RESPONDING TO ELECTION MEDDLING IN THE CYBERSPACE: AN INTERNATIONAL LAW CASE STUDY ON THE RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION

Alex Xiao*

International law is not the most perfect legal regime, and, perhaps to no one's surprise, it is even less perfect in cyberspace. The United States has been a victim to a series of malicious cyber operations in recent years, and the key question is how to respond to and deter them. This Article offers a detailed survey of the Russian interference in the 2016 presidential election in the context of international law. Adapting the framework created by Tallinn Manual 2.0*, the Article examines the international legal basis of the response measures employed by the United States and other possible alternative responses to the Russian operation. It concludes that none of these responses are both squarely supported by international law and desirable as a matter of national security police. This Article intends to show that international law contains considerable gray areas in the cyber realm that allow sophisticated adversaries like Russia to harm the core interest of the United States without substantial legal repercussions. The Article concludes by suggesting that a deterrence mechanism based on proactive national security policy would be more effective and practical than one based on international law.*

* J.D. Candidate at Duke University School of Law, Class of 2020. I am extremely grateful to General Charlie Dunlap for his international law seminar that inspired this Article and for his guidance throughout my research process. Special thanks goes to Zhanna Malekos Smith and my colleagues at the Duke Journal of Comparative & International Law for valuable suggestions and edits. All errors are mine.

I. INTRODUCTION

Following the 2016 presidential election, the United States intelligence community found evidence of election meddling operations in the cyberspace linked to the Russian government.[1] The possibility that the Russian State compromised the integrity of the democratic process incited a great amount of fear and anger. Then Chairman of the Senate Armed Services Committee, Senator John McCain, called the Russian meddling an "act of war."[2] John Brennan, then Director of the Central Intelligence Agency, also emphasized that an attempt to influence the election process is a "very, very serious matter."[3]

In response to the operation, both the Obama and Trump Administrations have imposed economic sanctions on the Russian entities involved[4] and indicted numerous Russian individuals who played a role in election interference.[5] Due to the seriousness of the issue, many commentators are not satisfied with how the United States responded to Russia. Some, like Harvard Law Professor Jack Goldsmith, simply criticized the United States' lack of deterrence policy in cyberspace;[6] others went a step further, calling for fiercer responses than the ones employed.[7] Although

1. Press Release, White House, Office of the Press Secretary, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://perma.cc/3XXD-8K5C; OFF. OF THE DIR. OF NAT'L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [hereinafter ODNI REPORT].

2. Theodore Schliefer & Deidre Walsh, *McCain: Russian Cyberintrusions an Act of War,'* CNN (Dec. 30, 2016), https://www.cnn.com/2016/12/30/politics/mccain-cyber-hearing/.

3. THE ASPEN INST., ASPEN SECURITY FORUM 2016: A CANDID CONVERSATION WITH THE DIRECTOR OF THE CIA 29 (2016), https://perma.cc/XU94-KEYY.

4. The White House, *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment*, THE WHITE HOUSE: PRESIDENT BARACK OBAMA (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and.

5. *See* Peter Baker, *White House Penalizes Russians over Election Meddling and Cyberattacks,* N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html; Gardiner Harris, *Trump Administration Imposes New Sanctions on Putin Cronies*, N.Y. TIMES (Apr. 6, 2018), https://www.nytimes.com/2018/04/06/us/politics/trump-sanctions-russia-putin-oligarchs.html.

6. Jack Goldsmith, *The DNC Hack and (the Lack of) Deterrence*, LAWFARE (Oct. 9, 2016), https://www.lawfareblog.com/dnc-hack-and-lack-deterrence.

7. *See, e.g.*, Julia Manchester, *Dem Calls Russia Meddling 'Act of War,' Urges Cyber Attack on*

these demands for a stronger response might serve the country's sentiment of undergoing a direct attack on the democratic system, they do not have a solid basis under international law.

This Article offers a detailed analysis of the Russian interference in the 2016 election in the context of international law. It examines the international legal basis of the response measures employed by the United States and other possible alternative responses to the Russian operation. I argue that none of the three alternative measures examined are plainly applicable as a matter of international law, nor are they desirable as a matter of policy, mainly because of the great uncertainty that the current international law carries. I conclude the Article by arguing that a deterrence mechanism, based on policy instead of international law, would be more effective and practical.

II. CONTEXT OF THE 2016 RUSSIAN ELECTION MEDDLING OPERATION

The January 2017 report published by the Office of the Director of National Intelligence ("ODNI Report") is one of the most authoritative declassified reports on Russian interference in the 2016 election.[8] With high confidence,[9] the report attributes the Russian election meddling operation to President Vladimir Putin himself.[10] The report also states that the operation was intended to "undermine public faith in the U.S. democratic process, denigrate Secretary Hillary Clinton, and harm her electability and potential presidency."[11]

Notably, the Russian election meddling operation had multiple components.[12] The three major components are the following: The first and most publicly-reported part is its hacking-and-releasing campaign against the Democratic National Committee ("DNC") in March 2016,[13] launched by a Russian military intelligence agency known as the General Staff Main

Moscow Banks, THE HILL (July 17, 2018), https://thehill.com/hilltv/rising/397366-dem-rep-no-question-that-russia-hacking-effort-is-act-of-war (Rep. Steve Cohen (D-Tenn.) calling for cyber counter attack that would make "Russian Society valueless"); Mark Hertling & Molly K. Mckew, *Putin's Attack on the U.S. Is Our Pearl Harbor*, POLITICO MAGAZINE (July 16, 2018), https://www.politico.com/magazine/story/2018/07/16/putin-russia-trump-2016-pearl-harbor-219015 (calling for more consequential response to deter further attacks).

8. ODNI REPORT, *supra* note 1.

9. High confidence normally indicates that the judgment is confirmed by "high-quality information from multiple sources," although it does not imply certainty. *Id.* at 13.

10. *Id.* at ii.

11. *Id.* at 2.

12. *Id.* at 1.

13. *Id.*

Intelligence Directorate ("GRU").[14] The GRU hacked into the personal email accounts of DNC officials by infiltrating the DNC servers and selectively released the information gathered to multiple outlets, including Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks.[15] In the entire process of the hacking-and-release campaign, no property, including servers or personal computing devices, was damaged in any way.[16] Simultaneously, Russia's state-controlled media, RT and Sputnik, started to run a propaganda campaign supporting then-presidential-candidate Trump in its English content.[17]

Finally, a non-government entity closely tied to Russian intelligence, the Internet Research Agency ("IRA"), initiated a social media campaign during the 2016 presidential election.[18] The IRA spent over two million dollars purchasing anti-Clinton and pro-Trump advertisements on major social media platforms, including Twitter, Facebook, and Instagram.[19] On these platforms, hundreds of fake accounts were created to interact with voters.[20] Across platforms, the IRA created and used more than 120 groups and social media "troll" accounts during the election meddling operation.[21]

Each part of this operation had different international law implications. I will now discuss, given what we know about the Russian operation, what international law options the United States has in response.

III. LEGAL ANALYSIS IN THE CONTEXT OF *TALLINN MANUAL 2.0*

This note primarily relies on *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (hereinafter "*Tallinn Manual 2.0"*) as well as its academic critique and commentary to examine different international law response measures available to the United States government. Published in 2017, *Tallinn Manual 2.0* is an expansion of its previous 2013 version, *Tallinn Manual on the International Law Applicable*

14. *Id.*

15. *Id.* at 2–3.

16. *Id.* at 2

17. *Id.* at 3–4.

18. *Id.* at 4.

19. *See* Oliver Carroll, *St. Petersburg "Troll Farm" Had 90 Dedicated Staff Working to Influence US Election Campaign*, INDEPENDENT (Oct. 17, 2017), https://perma.cc/BL34-WK9F (discussing the IRA's operations and funding).

20. *See* Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html (discussing the IRA's use of fake social media accounts).

21. Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 35 (2018) [hereinafter Schmitt, *"Virtual" Disenfranchisement*].

to Cyber Operations.[22] Created by an independent group of international law experts from twenty nations ("*Tallinn Manual 2.0* experts"),[23] *Tallinn Manual 2.0* examines customary international law applicable in the context of conflicts in cyberspace and is the most comprehensive treatise available in this area.

Tallinn Manual 2.0 provides four major categories of responses to States facing hostile cyber operations: (1) self-defense, (2) the plea of necessity, (3) countermeasures, and (4) retorsion.[24] The availability of each response to a victim State depends on the different levels of hostile operation the victim State underwent.[25] This section will first examine retorsion, which is the international legal foundation of the response measures actually employed by the United States in response to the Russian election meddling operation. It will then discuss the possible alternative options for the United States: self-defense, the plea of necessity, and countermeasures. I conclude that, in the case of the Russian interference in the 2016 election, none of the three alternative response measures is warranted as a matter of international law and desirable as a matter of policy.

A. Retorsion

Following Russia's operation to influence the 2016 Presidential Election, the Obama administration responded by imposing sanctions on several Russian governmental and private organizations involved in the operation, as well as expelling dozens of Russian government officials by declaring them "*persona non grata,*" or, literally, "person not appreciated."[26] In March 2018, the Trump administration also imposed further sanctions on Russian oligarchs, governmental agencies, and Russian individuals involved in these cyber operations.[27]

The Obama and Trump Administrations' responses to the Russian

22. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, at xxiii (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

23. *See id.* at 5 (discussing membership of the International Groups of Experts and the drafting process).

24. *See generally* Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical* Vade Mecum, 8 HARV. NAT'L SEC. J. 239 (2017) [hereinafter *Vade Mecum*]. *See also* Sean Watts, *International Law and Proposed U.S. Responses to the D.N.C. Hack*, JUST SEC. (Oct. 14, 2016), https://perma.cc/Q8L5-C432 (discussing potential U.S. responses to Russia).

25. *Vade Mecum*, *supra* note 24, at 244.

26. The White House, *Fact Sheet*, *supra* note **Error! Bookmark not defined.**.

27. Peter Baker, *White House Penalizes Russians over Election Meddling and Cyberattacks*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html; Gardiner Harris, *Trump Administration Imposes New Sanctions on Putin Cronies*, N.Y. TIMES (Apr. 6, 2018), https://www.nytimes.com/2018/04/06/us/politics/trump-sanctions-russia-putin-oligarchs.html.

operation fall into the category of "retorsion" under international law.[28] Retorsion is a hostile but lawful measure against another State.[29] Economic sanctions and expulsion of diplomatic personnel are classic examples of retorsion,[30] both of which are hostile against another State but within the power of a sovereign State.[31] Before a State employs retorsion measures against another State, the former does not need to establish that the later has committed an internationally wrongful act, such as prohibited intervention.[32] Retorsion does not create any breach of international legal obligation and is, therefore, the mildest response measure that *Tallinn Manual 2.0* provides for States to respond to a hostile cyber operation.

The Obama Administration's use of retorsion as a response to the Russian hack implies two possibilities. Either the Administration believed that establishing the Russian government had committed an internationally wrongful act would be difficult or, alternatively, the Administration decided the mildest level of retaliation available was more desirable, even if such a case could be made. The following analysis will demonstrate that both reasons may be true by examining the alternative legal options in response to the Russian operation. I will first discuss the law regarding self-defense.

B. Alternative Legal Options: Self-Defense

After the reports of the Russian hack came out, many commentators started to call this effort to meddle with the U.S. elections an "act of war," urging strong retaliatory measures.[33] Some even compared the hacking to some of the most devastating attacks in U.S. history, such as the Japanese attack on Pearl Harbor and the September 11 terrorist attack.[34] Equating

---

28. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 64; *see also Vade Mecum*, *supra* note 24, at 258.

29. TALLINN MANUAL 2.0, *supra* note 22, at 112.

30. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 64.

31. *Id.* at 64 n.160 ("As noted by Professor Sean Murphy in his Statement of Defense of the United States, 'every state has the right to grant or deny foreign assistance, to permit or deny exports, to grant or deny loans or credits, and to grant or deny participation in national procurement or financial management, on such terms as it finds appropriate."); Statement of Defense of the United States at 57, Islamic Public of Iran v. United States of America, Claim No. A/30 (Iran-United States Claims Tribunal 1996), https://perma.cc/W92E-3LLM.

32. See Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 64 ("The cyber operations to which an act of retorsion responds need not constitute an internationally wrongful act, although they may."); *see also Vade Mecum*, *supra* note 24, at 258.

33. *See, e.g.*, Manchester, *supra* note 7 (for coverage of the remarks of Rep. Steve Cohen (D-Tenn.)); Michelangelo Signorile, *Russia Committed An Act Of War And Trump Won't Talk About It*, HUFFINGTON POST (July 16, 2018), https://www.huffingtonpost.com/entry/opinion-signorile-russian-hacking_us_5b4b6a09e4b022fdcc5a3aa3 (arguing that Russia committed an "act of war" against the United States).

34. Mark Hertling & Molly K. McKew, *Putin's Attack on the U.S. Is Our Pearl Harbor*, POLITICO

Russia's hacking to a kinetic attack (traditional, regular military attack), for example, the bombing of Pearl Harbor, carries great international law significance because this characterization could potentially permit the United States to respond to Russia in the form of self-defense.

Self-defense is the one alternative response measure the United States might consider using in light of a harmful operation. The United Nations Charter prohibits Member States from engaging in any "threat or use of force against . . . any [other] state,"[35] unless under authorization of the Security Council under Article 39 or, under Article 51, in "self-defence if an armed attack occurs against a Member of the United Nations. . . ."[36] The State's right to engage in self-defense under *jus ad bellum*, the right to war, has not only been entrenched in the United Nations Charter,[37] but also indisputably established by customary international law.[38] If a harmful cyber operation has amounted to the level of "armed attack," the victim State is then entitled, as a matter of international law, to respond by counter attacks that would otherwise be prohibited by Section 2(4) of the UN Charter.

The central challenge is defining when a harmful cyber operation rises to the level of an "armed attack." Customary international law uses the "scale and effects" analysis of an operation as a test, but fails to specify further guidance.[39] Hence, customary international law does not provide a practical bright-line rule for identifying the precise point at which a military operation amounts to an "armed attack." The *Tallinn Manual 2.0* experts unanimously agreed that, in the cyber context, the precise line would be unclear too, except in certain extreme scenarios.[40] For example, the *Tallinn Manaual 2.0* experts do agree that acts of cyber intelligence gathering and cyber theft, as well as cyber operations that "involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks[,]" while the operations that "seriously injur[ ]es or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy. . . ."[41]

Tallinn Manual 2.0 experts, however, do not agree whether the 2010

(July 16, 2018), https://politico.com/magazine/story/2018/07/16/putin-russia-trump-2016-pearl-harbor-219015.

35. U.N. Charter art. 2, ¶ 4.

36. *Id.* art. 51.

37. *Id.* (describing the right to self-defense as an "inherent right").

38. *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 51, 74, 76 (Nov. 6); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8); *Vade Mecum*, *supra* note 24, at 244 n.8 (citing Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US), 1986 I.C.J. 14, ¶¶ 176, 194 (June 27) [hereinafter Nicaragua]).

39. TALLINN MANUAL 2.0, *supra* note **Error! Bookmark not defined.**, r. 71.

40. *Id.*

41. *Id.*

Stuxnet operation, where a malicious computer malware was used to halt the Iranian nuclear program and ended up disabling thousands of centrifuges Iran used to purify uranium,[42] meets the "armed attack" threshold,[43] despite the fact that, arguably, a significant amount of property was damaged as one would see in a kinetic attack.[44]

Even when there is no physical harm to persons or physical damage to property, the *Tallinn Manual 2.0* experts are divided on whether there can be an incident characterized as an armed attack.[45] Some argue that it is not the destructive nature, but the extent of the ensuing effects that matter.[46] A cyber operation directed to cause a market crash at a major stock market would be a classic example that divides the two camps.[47]

The legal analysis of the condition precedent for self-defense is an even more complicated one for the United States. The United States holds the minority view that the threshold for an armed attack is identical to that of a prohibited use of force,[48] while customary international law sees only the "gravest forms of the use of force" as an armed attack.[49] This means that the United States reserves the flexibility to respond not only to armed attacks, but also to illegal uses of force, by imposing measures that fall into the self-defense category.[50]

---

42. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

43. TALLINN MANUAL 2.0, *supra* note 22, at 342.

44. Some have argued this would be enough. *See, e.g.*, James G. Stavridis, *Incoming: What Is a Cyber Attack?*, SIGNAL MAG. (Jan. 1, 2015), http://www.afcea.org/content/?q=incoming-what-cyber-attack [http://perma.cc/VR8Y-JN75] ("Because Stuxnet produced a destructive effect that we normally associate with attacks in other domains, there is no argument over whether it constituted a cyber attack."); *see also* Ryan Fairchild, *When Can a Hacker Start a War?*, PAC. STANDARD (Feb. 6, 2015), http://www.psmag.com/nature-and-technology/when-cyber-attack-constitutes-act-of-war [http://perma.cc/S2MQ-8AAD] (arguing that "Stuxnet would have qualified as an armed attack").

45. TALLINN MANUAL 2.0, *supra* note **Error! Bookmark not defined.**, at 341–42.

46. *Id.*

47. *Id.*

48. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL pt. 16.3.3.1, at 1017 (2016) (citing Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L. J. ONLINE 7 (Dec. 2012) ("To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response—such responses must still be necessary and of course proportionate.")).

49. *See* Nicaragua, *supra* note 38, ¶ 191.

50. This flexibility could create an advantage for the United States, because since the *Caroline* incident, customary international law allows operations for self-defense purposes to be anticipatory, rather than reactive if the state can show that an attack is imminent, which might grant the United States

The accurate legal standard for what acts amount to a use of force, but not an armed attack, carries great uncertainty.[51] The *Tallinn Manual 2.0* experts agreed that, in the cyber realm, the customary "scale and effects" standard for determining what amounts to an armed attack should also apply when determining which acts amounts to a use of force,"[52] which, again, does not provide much practical value.

The *Tallinn Manual 2.0* experts have reached a consensus on only a few cases. For example, on the one end, *Tallinn Manual 2.0* experts unanimously categorized the Stuxnet incident as a use of force.[53] On the other end, they also agreed that neither psychological operations in cyberspace only seeking to weaken confidence in a government, nor a ban on e-commerce intended to undermine the victim state's economy, amount to uses of force.[54] *The Tallinn Manual 2.0* experts also drew an analogy to the International Court of Justice's ("ICJ") *Nicaragua* opinion, asserting that "a State that provides an organized armed group with malware and the training necessary to carry out cyber operations against another State has engaged in a use of force against the latter" as long as the supported operations themselves rise to a use of force.[55]

Given the great elusiveness of the use of force standard, the *Tallinn Manual 2.0* experts provide an open list of factors that States are likely to use in assessing whether a cyber operation has reached the level of a use of force:[56]

1. **Severity**: the level of harm inflicted on individuals and property, measured by the scope, duration, and intensity of the consequences. The *Tallinn Manual 2.0* experts believe severity is the most important factor in categorizing cyber operations.
2. **Immediacy**: the more immediate the effects caused by the cyber operation, the more likely such an operation amounts to a use of force.
3. **Directness**: the more direct the causal link between the

---

the first-hand advantage in a military conflict. *See* Letter from Daniel Webster to Lord Ashburton (July 27, 1842), http://avalon.law.yale.edu/19th_century/br-1842d.asp; *see also* William H. Taft, IV, *International Law and the Use of Force*, 36 GEO. J. INT'L L. 659, 659–60 (2005) (stating that state's right to use force before an imminent attack is well-established).

51. TALLINN MANUAL 2.0, *supra* note **Error! Bookmark not defined.**, at 330 (stating the United Nation Charter does not provide specific criteria determining what actions rise to the illegal use of force).

52. *Id.*

53. *Id.* at 342.

54. *Id.* at 331.

55. *Id.* at 332 (citing Nicaragua, *supra* note 38) (judgment that arming and training a guerrilla force that is engaged in hostilities against another State qualified as a use of force).

56. *Id.* at 334.

operation and its consequences, the more likely such an operation amounts to a use of force.

4. **Invasiveness**: the more classified and protected the targeted system is, the more invasive the operation, and, therefore, the more likely such an operation amounts to a use of force.
5. **Measurability of effects**: the more quantifiable and identifiable the effects of a cyber operation are—e.g. the amount of data corrupted, the percentage of server disabled, etc.—the more likely that a State would characterize it as a use of force.
6. **Military character**: the more military involvement, the more likely an operation is characterized as a use of force.
7. **State involvement**: the clearer and closer a nexus between a State and cyber operations, the more likely an operation rises to a use of force.
8. **Presumptive legality**: certain acts are not prohibited by international law *per se*, including propaganda, psychological operations, espionage, or mere economic pressure. If a cyber operation falls into any of these categories, it is less likely to amount to a use of force.

Except for severity, none of the aforementioned factors are likely sufficient to justify categorizing a cyber operation as a use of force on their own.[57] Although this rubric offers a more expanded definition of a use of force, applying it real-time to the effects of a still-developing operation may prove difficult.[58] It is useful, however, for this Article's analysis on the DNC hack.

The Russian election meddling operation cannot be categorized as an armed attack under the framework of *Tallinn Manual 2.0* because no physical damages were inflicted on persons or objects. This operation is a much weaker case under the current international law framework than that of the Stuxnet operation, where physical property—thousands of Iranian centrifuges—was damaged and disabled.[59] If the *Tallinn Manual 2.0* experts could not reach a consensus on whether Stuxnet qualified as an armed attack, the DNC hack is even more unlikely to be considered as such.

---

57. Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE INT'L L.J. ONLINE 1, 14 (Oct. 18, 2017), https://ssrn.com/abstract=3180687 [hereinafter Schmitt, *Grey Zones*].

58. Priyanka R. Dev, *"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: the Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 TEX. INT'L L.J. 381, 391 (2015).

59. *See* Ryan Fairchild, *When Can a Hacker Start a War?*, PAC. STANDARD (Feb. 6, 2015), http://www.psmag.com/nature-and-technology/when-cyber-attack-constitutes-act-of-war.

The "scale and effects" analysis is even more unlikely to qualify the DNC hack as an armed attack.[60] Although the Mueller investigation and indictments against Russian individuals have provided much more information, the actual effects of the hack are still almost unmeasurable.[61] The way that the Russian election interference operated in influencing the information environment—essentially spreading narratives and messages that were false but also subscribed to by certain American groups, such as the subscribers of Infowars—made it hard for analysts to figure out (1) which parts of the information environment before the 2016 election was created by Russian trolls and (2) which parts originated in the United States.

Categorizing the Russian DNC hack as an armed attack might also invite an escalation of cyber conflict by triggering Article 5 of the North Atlantic Treaty Organization ("NATO") Charter,[62] which calls for a collective response from all NATO States. It could alienate NATO partners to put the entirety of NATO in a confrontation with Russia over an election meddling operation that caused no physical damage. After all, Estonia, even after suffering a much stronger attack from Russia in 2007 that temporarily disabled a large percentage of its Internet system, did not invoke Chapter 5 for these considerations.[63]

Under *Tallinn Manual 2.0* standards, the DNC attack is also unlikely to qualify as a use of force for two reasons. First, on its face, the Russian operation is closer to "non-destructive cyber psychological operations intended solely to undermine confidence in a government,"[64] which does not constitute a use of force, than the Stuxnet operation, which, again caused damages on a large amount of State property.

Second, the "scale and effect" factors drawn from *Tallinn Manual 2.0* also support the same conclusion that the Russian operation does not constitute a use of force:

1. **Severity**: Weak. No harm or damages were inflicted on people or property.
2. **Immediacy**: Strong. The effects of the DNC hack were immediately felt by the United States electorate in a heated

60. *See* TALLINN MANUAL 2.0, *supra* note 22, r. 71.

61. *See* Molly Mckew, *Did Russia Affect the 2016 Election? It's Now Undeniable*, WIRED (Feb. 16 2018), https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/.

62. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

63. Ryan J. Hayward, *Evaluating the "Imminence" of a Cyber Attack for Purposes of Anticipatory Self-defense*, 117 COLUM. L. REV. 407, 411 (2017); *see also* Emily Tamkin, *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?*, FOREIGN POLICY (Apr. 27, 2017), https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

64. TALLINN MANUAL 2.0, *supra* note 22, at 331.

election.

3. **Directness**: Strong. Although the actual effects of the DNC hack are extremely hard to quantify, one can certainly argue that the DNC emails disclosed after the hack directly influenced certain voters' behaviors in the 2016 elections.
4. **Invasiveness**: Weak. No target in this operation is a protected or classified system by the United States government. The DNC is a private organization and it uses its servers to promote the mission of the Democratic Party. The Russians never attacked the voting system itself or any government entities related to the election.
5. **Measurability of effects**: Weak. We are able to measure how much information the Russians stole. However, no data or servers were actually corrupted or damaged. The Russians selectively disseminated the information they gathered for political gain without using physically destructive means. Collecting information, despite via illegal means under United States domestic law, does not by itself violate international law.[65]
6. **Military character**: Strong. The Central Intelligence Agency and the Federal Bureau of Investigation found with a high degree of confidence that Russian military intelligence units were behind the operation.[66] The GRU hacked into the personal email accounts of Democratic Party officials and distributed the information gathered.
7. **State involvement**: Strong. For the same reason mentioned above, State involvement is extremely close to this operation. The attack did not come from a private organization supported by the Russian government, but from the military intelligence agency itself.
8. **Presumptive legality**: Unclear. International law does not provide an answer on this question because scholars are still arguing whether what the Russians did during the 2016 Election was a psychological operation through cyber espionage, which is legal under international law, or something more severe.[67] This factor would not help us answer the

65. *See id.* at r. 32 (espionage does not violate international law).

66. ODNI REPORT, *supra* note 1, at 13.

67. *Compare* 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/, *with* Ram Sachs, *Hacking the Election*, YALE INT'L L. J. ONLINE (Oct. 28, 2016),

> question of whether the Russian operation constitutes a use of force because, in this case, the characterization of the Russian operation is the most important question that needs to be answered.

Although some of the *Tallinn Manual 2.0* factors seem to support categorizing the Russian Hack as a use of force, the most important factor in the analysis—the severity of the effects caused by the cyber operation—does not. The non-violent nature of the operation makes a use of force categorization extremely difficult. Being able to attribute a cyber operation that had certain unquantifiable effects on the 2016 elections to the Russian government does not seem to raise the operation to the level of a use of force because it would not effectively distinguish this operation from other lower level offenses under international law, such as prohibited intervention, which will be discussed in later parts of this Article.

One way to increase the severity of the effects of the Russian operation as a matter of law would be categorizing the election system as "critical infrastructures"[68] and treating meddling with the elections akin to tampering with a major dam or an electrical grid. However, the DNC servers are not related to the election itself, but are instead used to promote the interest of a private organization, the Democratic Party. Therefore, even if the election system is categorized as a critical infrastructure as a matter of law, Congress must go the extra mile to consider ways to protect private entities like the DNC to respond to cyber operations like the DNC hack in the future. Either way, classifying the election system as critical infrastructure was unavailable for both the Obama and the Trump Administrations because such classification was not in place before the Russian operation.

Self-defense would not have been a measure available to the United States to respond to the Russian DNC hack in 2016. This is because the operation amounts to neither an armed attack nor a use of force under customary international law, as reflected in *Tallinn Manual 2.0*. The Russian operation, however, could have been categorized as violating other aspects of international law, to which the United States may respond by either invoking the plea of necessity[69] or imposing countermeasures.[70] I will next discuss the legal requirements and the applicability of invoking the plea of necessity.

---

http://www.yjil.yale.edu/hacking-the-election/#_ftnref7.

68. *See generally* Eric Jensen, *Computer Attacks on Critical National Infrastructure*, 38 STAN. J. INT'L L. 207, 209 (2002); Scott J. Shackelford et al., *Making Democracy Harder to Hack*, 50 U. MICH. J. L. REFORM 629 (2017).

69. TALLINN MANUAL 2.0, *supra* note 22, at 135.

70. *Id.* at 111.

C. Alternative Legal Options: The Plea of Necessity

Adopting the law of State responsibility,[71] Rule 26 of *Tallinn Manual 2.0* provides that "[a] State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."[72] Like self-defense, the plea of necessity allows the State to respond to certain situations with means that would otherwise be a violation of international law.[73] The threshold for the plea of necessity consists of three elements.

First, the State's interest that is being infringed must be "essential." The *Tallinn Manual 2.0* experts note that, absent an internationally accepted standard, the "determination of whether something is essential is always contextual," varying from State to State.[74] The *Tallinn Manual 2.0* experts also agreed that States' unilateral classification of certain State interests as "critical" is not determinative of the issue as a matter of international law.[75]

Second, the potential harm to the critical interest identified by the victim State must also be "grave" and "imminent," adding requirements of severity and temporality. The *Tallinn Manual 2.0* experts agreed that to be "grave," the potential harm must be "especially severe," undermining "an interest in a fundamental way, like destroying the interest or rendering it largely dysfunctional."[76]Although the risk of physical damage is not required in order to meet the gravity requirement, "mere inconvenience, irritation, or

71. *See* Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, art. 25 (2001) [hereinafter Articles on State Responsibility].

72. TALLINN MANUAL 2.0, *supra* note 22, at 135.

73. *See* Articles on State Responsibility, *supra* note 71, art. 25 ("1. Necessity may not by invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of the State unless the act: (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States toward which the obligation exists, or of the international community as a whole. 2. In any case, necessity may be invoked by a State as a ground for precluding wrongfulness if: (a) the international obligation in question excludes the possibility.").

74. TALLINN MANUAL 2.0, *supra* note 22, at 135. For example, states tend to classify certain infrastructures as critical, but in different scopes. *Compare* CRITICAL FIVE, FORGING A COMMON UNDERSTANDING FOR CRITICAL INFRASTRUCTURE—SHARED NARRATIVE (2014), https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf [https://perma.cc/HWU3-342S] (Australia, Canada, New Zealand, the United Kingdom, and the United States in 2014 proposed a common definition of critical infrastructure), *with* U.N. Secretary-General, Letter dated Jan. 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations, U.N. Doc. A/69/723 (Jan. 13, 2015) (proposing an international code of conduct for information security to the General Assembly).

75. TALLINN MANUAL 2.0, *supra* note 22, at 136.

76. *Id.*

minor disruption" of the interest will never be sufficient.[77]

The imminence requirement carries more controversy. *Tallinn Manual 2.0* adopts the standard of imminence from the Articles of State Responsibility, which is a set of international law standards developed and codified by the International Law Commission, a United Nations task force of international law experts. The standard states that such imminence must be "objectively established and not merely apprehended as possible."[78] The *Tallinn Manual 2.0* experts also draw an analogy from the anticipatory self-defense doctrine, asserting that peril is always imminent when the "window of opportunity" to prevent the hostile operation is about to close.[79]

What complicates the matter further is that, as the *Tallinn Manual 2.0* experts recognized, customary international law does not only view the imminence requirement in the temporal sense.[80] The *Gabčíkovo-Nagymaros Project* judgment of the ICJ held that the imminence requirement is satisfied even if the harm in question could occur "in the long term," as long as that fact did not render the harm "less certain and inevitable."[81] An example would be a cyber operation targeting a State's financial system with certain immediate effects such as a stock market crash, but the loss of confidence in the long term may be the "grave and imminent" peril that justifies the victim State to resort to the plea of necessity.[82]

The *Gabčíkovo-Nagymaros* interpretation of imminence, however, raises the issue regarding the requisite degree of certainty of harm that would justify the disregard of the requirement of the temporal approximate.[83] *Tallinn Manual 2.0* adopts the reasonableness standard available from the Articles on State Responsibility, stating that the decision to take the plea of necessity must be based on evidence "reasonably available at the time."[84] In addition, a State may only act when it is reasonable for a State in a similar situation to do the same.[85]

The third and final requirement for acting pursuant to the plea of

77. *Id.*

78. *Id.* at 138 (citing Articles on State Responsibility, *supra* note 71, art. 25, cmt. 15).

79. *Id.* at 139.

80. *Id.* at 138.

81. TALLINN MANUAL 2.0, *supra* note 22, at 138 (citing Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7, ¶ 54 (Sept. 25)).

82. TALLINN MANUAL 2.0, *supra* note 22, at 139.

83. Christian Schaller, *Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity*, 95 TEX. L. REV. 1619, 1633–34 (2017).

84. TALLINN MANUAL 2.0, *supra* note 22, at 138 (quoting Articles on State Responsibility, *supra* note 71, art. 25).

85. *Id.*

necessity is that there must not be any other way to address the situation.[86] When assessing alternative measures, cost and inconvenience alone are not decisive factors.[87] This means, even when a State is anticipating an attack on a major infrastructure, if the State can find a viable way to shift the operation to other infrastructure while resolving the situation, it must do so, rather than retaliating against the attacker in manners that would violate international law, such as hacking back.[88]

Another key limitation on a State invoking the plea of necessity is that it "may not engage in cyber operations that seriously impair the essential interests of affected States,"[89] rendering them in comparable peril experienced by the invoker. As Michael Schmitt, the Director of *Tallinn Manual 2.0* Project, pointed out, this is because international law seeks to balance the rights and obligations of States because they are equal as sovereigns.[90]

Despite the limitations, the plea of necessity does provide one key advantage: a State may resort to the plea of necessity when the attacker cannot be identified.[91] Therefore, the State does not need to attribute a hostile operation to a State actor nor show that a legal obligation under international law has been breached in order to initiate a response.[92] For example, a victim State may shut down its cyber connection with the country that houses the source of the attack without proving the source has any connections with the government of that country, as long as the victim State deems that the situation satisfies the requisites of the plea of necessity. The flexibility of the plea to necessity is, conceptually, extremely useful in the cyber context, where confident attack attribution is rare and legal categorization uncertain.[93]

Having outlined the relevant rule, I now discuss whether the plea of necessity was a measure available and desirable for the U.S. decision-makers facing the 2016 Russian cyber operation. I conclude that the 2016 Russian cyber operation does not satisfy the requisites of the plea of necessity as a matter of international law.

Although there are conceivable arguments supporting the availability

86. *Id.* at 139

87. *Id.*

88. *Id.*

89. *Id.* at 137 (citing Articles on State Responsibility, *supra* note 71, art 25(1)(b)).

90. *Vade Mecum*, *supra* note 24, at 252.

91. *See* TALLINN MANUAL 2.0, *supra* note 22, at 138 ("In situations in which the exact nature or origin of a cyber incident is unclear, cyber measures may be justified on the basis of the plea of necessity.").

92. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 65.

93. *See* Schmitt, *Grey Zones*, *supra* note 57, at 14 ("Agreement on a bright line test for qualification of non-destructive or injurious cyber operations as a use of force proved elusive.").

of this measure, it is not a desirable legal option to pursue as a matter of policy. First, the Russian hack and accompanying operations in 2016 very likely infringed on an "essential interest" of the United States. It is reasonable to argue that the election of the highest political office of the country falls into that category. The plea of necessity does not require State entities themselves to be the target of the operation. Therefore, although the hacked servers were privately owned, one can still argue that the uncorrupted operation of the major political parties in the United States serves as a crucial national interest.

The more serious problem arises in the "grave and imminent peril" requirement. The immediate effects of the Russian operation are still up for debate. On the government side, although President Trump has been denying the operation's effect on the outcome of the 2016 election,[94] the intelligence community has not yet officially provided any definite answers. The ODNI Report explicitly stated that it "did not make an assessment of the impact that Russian activities had on the outcomes of the 2016 election."[95] Non-government commentators are also divided on the issue: while most observers have remained agnostic about the actual effects of the Russian operation,[96] some analysts have only recently started to explicitly assert the high likelihood that the election result was altered by the Russian election meddling.[97] Without an unequivocal causal link between the interference and the harm, it is difficult for the United States to declare that the Russian operation has undermined its election system of the United States in a fundamental way, therefore amounting to a "grave and imminent peril" and justifying the United States to launch a response measure allowed under the plea of necessity doctrine.[98]

---

94. *See, e.g.*, Donald J. Trump (@realDonaldTrump), TWITTER (Feb. 17, 2018, 8:22 PM), https://perma.cc/M4HG-UJR6 ("General McMaster forgot to say that the results of the 2016 election were not impacted or changed by the Russians and that the only Collusion was between Russia and Crooked H, the DNC and the Dems. Remember the Dirty Dossier, Uranium, Speeches, Emails and the Podesta Company!"); *see also* Jane Mayer, *How Russia Helped Swing the Election for Trump*, THE NEW YORKER, Sept. 2018 (observing that in public, President Trump "has characterized all efforts to investigate the foreign attacks on American democracy during the campaign as a 'witch hunt' . . . [and] insisted that 'the Russians had no impact on our votes whatsoever'").

95. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION, at i (2017).

96. *See, e.g.*, Nate Silver, *How Much Did Russian Interference Affect The 2016 Election?*, FIVETHIRTYEIGHT (Feb. 16, 2018), https://fivethirtyeight.com/features/how-much-did-russian-interference-affect-the-2016-election/.

97. *See, e.g.*, KATHLEEN HALL JAMIESON, CYBERWAR – HOW RUSSIAN HACKERS AND TROLLS HELPED ELECT A PRESIDENT: WHAT WE DON'T, CAN'T, AND DO KNOW 15–16 (2018) (listing several ways Russia attempted to influence the outcome of the 2016 Presidential Election).

98. *See* TALLINN MANUAL 2.0, *supra* note **Error! Bookmark not defined.**, at 136 (stating that the

There is one potential argument supporting the notion that the Russian operation caused a "grave and imminent peril" to an essential U.S. interest: the infringement on the U.S.' election system is fundamental because the 2016 Russian interference will erode the confidence in the democratic system in the long term.[99] This argument would also satisfy the "imminence" requirement by citing the ICJ's *Gabčíkovo-Nagymaros Project* interpretation of imminence,[100] showing that a certain and grave danger is impending if no action is taken immediately. Once the imminence requirement is met, it would be easier for the decision-makers to argue that the specific measure(s) they chose are the only one(s) available to prevent Russia from initiating further similar operations.

Although this argument could allow the United States to invoke the plea of necessity and, therefore, take much stronger measures than retorsion to respond to the Russian operation, it is not a desirable policy choice because it will invite State actors to abuse the rule, leading to escalation of conflict in cyberspace. If the United States were to resort to the plea of necessity under the argument mentioned above, the United States is creating a a very flexible standard as precedent. The ICJ's *Gabčíkovo-Nagymaros Project* interpretation of imminence potentially allows the State to take actions that would violate international law by claiming that doing so is necessary to prevent a harm in the relatively distant future.[101] There has not been any *opinio juris* with regard to the plea of necessity in the cyber context. If the United States sets a precedent with such a flexible standard, it would almost certainly invite abuse from other State actors, including adversaries of the United States. A world where States could easily obtain justifications of both cyber and kinetic operations under international law would become more susceptible to escalation of cyber conflicts, bringing greater danger to

---

grave and imminent peril element requires that the peril be "especially severe").

99. The intelligence community does have evidence to show that the election meddling seems to be a long-term tactic by the Russian government and more attempts are happening. *See* Ashish Kumar Sen, *Director of National Intelligence Dan Coats: Russia is Attempting to Influence US Midterms, Divide Transatlantic Alliance*, ATLANTIC COUNCIL (June 9, 2018), http://www.atlanticcouncil.org/blogs/new-atlanticist/director-of-national-intelligence-dan-coats-russia-is-attempting-to-influence-us-midterms-divide-transatlantic-alliance ("Coats said Russia had already undertaken an 'unprecedented influence campaign to interfere in the US electoral and political process' in 2016."); *see also* Government's Motion for a Protective Order Under Federal Rule of Criminal Procedure 16(d)(1) at 7, United States v. Concord Mgmt. & Consulting LLC, 385 F. Supp. 3d 69 (D.D.C. 2019) (Crim. No. 18-cr-32-2 (DLF)) ("[T]he substance of the government's evidence identifies uncharged individuals and entities that the government believes are continuing to engage in interference operations like those charged in the present indictment.").

100. *See* TALLINN MANUAL 2.0, *supra* note 22, at 138 (citing to *Gabčíkovo-Nagymaros* acknowledging that "the harm in question could occur 'in the long term'").

101. Christian Schaller, *Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity*, 95 TEX. L. REV. 1619, 1633–34 (2017).

everyone connected to the cyberspace.

In conclusion, the plea of necessity is not, and should not be, a legal tool available for U.S. decision-makers addressing the Russian election meddling operation. I now turn to the third kind of response measure available in international law: countermeasures.

D. Alternative Legal Options: Countermeasures

Countermeasures are State actions that "would otherwise be contrary to the international obligations of an injured State vis-a-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation." [102] Countermeasures are responses to internationally wrongful acts attributed to State actors.[103] They are different from the plea of necessity, which does not require the injured State to either identify an international wrongdoing or attribute the wrongdoing to a State actor before taking action. The plea of necessity excuses the injured State from imposing otherwise wrongful actions against States not responsible for the injury, as long as the condition precedents are met.[104] In contrast, victim states can only impose countermeasures on responsible States.[105]

In this section, I will first discuss the legal limitations and advantages of countermeasures. Next, I will explore the legal issues associated with attribution, and then examine two different types of wrongdoings under international law: violation of sovereignty and prohibited intervention. These are the claims that the United States could allege against Russia to employ countermeasures. I conclude, in this section, that countermeasures would not be available to the United States as a response to the Russian operation in 2016 as a matter of international law because the United States would not be able to establish that the Russian government has committed legal wrongdoings, a requirement for imposing countermeasures.

1. Legal Limitations and Practical Advantages of Countermeasures

There are many legal restrictions to employing countermeasures. First, to be consistent with the United Nations Charter's general mission of

102. Articles on State Responsibility, *supra* note 71, at 128; TALLINN MANUAL 2.0, *supra* note 22, at 111. *See also* Nicaragua, *supra* note 38, at 127.

103. Articles on State Responsibility, *supra* note 71, art. 22.

104. *See* TALLINN MANUAL 2.0, *supra* note 22, at 114 (stating that countermeasures must be used to respond to actions "attributable to a State, while acts pursuant to the plea of necessity must be taken in response to the cyber operation of non-State actors (or even the author of the act is unidentified.)" This means the pleas of necessity, unlike countermeasures, do not have a limitation on the target of the response measures.

105. *Id.*

minimizing escalation, international law does not permit violent countermeasures: "Countermeasures shall not affect . . . the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations."[106] Therefore, reciprocal violent countermeasures in response to a prohibited use of force would also be illegal under Article 2(4) of the United Nations Charter.[107]

Non-violent countermeasures are also subject to limitations. First, the purpose of countermeasures may not be retaliation or punishment.[108] Rather, countermeasures must be designed to put a stop to the unlawful operation and seek assurances (communication by the responsible State that the unlawful act will cease and not be repeated), guarantees (measures designed to ensure non-repetition), or reparations (including restitution, compensation, and apology) from the wrongdoer.[109] Therefore, an injured State may not employ countermeasures in response to a wrongful act that has ceased and is unlikely to happen again.[110] In the cyber context, a classic example of an appropriate countermeasure would be that the victim State initiates a cyber operation designed to end an ongoing malicious cyber operation from the aggressor State.[111]

Furthermore, countermeasures must also be proportionate to the injury to which they respond.[112] The "injury" here refers to the damage that the victim State suffered from the wrongdoer's breach of an international obligation (such as engaging in prohibited intervention and violating sovereignty that will be discussed later) that justifies the victim employing proportionate countermeasures against the wrongdoer.[113]

Despite these limitations, countermeasures do carry significant advantages as an option of responding to malicious cyber operations. First, countermeasures may be directed at targets other than the entity that actually

106. *Id.* art. 50.

107. TALLINN MANUAL 2.0, *supra* note 22, at r. 22, cmt. 11 (noting that the majority of experts consider "the obligation to refrain from the use of force" to be "a key limitation on an injured State when conducting countermeasures").

108. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 65.

109. Articles on State Responsibility, *supra* note 71, arts. 49–53; TALLINN MANUAL 2.0, *supra* note 22, rr. 20–25, 27–29; *see also* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 64 n.162.

110. Articles on State Responsibility, *supra* note 71, arts. 49(2), 52(3)(a). There are other limitations not mentioned because they are not relevant to the purpose of this article. For example, "countermeasures cannot violate fundamental human rights, *jus cogens* norms, the prohibition on belligerent reprisals, or dispute settlement procedures." Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 578 n.51 (2018).

111. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 64–65.

112. TALLINN MANUAL 2.0, *supra* note 22, r. 23.

113. *Id.* at 127.

carries out the operation that amounts to an internationally wrongful act.[114] This means that the United States may respond to the cyber operation launched by the Russian intelligence agency by hacking back a vulnerable target in the Russian government. Second, like the plea of necessity, countermeasures need not be in kind.[115] Thus, the United States may respond to cyber election interference by imposing trade sanctions that might violate a treaty between the two States.[116] Third, compared to the plea of necessity, the United States would be less likely to create an escalation of conflict in the international community by setting a precedent of imposing countermeasures in response to a cyber operation. This is because, different from the plea of necessity, countermeasures require an attributable internationally wrongful act from a State actor as a condition precedent, which is an arguably clearer standard and, therefore, harder for adversaries of the United States to exploit in the future.

2. Attribution

To establish a basis for countermeasures, the injured State must be able to make both factual and legal attribution to connect the internationally wrongful act to the responsible State.[117]

Factual attribution refers to the degree of certainty that a State is responsible for a cyber operation.[118] Generally, international law requires States to make determinations on factual matters in a "reasonable" standard.[119] *Tallinn Manual 2.0* experts agree that, in the cyber context, if the injured State is mistaken in its factual attribution and imposes countermeasures against a State not responsible for its injury, then the injured State must take responsibility for its breach of international obligations.[120]

Legal attribution considers whether a State is responsible for the cyber operation committed as a matter of law and is governed by the law of State

114. *Id.* at 112–13.

115. *Id.* at 128–29.

116. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 65.

117. *Id.* at 58–59.

118. *Vade Mecum*, *supra* note 24, at 254.

119. TALLINN MANUAL 2.0, *supra* note 22, at 81–82 ("Reasonableness is always context dependent. It depends on such factors as, *inter alia*, the reliability, quantum, directness, nature (e.g., technical data, human intelligence), and specificity of the relevant available information when considered in light of the attendant circumstances and the importance of the right involved.").

120. *See* Articles on State Responsibility, *supra* note 71, art. 49, ¶ 3; TALLINN MANUAL 2.0, *supra* note 22, r. 20, ¶ 16; *see also Vade Mecum*, *supra* note 24, at 254 n.66 (explaining the rationale behind the rule is that "because countermeasures open the door to responses that would otherwise be unlawful[,] [o]ther states should not be required to bear the risk of mistake, even reasonable ones. . .").

responsibility.[121] States are responsible for the acts of their organs, including armed forces, security services, and intelligence agencies.[122] An organ of the State is established either by domestic law or by practice, serving as an instrument of and in complete dependence on the State.[123] GRU would be a clear example of a State organ as a Russian military intelligence agency. A State is responsible for an organ's actions even when the organ agency has acted beyond its assigned responsibility, as long as the agency is acting in an official capacity, rather than a private one.[124] This means the Russian State would be responsible for the election meddling, even if the operation was unauthorized, as long as the operation was not carried out for private purposes. Under these standards, and in light of the factual findings of the ODNI Report, Russia is responsible for all cyber operations by GRU, namely the hacking of the DNC servers and the dissemination of the information collected.

A State is also responsible for actions taken by actors that are not State organs when the actions are pursuant to the "instructions of, or under the direction or control of" the State.[125] International law still has significant gray areas with regard to the exact contour of this rule.[126] However, this Article uses Professor Schmitt's analysis stating that it is at least reasonable to attribute the actions of actors other than the organs of States, including the Internet Research Agency and Russian individuals involved in the social media operations during the 2016 election, to the Russian government because they acted under the strict direction of the Russian State in this incident.[127]

After attributing the election meddling operation to the Russian government, the next question is whether any aspect of the operation has amounted to a breach of an international legal obligation. I will examine the two legal arguments below that have received the most attention with regard to the Russian election meddling: violation of sovereignty and illegal intervention of internal State affairs.

---

121. Articles on State Responsibility, *supra* note 71, art. 2.

122. Articles on State Responsibility, *supra* note 71, art. 4(1); TALLINN MANUAL 2.0, *supra* note 22, r. 15.

123. Articles on State Responsibility, *supra* note 71, art. 4, cmt. 9.

124. *See id.* art 4, cmt. 11.

125. TALLINN MANUAL 2.0, *supra* note 22, r. 17(a).

126. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 58–63 (arguing that a strict application of the international law standards would make it difficult to conclusively attribute the actions of the non-state-organ actors during the 2016 Russia operation to the Russian government).

127. *Id.* at 63.

3. Breach of Legal Obligations: Violation of Sovereignty

Violating another State's sovereignty is a breach of an international obligation, which allows the victim State to respond with countermeasures.[128] It may seem intuitive to accuse the Russian government of violating the sovereignty of the United States by engaging in cyber operations that intended to undermine a major national election. However, a close examination of international law does not support this argument.

Customary international law defines sovereignty as something that signifies "[i]ndependence in regard to a portion of the globe as the right to exercise therein, to the exclusion of any other State, the functions of a State,"[129] indicating two major aspects of sovereignty: territorial integrity and State functions.[130] A violation of either aspect amounts to a violation of State sovereignty.

First, with regard to territorial integrity, *Tallinn Manual 2.0* experts agreed that a remotely conducted cyber operation causing either physical damage to objects (both private and governmental) or injury to persons violates sovereignty.[131] In the cyber context, damage to objects not only means physical damage, but also a loss of functionality, as dysfunction of cyberinfrastructure is often the result of hostile cyber operations.[132] However, *Tallinn Manual 2.0* experts disagreed on the extent of the loss of functionality required to qualify as a violation of territorial integrity.[133] Some insisted that there must be an irreversible loss of function, while, for others, altering or deleting data stored in the cyberinfrastructure would suffice, even if the loss of functionality might be temporary and restorable.[134] An example of the former position would be the Stuxnet operation, which destroyed thousands of Iranian centrifuges,[135] while a major denial-of-service attack would suffice the latter position.[136] However, with respect to the Russian election meddling, neither of the positions above are likely to establish a violation of sovereignty because no known damage or loss of functionality was caused to information and communication technology in the United States.

Second, a remote cyber operation amounting to an interference of

128. TALLINN MANUAL 2.0, *supra* note 22, r. 20.
129. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).
130. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 43.
131. TALLINN MANUAL 2.0, *supra* note 22, at 20.
132. *Id.* at 20–21.
133. *Id.* at 21.
134. *Id.*
135. Sanger, *supra* note 42.
136. TALLINN MANUAL 2.0, *supra* note 22, at 21.

inherently governmental functions also violates the sovereignty of the victim State.[137] Holding national elections would be a classic example of an inherently governmental function, which States enjoy the exclusive right to perform.[138]

However, as a matter of international law, it is unclear exactly what cyber activities amount to an illegal "interference" of such function. The extreme cases are clear. On the one hand, a cyber operation that affects public voting infrastructures, such as voting machines or voting registration systems, would be a clear interference of inherently governmental functions.[139] On the other hand, *Tallinn Manual 2.0* experts agreed that political propaganda during foreign elections would not amount to an illegal interference because prevalent *opinio juris* does not treat hostile political propaganda as a violation of sovereignty.[140]

Given these standards, some aspects of the Russian operation in 2016 were not a violation of the United States' sovereignty. Examples include the Russian's propaganda campaign during the election and the political advertisements on United States social media platforms.[141] A stronger case might exist with regard to the Russian trolls that used fake, or sometimes even stolen, American identities to influence American voters. This is because the Russian trolls manipulated the American electorate's ability to assess the messages relevant to their decision-making process.[142]

However, this is hardly an unassailable argument because it was ultimately the voter who made up his or her own mind when going to the polling station. Propaganda and internet trolls are much less severe than an actual cyber-attack to tamper with voting machines, physically impeding voters from casting their votes. Furthermore, it seems to be an ill-advised political strategy to argue that the foreign trolls, as such, have risen to a level as severe as interfering with a fundamental governmental function because it would project political weakness, rather than strength. The robustness of the American liberal democracy has always been its strongest soft power against authoritarian adversaries like Russia. For that reason, projecting weakness in the democratic system just to hold Russia accountable under international law would not sustain a careful cost-benefit scrutiny.

Finally, the hacking of DNC servers would also fail to amount to a violation of sovereignty because an information-gathering hacking operation

137. *Id.* at 21–22.

138. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 45.

139. *Id.* at 46.

140. TALLINN MANUAL 2.0, *supra* note 22, at 26.

141. *See generally* ODNI REPORT, *supra* note 1.

142. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 47.

only amounts to espionage, which is not prohibited *per se* under international law.[143]

In conclusion, the different aspects of the Russian operation in 2016 do not seem to amount to an illegal violation of sovereignty under international law. Next, I will examine the argument on illegal intervention.

4. Breach of Legal Obligations: Illegal Intervention

The intervention in another State's internal affairs is the second internationally wrongful act that the United States might be able to allege against Russia in order to use countermeasures. Illegal intervention consists of two elements under customary international law: (1) the operation must have an effect on the internal affairs that are part of the victim State's *domaine reserve* and (2) the effect of the operation must be coercive.[144] Similar to the violation of sovereignty, an operation of illegal intervention can target both private and governmental entities[145] and can only be committed by a State actor.[146]

As the ICJ explained in the *Nicaragua* judgment, *domaine reserve* refers to "matters in which each State is permitted by the principle of sovereignty, to decide freely. . . . [F]or example, the choice of a political . . . system."[147] Employing coercive measures regarding such choices amounts to a wrongful intervention as a matter of international law.[148] For the purposes of this Article, a national election clearly falls into the category of *domaine reserve*. The determinative question is whether the Russian election meddling operation was coercive.

Tallinn Manual 2.0 experts agreed that coercion "refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[149] Also, "coercion must be distinguished from persuasion, criticism, public diplomacy, [and] propaganda"[150] because, different from coercion, "such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State or seek no action on the part of the target

143. *See* TALLINN MANUAL 2.0, *supra* note 22, at 168–74 (discussing Rule 32 regarding peacetime cyber espionage).

144. *See* Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 48.

145. *See* TALLINN MANUAL 2.0, *supra* note 22, at 315–16 (discussing the example of attacking another State's commercial banks).

146. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 48.

147. Nicaragua, *supra* note 38, ¶ 205.

148. *Id.*

149. TALLINN MANUAL 2.0, *supra* note 22, at 317.

150. *Id.* at 318.

State at all."[151] The exact standard of coercion, however, is still underdeveloped. Just like the violation of sovereignty, the extreme cases on both ends of the spectrum are clear: in the election context, an attack disabling the voting infrastructure to prevent voters from casting their ballots would be an example of coercion, while mere espionage or propaganda campaigns would not amount to prohibited intervention as a matter of international law. [152]

Therefore, the hacking of the DNC servers, disseminating the information collected from the hacking, and the propaganda campaign on both social media and the Russian State media would not constitute coercive acts. None of these activities compelled the voters to engage in involuntary actions or inactions, but, rather, they were simply influencing and persuading the voters to act in a certain way.

The only activity that arguably amounts to "influencing plus" are the Russian trolls disguised under fake or stolen American identities.[153] This is because by covering its true identity, the troll operation impeded the American electorate's ability to consider the source of information that influences their decision-making process, therefore distorting their ability to control their own governance.[154] However, even if this can be established, the United States might still have a hard time holding Russia accountable under the non-intervention framework because the United States did not come to this issue with clean hands.

The "clean-hands principle" under international law means a State cannot make claims against another State when the former is guilty of the same offense against the latter because international obligations are reciprocal in nature.[155] When it comes to election meddling, the United States has been accused of engaging in many massive intervention operations itself. Some studies show that the United States intervened in elections of other States on more than eighty occasions between 1946 and 2000.[156] In the specific case of Russia, it is alleged that the United States saved its preferred

151. *Id.* at 318–19.

152. Schmitt, *"Virtual" Disenfranchisement*, *supra* note 21, at 50.

153. *Id.* at 51.

154. *Id.*

155. Judge Hudson articulated the definition of the "clean-hand" principle in his Individual Opinion in the *River Meuse* Case before the International Court of Justice: "[i]t would seem . . . that where two parties have assumed an identical or a reciprocal obligation, one party which is engaged in a continuing non-performance of that obligation should not be permitted to take advantage of a similar non-performance of that obligation by the other party." Diversion of Water from the River Meuse (Neth. v. Belg.), Judgement, 1937 P.C.I.J. (ser. A/B) No. 70, ¶ 323 (June 28).

156. Nina Agrawal, *The US Is No Stranger to Interfering in the Elections of Other Countries*, L.A. TIMES (Dec. 21, 2016), http://www.latimes.com/nation/la-na-us-intervention-foreign-elections-20161213-story.html.

candidate, Boris Yeltsin, from near defeat by intervening in the 1996 presidential election.[157] The Russian State media has also accused the United States of attempting to intervene in the 2011 parliamentary elections in Russia.[158] Although the clean-hands principle has not been conclusively accepted as a valid defense in international law,[159] it can create more application difficulties, if the United States attempts to respond to the Russia election meddling via countermeasures on the basis of illegal intervention.

Countermeasures provide many advantages as a response measure. However, in the specific case of the Russian election meddling, there is no solid legal argument available to establish a breach of a legal obligation to justify using them.

This section examined most major alternative response measures available to the United States facing the Russian election meddling operation in the context of *Tallinn Manual 2.0*. It shows that, other than retorsion, the Obama administration did not and the Trump administration does not have an alternative response measure available that is legally unassailable. Furthermore, even when using stretched legal argument to justify the use of these alternative measures, the alternative measures are politically undesirable. Therefore, even though no one seems satisfied with how the United States has been responding to the Russian election meddling, the argument that the United States should hit back harder does not have any grounds as a matter of international law.

That said, I do believe there are measures the United States can take to avoid further election meddling similar to the Russian operation in 2016. In the following section, I will discuss why I believe a practical solution at this point would not be based on international law, but foreign policy.

III. POLICY RECOMMENDATIONS AND CONCLUSION

In this section, I conclude by arguing that a practical course of action for the United States in defending itself against hostile cyber operations like the 2016 Russian election meddling is to make a clear policy declaration. This declaration should specify what kind of cyber operations the United States will not engage in against other States and, at the same time, will not

157. Markar Melkonian, *US Meddling in 1996 Russian Elections in Support of Boris Yeltsin*, GLOBAL RESEARCH (Jan. 13, 2017), https://www.globalresearch.ca/us-meddling-in-1996-russian-elections-in-support-of-boris-yeltsin/5568288.

158. Robert Bridge, *Election-meddling Fiasco Hits US-Russia Relations*, RUSSIA TODAY (Dec. 9, 2011), https://www.rt.com/russia/russia-us-elections-clinton-putin-2012-usaid-427/.

159. *See* Patrick C. R. Terry, *"Don't Do as I Do"—The US Response to Russian and Chinese Cyber Espionage and Public International Law*, 19 GERMAN L.J. 613, 624 (2018) ("Whether the clean-hands-principle has actually developed into a rule of customary international law—as a wholesale preclusion or as a factor in assessing the admissibility of a claim put forward by an injured State—is contentious.").

tolerate if these operations are launched against the United States. For example, the United States can declare that it will refrain from meddling in the elections of other States via cyber means and simultaneously not tolerate any election meddling operations against the United States, regardless of international law's characterization of the operation. This would be an effort of unilateral arms control that respects the international law norm of reciprocal obligations.[160]

The measure previously described is an idea inspired by Professor Jack Goldsmith, who argued that the United States should consider signing an agreement of mutual restraint with its adversaries on certain types of cyber operations, such as election meddling, in exchange for a cease-fire in these areas because they are just so damaging and hard to deter.[161] In my opinion, it is hard to know if a cyber "arms control" agreement with Russia proposed by Professor Goldsmith would be practical in the short term because both countries have different opinions on cyber laws and a negotiation on an agreement like this will likely expose the cyber capabilities of the United States. However, I do believe it is extremely important for the United States to at least unilaterally clarify in a public declaration what it will and will not do with its cyber capabilities, which would have the following two benefits.

First, such a declaration would bring clarity that international law has failed to provide. The international law analysis in this Article confirms one prevalent notion in the academic community of international law and cyber conflict, that is, the *lex lata* international law carries substantial gray areas. The legal uncertainty in this area creates fertile grounds for exploitation, the Russian election meddling being just one example of many, and it is occurring at a growing frequency.[162] The lack of clarity by itself invites more conflicts because parties exploiting the system will make more attempts to explore where the boundaries are. If the "rules of the game" have more clarity, fewer operations would be launched because the cost-benefit analysis would be clearer for adversaries contemplating an operation. Furthermore, more clarity also decreases the chances of escalation and decreases the chances of misinterpretation of actions.

Second, a self-restraint on crucial areas of cyber operation fits today's political reality. The first reality is that although the United States remains

160. *Vade Mecum*, *supra* note 24, at 252 (pointing out that international law seeks balance between obligations and responsibilities between equal sovereignties).

161. Jack Goldsmith, *Contrarian Thoughts on Russia and the Presidential Election*, LAWFARE (Jan 10, 2017), https://www.lawfareblog.com/contrarian-thoughts-russia-and-presidential-election.

162. *See generally* DAVID SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE 295–309 (2018) [hereinafter SANGER, THE PERFECT WEAPON].

the world's strongest, most skillful, and stealthiest cyber power,[163] it is also among the most vulnerable ones when facing a hostile cyber operation.[164] This is mainly because the United States is among one of the most connected and digitalized countries, which creates more targets for our adversaries to attack.[165] Also, in the context of election meddling, being a liberal democracy that protects free speech in the cyberspace could be a vulnerability when facing an authoritarian adversary like Russia because a liberal democracy would have a much harder time containing false information in the age of social media.[166] The second reality is that the United States is not even close to having a perfect defense system in cyberspace.[167] This is partly due to the nature of cyber conflict. As Rebecca Croot articulated, "[d]efenders are playing an elaborate game of whack-a-mole, where a single missed attack can have devastating effects."[168]

Before raising an effective defense against high-stakes attacks is achievable, the only option left is deterrence. The United States' efforts thus far in building deterrence do not seem to be effective.[169] Publicly identifying specific high-stake areas, like elections and critical infrastructures, that the United States will not tolerate as targets of a hostile cyber operation as a matter of policy would enable the United States to employ response measures that might otherwise not be available under international law. This would better deter similar election meddling operations in the future because the United States could employ more severe and sophisticated response measures.

The specifics of this proposed unilateral declaration, however, are beyond the scope of this paper and require further examination. What this Article tries to show is that current international law does not support the popular "we-should-hit-back-harder" argument in light of the Russia election interference. Response measures available in international law are, by nature, reactive, and the laws regulating them contain substantial gray areas prone to exploitation. To create a more effective deterrence

163. Joe Uchill, O*bama: US Government Has Largest Capacity to Hack*, THE HILL (Sept. 6, 2016), https://thehill.com/policy/cybersecurity/294572-obama-us-has-largest-cyber-capacity.

164. *See generally* Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations*, HOOVER INST. (2018), https://www.hoover.org/sites/default/files/research/docs/381100534-strengths-become-vulnerabilities.pdf.

165. *See id.*

166. *See id.*

167. *See* Goldsmith, *supra* note 161; *see also* SANGER, THE PERFECT WEAPON, *supra* note 162, at 308.

168. Crootof, *supra* note 110, at 580.

169. Goldsmith, *supra* note 161.

mechanism, we should consider options outside of international law.