnell-election-security-bill-.html.

34 *See* Lawrence Norden & Edgardo Cortés, *What Does Election Security Cost?*, BRENNAN CTR. FOR JUST. (Aug. 15, 2019), https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost (providing a breakdown of cost estimates that far exceeds the efforts made thus far to secure U.S. election integrity).

35 IRA Indictment, *supra* note 7, at 1–2.

36 Press Release, U.S. Dep't of State, Sanctions Announcement on Russia (Dec. 19, 2018), https://www.state.gov/sanctions-announcement-on-russia; Lara Jakes, *With Sanctions on Russians, U.S. Warns Against Foreign Election Meddling*, N.Y. TIMES (Sept. 30, 2019), https://www.nytimes.com/2019/09/30/us/politics/us-russia-sanctions-election-meddling.html; David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

37 Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SECURITY (Jan. 5, 2017), https://www.justsecurity.org/35999/international-law-response-russian-election-interference.

38 TALLINN MANUAL 2.0, *supra* note 10, at 111.

The United States does appear to have taken retaliatory cyber operations against Russia,[39] though it is unclear whether it acted out of a belief that such measures would be lawful under international law as reprisals.

Overall, although a strong case can be made that Russia's election interference constitutes a breach of international law, the U.S. response to Russian interference in its 2016 election through primarily domestic—rather than international—law further highlights the considerable interpretative ambiguities and challenges of enforcing international law, especially in the cyber realm. As both technology and the law develop, the antecedent definitional questions as well as deliberations on how to respond are likely to become all the more pressing in the future.

[39] For examples of these retaliations, see, e.g., Julian E. Barnes, *U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections*, N.Y. TIMES (Oct. 23, 2018), https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html; Austin Carson, *Obama Used Covert Retaliation in Response to Russian Election Meddling. Here's Why.*, WASH. POST: MONKEY CAGE (June 29, 2017), https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/29/obama-used-covert-retaliation-in-response-to-russian-election-meddling-heres-why; David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (June 15, 2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.