Idaho Law Review

Volume 56 | Number 2 Article 13

Fighting Election Hackers and Trolls on Their Own Turf: Defending Forward in Cyberspace

Jonathan K. Sawmiller

FIGHTING ELECTION HACKERS AND TROLLS ON THEIR OWN TURF: DEFENDING FORWARD IN CYBERSPACE

MAJ JONATHAN K. SAWMILLER*

TABLE OF CONTENTS

When our republic was founded, nations who wished to influence U.S. elections had to rely on the mass media technology of the day, the printing press. In the 1796 presidential election, when the French government attempted to influence electoral college voters in the swing state of Pennsylvania to vote for the perceived pro-French candidate, Thomas Jefferson, it did so through letters by French minister Pierre-Auguste Adet published in a Philadelphia newspaper.[1] Today, foreign adversaries who wish to influence U.S. voters can do so cheaply, efficiently, and covertly through cyberspace,[2] while remaining safely behind their own borders. Worse yet, foreign adversaries can use cyberspace to gain access to U.S. voting infrastructure in order to disrupt elections or even manipulate election results.

In part to counter this new threat to elections, the U.S. Department of Defense (DOD) recently adopted a strategy to "*defend forward* to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[3] This bold approach blazes a new path through unsettled territory in the international law arena. As this essay explains, defending forward is permissible

* Chief of Cyber Operations Law, 16th Air Force / Air Forces Cyber / Joint Force Headquarters – Cyber (Air Force), United States Air Force. J.D., University of Idaho, 2011. LL.M., Space, Cyber, and Telecommunications Law, University of Nebraska, 2018. The views presented are those of the author and do not necessarily represent the views of the Department of Defense or its components. All information is unclassified and derived from publicly-available sources.

1. Alden Fletcher, *Foreign Election Interference in the Founding Era*, LAWFARE (Oct. 25, 2018), https://www.lawfareblog.com/foreign-election-interference-founding-era.

2. The Department of Defense defines cyberspace as "[a] global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS GL-4 (2018).

3. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

under international law, and essential to ensuring future U.S. elections are free from foreign interference.

I. A NEW THREAT TO U.S. ELECTIONS – RUSSIAN CYBER ACTIVITIES IN 2016

The Russian Federation, like its Soviet predecessor, has a long history of conducting covert influence campaigns focused on U.S. presidential elections, using intelligence assets and the U.S. press to support its preferred candidates and disparage those it opposes.[4] In 2016, Russia targeted U.S. elections with a multifaceted influence campaign that for the first time took full advantage of cyberspace. The campaign combined cyberespionage, public release of embarrassing information obtained through hacking, propaganda messaging by Russian government agencies and state-funded media, and proxy organizations employing professional "trolls" for social media messaging.[5] This campaign was "a significant escalation in directness, level of activity, and scope of effort compared to previous operations aimed at US elections."[6]

In March 2016, Russian military hackers from Russian General Staff Main Intelligence Directorate (GRU) Unit 26165 successfully spear-phished employees of the presidential campaign of Hillary Clinton, the Democratic Congressional Campaign Committee (DCCC), and the Democratic National Committee (DNC), acquiring credentials that provided an initial access vector to those organizations' networks.[7] After gaining access, Unit 26165 hackers traversed the networks, exfiltrated copies of emails and documents, covertly monitored the activity of network users, and implanted malware to maintain access.[8] Between July and October 2016, another GRU organization, Unit 74455, publicly released over 50,000 of these documents through fictious personas and anonymous websites.[9] The documents were political dynamite, generating accusations the Clinton campaign had collaborated with the DNC to suppress Democratic primary votes for another candidate, Sen. Bernie Sanders.[10]

Russian state-supported global media, most prominently Russia Today and Sputnik, had overt roles in the influence campaign, while proxy organizations played a covert part.[11] Thirteen Russian nationals and three Russian companies, including the Internet Research Agency (IRA), were indicted in U.S. federal court for committing crimes while engaging in "information warfare against the United

4. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, Intelligence Community Assessment 2017-01D: Assessing Russian Activities and Intentions in Recent US Elections (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

5. *Id.* at 4.

6. *Id.* at 5.

7. Press Release 18-923, Dept. of Justice, Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election (July 13, 2018).

8. *Id.*

9. *Id.*; Indictment at 13–19, United States v. Netyksho, No. 1:18-cr-00215-ABJ (D.D.C. July 13, 2018), https://www.justice.gov/file/1080281/download.

10. *See, e.g.*, Aaron Blake, *Here Are the Latest, Most Damaging Things in the DNC's Leaked Emails*, WASH. POST (July 24, 2016), https://www.washingtonpost.com/news/the-fix/wp/2016/07/24/here-are-the-latest-most-damaging-things-in-the-dncs-leaked-emails/; Hilary Hanson, *Leaked Emails Suggest DNC Was Conspiring Against Bernie Sanders*, HUFFINGTON POST (July 26, 2016), https://www.huffpost.com/entry/wikileaks-dnc-bernie-sanders_n_579381fbe4b02d5d5ed1d157.

11. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 4.

States."[12] The indictment alleged that they "operated social media pages and groups designed to attract U.S. audiences," which "falsely claimed to be controlled by U.S. activists," and became their "means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the presidential election of 2016."[13] The indicted Russian oligarch Yevgeniy Viktorovich Prigozhin, who funded the IRA, "is a close Putin ally with ties to Russian intelligence."[14]

In moves that showed Russian intent to move beyond just an influence campaign into election manipulation, GRU personnel hacked into the website of a state board of elections and stole personally identifiable information related to approximately 500,000 voters.[15] They also hacked into the computers of a U.S. company that supplied software used to verify voter registration information for the 2016 U.S. elections.[16] Fortunately, it does not appear they were able to access electronic voting infrastructure and manipulate votes or voting results.[17]

II. A NEW RESPONSE—DEFENDING FORWARD IN CYBERSPACE

In August 2018, Congress responded by authorizing military defense of U.S. elections in cyberspace against Russia, China, North Korea, and Iran.[18] Subject to a determination that these nations are "conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes," Congress authorized the President and Secretary of Defense "to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks."[19]

In September 2018, the President issued a National Cyber Strategy, declaring that the U.S. will use all instruments of national power, including "military (both kinetic and cyber)," to "prevent, respond to, and deter malicious cyber activity against the United States."[20] Around the same time, the President issued National Security Presidential Memorandum 13, *United States Cyber Operations Policy*,

12. Press Release 18-198, Dept. of Justice, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System, (Feb. 16, 2018), https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

13. Indictment at 3, United States v. Internet Research Agency LLC, No. 1:18-cr-00032-DLF (D.D.C., Feb. 16, 2018), https://www.justice.gov/file/1035477/download.

14. *Id.* at 7–8; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 4, at 4.

15. United States v. Netyksho, No. 1:18-cr-00215-ABJ (D.D.C. July 13, 2018).

16. *Id.*

17. *Id.*

18. National Defense Authorization Act, Pub. L. No. 115-232, 132 Stat. 1636, 1642 (2018).

19. *Id.*

20. Letter from Donald J. Trump, President, U.S., on National Cyber Strategy of the United States of America, to the American People (Sept. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"which allows for the delegation of well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace."[21]

Also in September 2018, the DOD issued its own DOD Cyber Strategy, explicitly recognizing that the U.S. is "engaged in a long-term strategic competition with China and Russia," including "persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation . . . ."[22] In response, the DOD "must take action in cyberspace during day-to-day competition . . . to defend U.S. interests."[23] In a change to previous strategy focused on defensive actions within U.S. networks, the 2018 Strategy declares that the DOD "will *defend forward* to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[24] Geographic distance offers no safety due to the globally interconnected nature of cyberspace, so "attempting to protect from cyber attacks at or near the point of impact or just along international territorial boundary lines is not only artificial and naive, it is also ineffective and self-defeating."[25] Thus, in cyberspace, the U.S. "must *defend forward*, engaging adversaries before their actions can affect intended targets."[26]

The commander of U.S. Cyber Command explained that "[i]n practice, this means confronting our adversaries from where they launch cyber attacks . . . ."[27] Cyber Command forces "must operate against our enemies on their virtual territory . . . . Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment."[28] Maneuvering "as close as possible to the origin of adversary activity . . . [allows Cyber Command] to expose adversaries' weaknesses . . . [and] learn their intentions and capabilities,"[29] then take action to deny, degrade, disrupt, destroy, or manipulate (D4M)[30] cyber

---

21. Hon. Paul Ney, Jr., Dep't of Defense, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

22. DEP'T OF DEF., *supra* note 3, at 1.

23. Id.

24. *Id.* (emphasis added).

25. Paul Ney, Jr., *Charney Lecture: The Rule of Law in International Security Affairs: A U.S. Defense Department Perspective*, 52 VAND. J. TRANSNAT'L L. 773, 778–79 (2019).

26. *Id.* (emphasis added).

27. Paul M. Nakasone, Gen., Commander U. S. Cyber Command, Before the Senate Committee on Armed Services (Feb. 14, 2019), https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

28. Paul M. Nakasone, *A Cyber Force for Persistent Operations*, 92 JOINT FORCES Q. 12, 12 (2019).

29. *Achieve and Maintain Cyberspace Superiority*, COMMAND VISION FOR US CYBER COMMAND, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 (last visited May 20, 2020).

30. *See* JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12, CYBERSPACE OPERATIONS II-7 (2018). Degrade means "[t]o deny access to, or operation of, a target to a level represented as a percentage of capacity." *Id.* Disrupt means "[t]o completely but temporarily deny access to, or operation of, a target for a period of time." *Id.* Destroy means "to completely and irreparably deny access to, or operation of, a target . . . ." *Id.* Manipulation "controls or changes information, information systems, and/or networks in gray or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. . . .The targeted network may appear to operate normally until secondary or tertiary effects, including physical effects, reveal evidence of the logical first-order effect." *Id.*

infrastructure owned, operated, or controlled by the adversary. These D4M actions are obviously executed without the consent of the targeted adversary entity, and in the DOD's view may also be executed without the consent of the States in whose territory the targeted cyber infrastructure is located.[31]

In 2018, the DOD engaged in an interagency effort "to defend the integrity of America's 2018 mid-term elections."[32] U.S. Cyber Command and the National Security Agency "undertook an initiative known as the Russia Small Group to protect the elections from foreign interference and influence[,] . . . [taking part in] the collective intelligence and defense effort that demonstrated persistent engagement in practice."[33] According to media reports, this defense effort included military cyber operations against the IRA in St. Petersburg, Russia, that "blocked Internet access . . . . [for the IRA and] "basically took the IRA offline."[34]

Some former intelligence and cybersecurity officials categorized the operation as a signal meant to deter foreign misbehavior online and praised it as an appropriate tool of statecraft.[35] In contrast, one scholar argued this action was a "crossing of the Rubicon" in State relations, an event so significant that it might possibly "set a new standard for 'sub-warlike' cyber activity that begins the creation of new international norms of behavior . . . ."[36] Other scholars pointed out that international law is murky in this area, with scholarly disagreement on what rules of international law apply to cyber operations that affect data but do not result in death or injury to persons or damage to physical property.[37] Some scholars argue that the concept of State sovereignty prohibits such operations,[38] and others take the opposite view.[39] For its part, the Russian government refused to take a public position characterizing the legal nature of the reported U.S. cyber operation against

31. Ney, *supra* note 21.

32. Nakasone, *supra* note 27.

33. *Id.*

34. Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019), https://www.washingtonpost.com/world/ national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

35. Andy Greenberg, *US Hackers' Strike on Russian Trolls Sends a Message—but What Kind?*, WIRED (Feb. 27, 2019), https://www.wired.com/story/cyber-command-ira-strike-sends-signal/.

36. Paul Rosenzweig, *The New Contours of Cyber Conflict*, LAWFARE (Feb. 27, 2019, 12:19 PM), https://www.lawfareblog.com/new-contours-cyber-conflict.

37. Charlie Dunlap, *Cyber Norm Development: Is the U.S. at an Inflection Point?* LAWFIRE (Apr. 22, 2019), https://sites.duke.edu/lawfire/2019/04/22/cyber-norm-development-is-the-u-s-at-an-inflection-point/; Max Smeets & Herb Lin, *An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward*, LAWFARE (Nov. 28, 2018, 8:00 AM), https://www.lawfareblog.com/ outcome-based-analysis-us-cyber-strategy-persistence-defend-forward.

38. Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AJIL UNBOUND 213 (2017).

39. Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207 (2017).

the IRA.[40] In response to media reports, a spokesman for President Putin would say only with typical hyperbole that "U.S. territory is constantly being used to organize a huge number of cyber attacks against various Russian organizations. That's the reality with which we live."[41]

III. INTERNATIONAL LAW FRAMEWORK FOR ANALYZING DEFEND FORWARD CYBER OPERATIONS

It is generally undisputed that conduct of States in cyberspace is governed by existing international law, as it is when acting in other domains.[42] Rules of international law are found in international agreements to which States are parties, and also arise from customary international law, formed by "general and consistent practice of states followed by them from a sense of legal obligation," a concept called *opinio juris*."[43] However, despite fifteen years of effort by States through the U.N. Group of Governmental Experts process, a broad international consensus is currently still lacking on *how* specific bodies of existing international law, such as the *jus ad bellum*, apply to States' actions in cyberspace.[44] Furthermore, as a matter of State sovereignty, unless it chooses to be bound by "prohibitive rules" of international law, a State remains free to engage in conduct "which it regards as best and most suitable" to achieve its own national interests, even though that conduct may violate the domestic law of another State or otherwise be unfriendly to other States.[45]

The DOD takes the position that international law does not generally prohibit non-consensual cyber operations in another State's territory, unless the cyber operations constitute a use of force under the *jus ad bellum* or a prohibited coercive intervention in domestic affairs.[46] This position is key to justifying the DOD's adoption of the "defend forward" policy in its 2018 Cyber Strategy.[47] Because of this position, the DOD believes that its "commitment to defend forward[,] including to counter foreign cyber activity targeting the United States[,] comports with our obligations under international law and our commitment to the rules-based international order."[48] Exactly when a cyber operation (or a kinetic operation, for that matter) rises to the level of a use of force or coercive intervention is unsettled in international law, but some standards do exist and can be applied.

---

40. Polina Nikolskaya & Katya Golubkova, *Kremlin Says Cyber Attacks on Russia Often Launched from U.S. Territory*, REUTERS (Feb. 27, 2019, 3:02 am), https://www.reuters.com/article/us-usa-trump-russia-kremlin/kremlin-says-cyber-attacks-on-russia-often-launched-from-u-s-territory-idUSKCN1QG183.

41. *Id.*

42. U.N. Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).

43. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) (Am. Law Inst. 1987).

44. Michele G. Markoff, Deputy Coordinator, U.S. State Dep't, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017).

45. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at ¶ 46 (Sept. 7).

46. Ney, *supra* note 21.

47. *Id.*

48. *Id.*

A. Jus Ad Bellum Prohibition on the Use of Force

The modern framework for the *jus ad bellum*, the body of customary and treaty international law governing the resort to use of force by States, is the Charter of the United Nations. Its Article 2(4) requires all member states to "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."[49] The consensus view of States and scholars is that Article 2(4) prohibits all use of force in international relations, except as permitted by the Charter.[50]

The phrase "use of force" is not defined in the Charter, and international consensus is lacking over its precise meaning. In the scholarly view contemporaneous with the establishment of the Charter, use of force "is commonly understood to imply a military attack, an 'armed attack,'" with a State-controlled entity using traditional or non-traditional weapons such as poison gas "employed for the destruction of life and property" against another State,[51] and refers to "armed force" as distinguished from political or economic pressure.[52] Though we are in the modern era of cyberspace operations, the prohibition still applies to any use of force, regardless of the type of weapons employed.[53] As Professor Dinstein puts it, "when studied in context, the term 'force' in Article 2(4) must denote violence. It does not matter what specific means—kinetic or electronic—are used to bring it about, but the end result must be that violence occurs or is threatened."[54]

While not entirely settled, it is generally accepted that for violence by one State against another to be a use of force, it must reach a certain threshold of gravity.[55] It is unsettled in international law precisely where the threshold lies, and allegations of use of force are generally resolved through state action driven by geopolitical considerations rather than litigation based on legal definitions. The International Court of Justice has held that temporary entry by warships into territorial waters to remove illegally laid mines without causing injury or damage to anything other than the mines was not a use of force,[56] while laying mines in territorial waters, bombing ports, oil pipelines, and storage tanks (spilling millions of gallons of fuel), and rocketing a naval base constituted an illegal use of force.[57]

---

49. U.N. Charter art. 2, ¶ 4.

50. YORAM DINSTEIN, WAR, AGGRESSION, AND SELF-DEFENCE 80—83 (5th ed. 2011).

51. IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362 (1963).

52. LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE, VOL. II DISPUTES, WAR AND NEUTRALITY 153 (H. Lauterpacht ed., 7th ed. 1952).

53. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 18, 39 (July 8).

54. DINSTEIN, *supra* note 50, at 88.

55. OLIVIER CORTEN, THE LAW AGAINST WAR 70 (2010); MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 54 (2014).

56. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 35 (Apr. 9).

57. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 349–50 (June 27).

In assessing whether a particular cyber operation constitutes a use of force, the DOD applies a physical effects framework. It considers "whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine."[58] The DOD cites a former State Department legal advisor who has offered three examples that would qualify as a use force and involve "significant destruction."[59] These are cyber operations that (1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes. [60] The U.K. government takes a similar stance with regards to cyber operations resulting in death and destruction on an equivalent scale to an unlawful use of force or armed attack if committed with kinetic weapons, though to the examples of nuclear meltdown and crashing aircraft it adds targeting of essential medical services,[61] likely because of its experience with WannaCry ransomware disrupting medical care to thousands of National Health System patients across the U.K.[62]

While the examples above all involve significant destruction of property, injury, or loss of life, some scholars assert that cyber operations that are intended to cause *any* damage or destruction of physical objects are of sufficient gravity to qualify as a use of force.[63] These scholars also propose extending the definition of use of force beyond physical effects. They propose that states employ a multi-factor approach that "focuses on both the level of harm inflicted and certain qualitative elements of a particular cyber operation" to assess its overall "scale and effects," which they say may include economic or other non-physical effects.[64]

The U.S. and U.K. have rejected this view and focus on physical effects, many states are silent on their view of what constitutes a use of force in cyberspace, and a few states appear open to considering non-physical effects. France recently stated it would not rule out the possibility that it would choose to characterize a cyber operation without physical effects as a use of force against it.[65] The Netherlands has also gone on record supporting the general conclusions of a report stating that a cyber operation targeting the entire Dutch financial system or preventing the

58. Ney, *supra* note 21.

59. DEP'T. OF DEFENSE, LAW OF WAR MANUAL § 16.3.1 (2016) (citing Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-agency Legal Conference* (Sept. 18, 2012), *reprinted in* 54 HARV. INT'L L. J. ONLINE 1, 3–4 (Dec. 2012)).

60. *Id.*

61. Jeremy Wright, Attorney General of the U.K., Cyber and International Law in the 21st Century (May 23, 2018) (transcript available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century).

62. Matthew Field, *WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled*, TELEGRAPH (Oct. 11, 2018), https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

63. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 48 (Michael N. Schmitt & Liss Vihul eds., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

64. *Id.*

65. Ministère Des Armées [Ministry of Defense of the Republic of France], International Law Applied to Operations in Cyberspace (2019).

government from carrying out essential tasks such as policing or taxation would qualify as an armed attack,[66] a grave form of illegal use of force.

Applying a physical effects framework, it is reasonable to conclude that the U.S. can execute cyber operations precisely delivering D4M effects against the logical network layer[67] of foreign actors' information technology (IT) infrastructure used for hacking and influence operations, to prevent them from using this infrastructure to interfere with or influence U.S. elections, without violating the prohibition on the use of force. This is because D4M effects can be directed against data and logical processes of IT infrastructure without proximately causing injury or death to persons, or damage or destruction to physical objects, including computer hardware. The U.S. could use "impact" techniques that directly affect only data and logical processes of IT infrastructure,[68] with the secondary effects limited through choice of targets. For instance, executing a disk content wipe technique[69] against storage devices on an IT network used solely for social media influence operations would be very unlikely to cause a secondary effect of injury or death to persons, though the same technique directed against health provider IT networks might. In contrast, D4M effects directed at operational technology (OT) infrastructure, such as Industrial Control Systems (ICS), would be far more likely to proximately cause injury or death to persons, or damage or destruction to physical objects.[70]

66. Ank Bijleveld, Minister of Defence, Keynote address by the Minister of Defence, Ms. Ank Bijleveld, Marking the First Anniversary of the Tallinn Manual 2.0 (June 20, 2018) (transcript available at https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018).

67. DEP'T OF DEF., JOINT PUBLICATION 3-12: CYBERSPACE OPERATIONS I-3–I-4 (2018) ("The logical network layer consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not necessarily tied to a specific physical link or node, but to their ability to be addressed logically and exchange or process data). Individual links and nodes are represented in the logical layer but so are various distributed elements of cyberspace, including data, applications, and network processes not tied to a single node.").

68. See the ATT&CK Matrix for Enterprise IT Systems, a knowledge base of cyber tactics and techniques based on observations of real-world threat actors, for a description of common impact techniques. ATT&CK MATRIX FOR ENTERPRISE, https://attack.mitre.org/ (last visited May 20, 2020).

69. DISK CONTENT WIPE, https://attack.mitre.org/techniques/T1488/ (last visited May 20, 2020).

70. *See* ATT&CK FOR INDUSTRIAL CONTROL SYSTEMS, https://collaborate.mitre.org/attackics/ index.php/Main_Page (last visited May 20, 2020).

B. Prohibition on Coercive Intervention

Under the customary international law principle of non-intervention, cyber operations that do not rise to the level of a use of force are still prohibited if they coercively intervene in the core internal functions of another State, "such as the choice of political, economic, or cultural system."[71] This narrow zone of "matters in which each State is permitted, by the principle of State sovereignty, to decide freely" covered by the non-intervention principle is commonly referred to as the *domaine réservé* of a State.[72]

It is "imperative to distinguish intervention from interference" because intervention in *domaine réservé* is prohibited, while interference is permissible and "regarded as an inevitable by-product of an increasingly globalised world order where states are constantly interacting."[73] To be an internationally wrongful intervention, a State's actions "must be forcible, dictatorial, or otherwise coercive, in effect depriving the State intervened against of control over the matter in question."[74] Some types of state conduct are generally agreed to be outside the scope of prohibition, whether executed in cyberspace or other domains, such as espionage[75] and propaganda.[76]

However, "the precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space."[77] Aside from the general recognition of its high threshold, customary international law offers little guidance on what level of coercion raises an act from a lawful act of pressure to an internationally wrongful act of coercive interference.[78] The non-intervention principle is often breached by States, and "the precise contours and application of the prohibition of intervention are unclear in light of ever-evolving and increasingly intertwined international relations."[79]

In the view of the U.S., shared by other countries, "cyber operations by a State that interfere with another country's ability to hold an election or that manipulate another country's election results would be a clear violation of this prohibition."[80] The U.K. has taken the position that cyber operations that intervene in the fundamental operation of Parliament or in the stability of the U.K. financial system would violate the non-intervention principle.[81]

---

71. Ney, *supra* note 21; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

72. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 108 (June 27).

73. RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW 63 (2018).

74. OPPENHEIM'S INTERNATIONAL LAW, VOL. 1, PEACE 432 (Robert Jennings & Arthur Watts eds., 9th ed. 2008).

75. BUCHAN, *supra* note 73, at 65.

76. Sean Watts, *Low Intensity Cyber Operations and the Principle of Non-Intervention*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 250, 261 (Jens David Ohlin et al. eds., 2015).

77. Wright, *supra* note 61.

78. See Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law*?, 95 TEX. L. REV. 1579, 1587–88 (2017).

79. TALLINN MANUAL 2.0, *supra* note 64, at 314.

80. Ney, *supra* note 25 at 779.

81. Wright, *supra* note 61.

Applying the above standards, it is reasonable to conclude that the U.S. can execute cyber operations precisely delivering D4M effects against the logical network layer[82] of foreign actors' information technology (IT) infrastructure used for hacking and influence operations, to prevent them from using this infrastructure to interfere with or influence U.S. elections, without violating the prohibition on coercive non-intervention in domestic affairs. This is because foreign State actors do not have a sovereign right, as a core internal function of their States, to interfere with or influence elections in the U.S. In fact, the opposite is true. The choice of political system is a matter each State is permitted by the principle of State sovereignty to decide freely, and if a foreign State deprived the U.S. of control over its own elections through cyber operations, then that State would be in breach of the prohibition.

C. Sovereignty

Some scholars assert that cyber operations causing consequences to manifest in cyber infrastructure located in another State, including loss of functionality of computer systems due to data deletion or manipulation without physical effects, constitute a violation of a universal customary international law rule of "territorial sovereignty" that prohibits all nonconsensual access to its territory. [83] However, other scholars point out that sovereignty is a fundamental general principle that serves as a foundation for a State's development of specific rules of international law, not a universal rule prohibiting nonconsensual access to territory.[84] Rather, the specific rules that protect sovereign territory from foreign intrusion develop through international agreements and state practice, and "the fact that states have developed vastly different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace."[85] To further illustrate the point, there is no international convention prohibiting espionage, and States routinely practice espionage against each other, including espionage involving some degree of virtual and physical intrusion, showing the absence of a customary international law norm against it.[86]

The U.S. and U.K. both recognize the role of State sovereignty as a foundational principle that undergirds specific rules of international law, but reject the idea that from it is automatically extrapolated a specific rule in customary international law prohibiting cyber activity which doesn't rise to the level of a prohibited coercive intervention or use of force.[87] The DOD view is that there currently "is not sufficiently widespread and consistent State practice resulting

82. *See* DEP'T OF DEF., *supra* note 67 (defining logical network layer).
83. TALLINN MANUAL 2.0, *supra* note 63, at 17–27.
84. Gary Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207 (2017).
85. *Id.* at 210.
86. Ney, *supra* note 21; RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW 65 (2018).
87. Ney, *supra* note 21; Wright, *supra* note 61.

from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory."[88] While the DOD recognizes that there are differences of opinion among States, this suggests that State practice and *opinio juris* are presently not settled on this issue, particularly since many States have remained publicly silent in the face of numerous publicly known cyber intrusions into foreign networks.[89]

D. Legal Gray Zone and Retorsion

If defend forward cyber operations are carefully kept below the level of a use of force and coercive intervention, how might they be characterized under international law? One way of viewing them is that they fall within a "gray zone"—an arena of state conduct that is simply not regulated by current international law.[90] International law is positive and consent-based, arising from sovereign States' voluntary choices to be bound by "prohibitive rules" of international law.[91] Outside the boundaries of such rules, States remain free to act as they view best and most suitable for their own national interests,[92] including conducting cyber operations against other States with whom they are engaged in strategic competition.

Some defend forward operations conducted in response to specific adversary cyber actions can be viewed as acts of retorsion. "An act of retorsion is an unfriendly, but not otherwise unlawful measure, with sanctions and expulsion of diplomatic personnel being the most emblematic and frequent. The cyber operations to which an act of retorsion responds need not constitute an internationally wrongful act, although they may."[93] Acts of retorsion can include "under the threshold" cyber operations against the actor that initiated the first-in-time unfriendly operation.[94] The alleged U.S. cyber operations in response to Russian 2016 election meddling, as reported by the news media, would fall into the category of retorsion.

A recent survey of State practice in responding to cyber operations against them showed that States generally do not accept or rely on the normative categories of international law, such as use of force, coercive interventions, or violations of sovereignty, to draw meaningful legal distinctions in their reactions to cyber operations.[95] Rather, "states seem to prefer to engage in cyberoperations and counteroperations 'below the radar,' and to retain, for the time being, some degree of stability in cyberspace by developing 'parallel tracks' of restricted attacks, covert retaliation, and overt retorsion, subject to certain notions of proportionality."[96]

---

88. Ney, *supra* note 21.

89. *Id.*

90. See Harvey Rishikof et al., *Gray Zone as State Actors Continue to Wage Cyberwar on the United States, They Have a Powerful Ally–Gaps and Ambiguities in the Law*, 104 A.B.A. J. 30, 32 (2018).

91. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, ¶ 46 (Sept. 7).

92. *Id.*

93. Michael Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 64 (2018).

94. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L. L. 583, 645 (2018).

95. *Id.* at 653–54.

96. *Id.* at 654.

IV. THE FUTURE

What will DOD cyber operations defending U.S. elections look like a decade from now? Presumably, these operations will expand in size and reach. It's unlikely that adversary attempts at election hacking and influence operations against the U.S. will decrease. Because of the success that Russia enjoyed in 2016, which is still resounding in the U.S. political process today, it is likely that Russia will continue to direct influence operations at U.S. elections.[97] As barriers to entry to fielding effective cyber forces and capabilities continue to drop, more adversary nations will achieve a relatively low-cost and low-risk capacity to conduct cyber operations against U.S. elections. While only Russia targeted the 2016 elections, already the U.S. government has warned American voters that "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions" in the 2020 elections.[98] They will attempt to do so "through a variety of means, including social media campaigns, directing disinformation operations or conducting disruptive or destructive cyber-attacks on state and local infrastructure."[99]

It's likely the DOD and its defend forward strategy will continue to play a key role in defending U.S. elections against foreign interference and influence in cyberspace. Already, in response to adversary threats to the 2020 elections, the DOD, along with U.S. law enforcement and intelligence agencies, has "ma[de] it clear to foreign actors that any effort to undermine our democratic processes will be met with sharp consequences."[100] The U.S. Cyberspace Solarium Commission, a bipartisan, intergovernmental body established by Congress to develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences, including cyber-enabled election interference, recently recommended that the DOD's defend forward approach be expanded to include all instruments of national power, in an "overall integrated effort to apply every authority, access, and capability possible (e.g., laws, financial regulation, diplomacy, education) to the defense of cyberspace in a manner consistent with international law."[101]

How adversaries will react to the new strategy is still unknown and will be key to determining the future viability of the defend forward strategy. Will DOD cyber

---

97. ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 288 (2d ed. 2017).

98. *Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections*, DEP'T HOMELAND SECURITY (Nov. 5, 2019), https://www.dhs.gov/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020-elections.

99. *Id.*

100. Maggie Miller, *Senior Administration Officials Warn of Foreign Influence Campaigns Ahead of Super Tuesday*, HILL (Mar. 2, 2020, 4:21 PM), https://thehill.com/policy/cybersecurity/485551-senior-administration-officials-warn-of-foreign-influence-campaigns.

101. U.S. CYBERSPACE SOLARIUM COMM'N, OFFICIAL REPORT 24 (2020), https://www.solarium.gov/ report.

operations impose costs that create deterrence from future election meddling, and steer our adversaries back towards global norms of respect for the right of sovereign States to choose their leaders through democratic processes?[102] Or will the DOD be called on to persistently defend forward in cyberspace, to disrupt and degrade adversary capability to execute intended operations against U.S. 2030 elections? Perhaps in a decade we'll know, but the latter is a more likely scenario.

What about developments in international law? Unfortunately, given the relative intransigence of some States during the U.N. G.G.E processes from 2002-2017 that sought to establish broad State consensus on cyber-specific rules of international law and failed,[103] it's similarly unlikely that current U.N. attempts[104] will succeed in this endeavor. Instead, it's more likely that smaller groups of States will work towards regional or bilateral understandings, with the goal of establishing voluntary norms that may shape future State acceptance of binding international agreements.[105] At any rate, State practice will have had another ten years to evolve. Perhaps States will begin to coalesce their actions around a common view of how existing international law applies to cyber operations, working towards *opinio juris* and establishment of cyber-specific rules of international law that address election influence operations and permissible ways to respond to them.

Under international law as it stands today, the DOD's bold new approach of defending forward in cyberspace is not prohibited conduct for the U.S. or any other sovereign State. A decade in the future, defending forward in cyberspace is likely to remain both internationally lawful and essential to ensuring American elections are free from interference and influence by foreign States.

102. See Jason Healey, *The Implications of Persistent (and Permanent) Engagement in Cyberspace*, J. OF CYBERSECURITY, Aug, 2019.

103. Anders Henriksen, *The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace*, 5 J. CYBERSECURITY 1, 3 (2019).

104. *See Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. OFFICE FOR DISARMAMENT AFFAIRS, https://www.un.org/disarmament/ict-security/ (last visited May 20, 2020).

105. Stefan Soesanto & Fosca D'Incau, *The UN GGE is Dead: Time to Fall Forward*, EUROPEAN COUNCIL ON FOREIGN RELATIONS (Aug. 15, 2017), https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance#.