State Responsibility and Attribution of Cyber Intrusions After *Tallinn 2.0*

William Banks*

On July 22, 2016, WikiLeaks released a collection of more than 18,000 e-mails from the formally impartial Democratic National Committee (DNC) that showed bias against the Bernie Sanders campaign and a cozy relationship between the DNC and its top officials with the Hillary Clinton campaign.[1] Apparently timed to embarrass and disrupt the DNC and the Clinton campaign on the eve of the Democratic National Convention, the leak led to the resignation of key DNC officials, a formal apology to Senator Sanders and his supporters, and lingering impressions that the DNC was anything but neutral during the campaign and that the Clinton campaign could not be trusted.[2] On October 7, WikiLeaks began serial publication of thousands of e-mails to and from John D. Podesta, Mrs. Clinton's campaign manager. Released nearly daily over the last month of the campaign, the Podesta e-mails led to news reports and manipulation on social media that focused on tensions inside the Clinton campaign and campaign insiders' opinions that Clinton was not a strong candidate, among other things.[3] A second batch of DNC e-mails was released on November 6, two days before the election.[4]

The Federal Bureau of Investigation (FBI) first contacted the DNC in September 2015 to warn the Democrats that at least one of their computer systems had been compromised by hackers linked to the Russian

---

* Board of Advisors Distinguished Professor, Syracuse University College of Law; Professor of Public Administration and International Affairs, Maxwell School of Citizenship and Public Affairs, Syracuse University. The author thanks Taylor Henry, Syracuse University College of Law, J.D. 2018, for excellent research assistance.

1. Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [https://perma.cc/6GU5-CF2K]; Tom Hamburger & Karen Tumulty, *WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, WASH. POST (July 22, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.1e13fbea91df [https://perma.cc/5QUF-8YA9].

2. *Democratic National Committee Apologizes to Sanders Over Emails*, REUTERS (July 25, 2016), http://www.reuters.com/article/us-usa-election-dnc-statement-idUSKCN1052BN [https://perma.cc/36UY-FE75].

3. Lipton et al., *supra* note 1; Evan Osnos et al., *Trump, Putin, and the New Cold War: What Lay Behind Russia's Interference in the 2016 Election—and What Lies Ahead?*, NEW YORKER 40, 52–53 (Mar. 6, 2017), http://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war [https://perma.cc/WN33-Z2UM].

4. Joe Uchill, *WikiLeaks Releases New DNC Emails Day Before Election*, HILL (Nov. 7, 2016), http://thehill.com/policy/cybersecurity/304648-wikileaks-releases-new-dnc-emails-suffers-cyberattack [https://perma.cc/8UWR-UFWX].

government.[5] Inept responses and inattention from the DNC staff and casual follow-up from the FBI allowed the hackers free reign in DNC networks for more than six months until senior DNC officials learned of the hacks and hired a private security firm to protect their systems.[6]

Meanwhile, reports that Russian intelligence agencies were responsible for hacking the DNC, disseminating the materials to WikiLeaks, and encouraging or reporting "fake news" on social media and in nonmainstream publications swirled around the last months of the presidential election campaign.[7] A hacker calling itself Guccifer 2.0 took credit for the leaks,[8] and WikiLeaks would not reveal its source.[9] Over the remainder of the summer and early fall of 2016, several cyber experts and private security firms publicly claimed that the DNC hack had been carried out by Russian intelligence operatives and was directly controlled by the Russian government.[10]

On October 7, the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) issued a joint statement that the Intelligence Community was confident that the Russian government was responsible for the hack and publication of the materials in its attempt to "interfere with the US election process."[11] Although the joint

5. Lipton et al., *supra* note 1.

6. *Id.*

7. Sam Biddle, *Here's the Public Evidence Russia Hacked the DNC—It's Not Enough*, INTERCEPT (Dec. 14, 2016), https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/ [https://perma.cc/9UUZ-XERG]; Osnos et al., *supra* note 3.

8. Ellen Nakashima, *Cyber Researchers Confirm Russian Government Hack of Democratic National Committee*, WASH. POST (June 20, 2016), https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html?utm_term=.ec7d861e243c [https://perma.cc/KX3A-FV6E].

9. Hannah Albarazi, *WikiLeaks' DNC Email Leak Reveals Off the Record Media Correspondence*, CBS: SF BAY AREA (July 22, 2016), http://sanfrancisco.cbslocal.com/2016/07/22/hilary-leaks-wikileaks-releases-democratic-national-committee-emails/ [https://perma.cc/M3SC-2SVB].

10. Lucian Kim, *Russian Security Expert Maintains Putin Was Behind DNC Hack*, NPR (Jan. 26, 2017), http://www.npr.org/2017/01/26/511851752/russian-security-expert-maintains-putin-was-behind-dnc-hack [https://perma.cc/3BP5-7875]; Ellen Nakashima, *Cybersecurity Firm Finds Evidence That Russian Military Unit Was Behind DNC Hack*, WASH. POST (Dec. 22, 2016), https://www.washingtonpost.com/world/national-security/cybersecurity-firm-finds-a-link-between-dnc-hack-and-ukrainian-artillery/2016/12/21/47bf1f5a-c7e3-11e6-bf4b-2c064d32a4bf_story.html?utm_term=.527e73a904ef [https://perma.cc/9JZ4-GE8U]; Sam Thielman, *DNC Email Leak: Russian Hackers Cozy Bear and Fancy Bear Behind Breach*, GUARDIAN (July 26, 2016), https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2 [https://perma.cc/9N7B-ZMLK].

11. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, Director of National Intelligence (Oct. 7, 2016), https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement [https://perma.cc/4VXK-65F9]; Ellen Nakashima, *U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections*, WASH. POST (Oct. 7, 2016), https://www.washingtonpost.com/world/national-security/us-government-

statement constituted an official attribution of the DNC hack to the Russian government, the statement provided no evidence to support its assessment.

On December 9, the Central Intelligence Agency (CIA) briefed members of Congress on an Intelligence Community assessment that concluded the Russian government conducted these cyber operations during the 2016 presidential election in order to assist the candidacy of Donald Trump.[12] According to the Intelligence Community assessment, intelligence assets with direct ties to the Kremlin provided the DNC e-mails as well as others from prominent Hillary Clinton supporters, such as campaign chairman John Podesta, to WikiLeaks.[13] Their conclusion that Russia was behind the hack was delivered with "high confidence."[14] The CIA briefing was not a formal assessment by the Intelligence Community because of minor disagreements among the agencies and because intelligence officials did not yet have specific intelligence demonstrating that Russian government officials directed the hackers to pass along their information to WikiLeaks.[15] On December 16, CIA Director John Brennan stated that the FBI and DNI supported the CIA's conclusion that the Russian government interfered in the election to assist the Trump candidacy and to attack U.S. democratic processes.[16]

President Barack Obama reportedly raised the issue of Russian hacking with Russian President Vladimir Putin in a side meeting during the G20 summit in China in September 2016.[17] President Obama claimed that Russian hacking stopped after his meeting with Putin.[18] The hacking may

officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.655d3d88e3a6 [https://perma.cc/P8JE-T9MJ].

12. Adam Entous et al., *Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House*, WASH. POST (Dec. 9, 2016), https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.ccd9268101b8 [https://perma.cc/4LMY-LUU3].

13. *Id.*; David Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html [https://perma.cc/6CPG-6QJP].

14. Sanger & Shane, *supra* note 13.

15. Entous et al., *supra* note 12; *see also* Biddle, *supra* note 7 (detailing the limited evidence of links between the Russian government and WikiLeaks).

16. Adam Entous & Ellen Nakashima, *FBI in Agreement with CIA That Russia Aimed to Help Trump Win White House*, WASH. POST (Dec. 16, 2016), https://www.washingtonpost.com/politics/clinton-blames-putins-personal-grudge-against-her-for-election-interference/2016/12/16/12f36250-c3be-11e6-8422-eac61c0ef74d_story.html?utm_term=.fb5453a21996 [https://perma.cc/U8YY-NSSG].

17. Scott Detrow, *Obama on Russian Hacking: 'We Need to Take Action. And We Will'*, NPR (Dec. 15, 2016), http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will [https://perma.cc/Q2VB-URZL].

18. Louis Nelson, *Obama Says He Told Putin to 'Cut It Out' on Russia Hacking*, POLITICO (Dec. 16, 2016), http://www.politico.com/story/2016/12/obama-putin-232754 [https://perma.cc/QDX7-URNT].

have stopped, but the leaks from WikiLeaks continued, prompting President Obama to contact President Putin on the Moscow–Washington hotline on October 31.[19] Obama reportedly emphasized the gravity of the hacks to Putin, and he told Putin that "international law, including the law for armed conflict, applies to actions in cyberspace."[20] Meanwhile, the media reported on October 14 that President Obama ordered the CIA to develop options for a U.S. cyber response to the Russian efforts to interfere in the U.S. presidential election.[21] NBC News characterized the charge to the CIA as coming up with options for a retaliatory cyberattack against the Russian Federation.[22]

On December 29, the FBI and DHS released *Joint Analysis Report: GRIZZLY STEPPE—Russian Malicious Cyber Activity*.[23] The report reinforced the agencies' earlier conclusions that Russia was behind the DNC hack, and it provided new technical details about the methods used by Russian assets, including malware samples.[24] Still, the report offered little forensic evidence to confirm the government's attribution statement from October.[25]

Finally, on January 6, 2017, after briefing President Obama, President-elect Donald Trump, and members of the Senate and House in a classified session on behalf of the CIA, National Security Agency (NSA), and FBI, DNI James Clapper released an unclassified version of *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*.[26] Presumably the classified report included the details on Russian attribution. The public report concluded that Russia had conducted a large-scale cyber operation on the orders of President Vladimir

19. William M. Arkin, Ken Dilanian & Cynthia McFadden, *What Obama Said to Putin on the Red Phone About the Election Hack*, NBC NEWS (Dec. 19, 2016), http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116 [https://perma.cc/5CKG-G5XC].

20. *Id.*

21. William M. Arkin, Ken Dilanian & Robert Windrem, *CIA Prepping for Possible Cyber Strike Against Russia*, NBC NEWS (Oct. 14, 2016), http://www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636 [https://perma.cc/3VG4-N2YB].

22. *Id.*

23. U.S. DEP'T OF HOMELAND SEC. & FED. BUREAU OF INVESTIGATION, JOINT ANALYSIS REPORT: GRIZZLY STEPPE—RUSSIAN MALICIOUS CYBER ACTIVITY (2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf [https://perma.cc/RGW3-QKYT] [hereinafter RUSSIAN MALICIOUS CYBER REPORT].

24. *Id.*; David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=1 [https://perma.cc/3SKD-V4MT].

25. RUSSIAN MALICIOUS CYBER REPORT, *supra* note 23; Katie Bo Williams, *FBI, DHS Release Report on Russia Hacking*, THE HILL (Dec. 29, 2016), http://thehill.com/policy/national-security/312132-fbi-dhs-release-report-on-russia-hacking [https://perma.cc/4F57-AG84].

26. 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 1 (2017) [hereinafter ODNI REPORT RUSSIAN INTERFERENCE].

Putin with the intention of "undermin[ing] public faith in the US democratic process."[27] Their objective was to "denigrate Secretary Clinton, and harm her electability and potential presidency" while helping Donald Trump win the election.[28] The report concluded "with high confidence that Russian military intelligence (General Staff Main Intelligence or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release U.S. victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks."[29] In addition to hacking and releasing the e-mails and attachments, the Russian campaign included extensive use of social media and Internet trolls, along with propaganda on Russian-controlled media, including Russian TV channel RT America.[30]

Based on these reports, and more than five months after WikiLeaks published the DNC material, on December 29 the Obama administration announced a series of self-help retorsion[31] responses: sanctions on nine Russian intelligence agencies, companies, and individuals; expulsion of thirty-five intelligence assets in the United States; closure of two Russian compounds in the United States used by their intelligence agents; and release of information on Russian cyber activities designed to help defenders of cyber networks disrupt malicious Russian cyber activity.[32]

Despite the fact that the U.S. responses to the DNC hack were the strongest and most public ever by the United States in response to a State-sponsored cyber intrusion, reactions to the U.S. actions have been critical. In

---

27. *Id.* at ii.

28. *Id.*

29. *Id.* at ii–iii.

30. *Id.* at 2, 4, 6.

31. Retorsion consists of politically unfriendly but lawful responses to a State's actions that attempt to alter the State's conduct. Thomas Giegerich, *Retorsion*, *in* 8 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INT'L LAW 976 (2012); *see also* Tom Ruys, *Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework*, *in* RESEARCH HANDBOOK ON UN SANCTIONS AND INTERNATIONAL LAW 1, 5 (Larissa van den Herik ed., 2016) (considering retorsion as a form of "self-help").

32. Office of the Press Sec'y, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [https://perma.cc/XZ36-34S5]. On December 28, 2016, President Obama issued Exec. Order No. 13,757, allowing for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 82 Fed. Reg. 1 (Dec. 28, 2016). The Order amends an April 1, 2015 order, Exec. Order 13,694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in certain cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health and financial stability of the United States. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, 80 Fed. Reg. 18,077 (Apr. 1, 2015).

general, critics wondered why the United States waited so long and why we did not do more than impose those limited self-help measures. The responses were viewed as "too little, too late,"[33] or "confusing" and "weak,"[34] or simply "insufficient."[35]

Russian intelligence agencies have been penetrating sensitive computer networks inside the United States for more than twenty years.[36] President Obama was regularly briefed on escalating Russian hacking of government computers, but he declined to name the Russians publicly or impose sanctions, fearing an escalating cyberwar and needing Russian cooperation in negotiations over Syria.[37] When senior DNC executives first met with senior FBI officials in mid-June 2016, before any of the hacked materials had been published, DNC participants asked that the federal government formally blame the Russian government for the intrusions to emphasize to the American people that the hacks were foreign espionage, not routine hacking.[38] Nonetheless, the formal attribution of Russian government responsibility for the hacks did not come until October 7, and the limited sanctions were not announced until December 29.

Why did the United States wait so long to respond to the Russian intrusions? And why did we limit our responses to largely ineffectual self-help? The linchpin to understanding the timing and nature of the U.S. responses is a foundational component of cyber relations at international law—attribution. In common parlance, attribution means who is responsible, or assigning a cause to an action.[39] In the cyber domain, attribution means "identifying the agent responsible for the action."[40] Because the Internet facilitates anonymous communications and "was not designed with the goal of deterrence in mind,"[41] attribution of cyber intrusions can be challenging, particularly when the exploiters craft their intrusions to confound finding who is responsible.

---

33. Rebecca Crootof, *The DNC Hack Demonstrates the Need for Cyber-Specific Deterrents*, LAWFARE (Jan. 9, 2017), https://www.lawfareblog.com/dnc-hack-demonstrates-need-cyber-specific-deterrents [https://perma.cc/RU7U-5F4S].

34. Michael Morell, *Intelligence, Trump, Putin, and Russia's Long Game*, CIPHER BRIEF (Jan. 4, 2017), https://www.thecipherbrief.com/column/network-take/intelligence-trump-putin-and-russias-long-game-1091 [https://perma.cc/4P2E-PB39].

35. Maggie Penman & Ammad Omar, *Obama Announces Sanctions Against Russia In Response to Alleged Hacking*, NPR (Dec. 29, 2016), http://www.npr.org/sections/thetwo-way/2016/12/29/507430861/u-s-retaliates-against-russia-over-cyberattacks [https://perma.cc/FL8N-UJWJ].

36. Lipton et al., *supra* note 1.

37. *Id.*

38. *Id.*

39. David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 531 (2011).

40. *Id.*

41. *Id.*

Cyber attribution is more art than science and presents a multifaceted set of problems.[42] Law is only a part of the attribution calculus, and understanding the components of attribution is essential for shaping a legal and policy strategy to deter harmful cyber intrusions in the future.[43] As stated by former Assistant Attorney General for the National Security Division John Carlin,

> [A]ttributing activity on the Internet is challenging. Hackers often route their malicious traffic through third-party proxies they either rent or compromise. An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act. Even attributing an attack to the actual originating computer may be insufficient; we may know the machine used to execute a hack, but not the person or group that controlled it. Thus, technical investigation must often be supplemented by credible human intelligence. And all of this must be done quickly and consistently; attribution is of little use if it takes years and only identifies a small fraction of attackers.[44]

Attribution is a much discussed but underdeveloped part of international cyber law, particularly when States are the suspected responsible party. This Article will examine the treatment of attribution in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[45] and critique the current state of international attribution law for cyber operations. In a nutshell, *Tallinn 2.0* fairly summarizes what amounts to substantially underdeveloped customary international law on attribution of cyber operations. Because cyber attribution remains challenging and often time-consuming when State responsibility is suspected, international law places States in an untenable posture in responding to cyber intrusions below the use of force level. I argue that States, including the United States, must make some difficult tradeoffs between secrecy and transparency and publicly identify some public-infrastructure "red lines" and attribution benchmarks that can help States create an international roadmap for deterrence of harmful

---

42. *Id.* at 324 (asserting that attribution "is not actually a technical issue at all, but a policy concern with multiple solutions depending on the type of technical issue . . . to be solved. . . . [S]olutions . . . lie outside the technical realm, and are instead in the space of law, regulation, multinational negotiation, and economics"); *id.* at 350.

43. *See* John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 396–97 (2016) (describing attribution as an element of whole-of-government responses to cyber threats and the various parties involved in attribution).

44. *Id.* at 409 (footnotes omitted).

45. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

cyber intrusions in the future. The United States should also make clear that it will employ a range of lawful responses to State-sponsored cyber intrusions, including commercial and trade-based tools.

I. *Tallinn 2.0* and Attribution

As was the case with the release of the *Tallinn Manual on the Law of Cyber Warfare* in 2013, expectations are high that the second project will coalesce disparate understandings of the international law of cyberspace.[46] Indeed, the *Tallinn Manual* provided much-needed confidence for States that international law applies in the cyber domain and supplied a framework for applying to cyberspace widely understood norms from kinetic conflict.[47] The *Tallinn Manual* also consisted in the main of what is at the core of *Tallinn 2.0*: the opinions of a distinguished International Group of Experts (IGE) on how international law norms apply to cyberspace. Where the first project applied the *jus ad bellum* and *jus in bello* to cyber incidents that cross a use-of-force threshold,[48] the objective of the second project was in some ways much more ambitious and arguably more important—examination of the international legal framework that applies to malevolent cyber operations that do not rise to the use-of-force level.[49]

Like the first book, *Tallinn 2.0* is intended as a restatement that reflects the law as it is (*lex lata*).[50] It also contains extensive commentary, providing the rationale for each rule. Still, *Tallinn 2.0* is not a treatise on international cyber law, nor does it establish new international law or represent the views of any States on their cyber operations. There could be no such treatise at this time because of insufficient State practice, a paucity of official State legal views, and a lack of consensus on norms. The Rules provided in *Tallinn 2.0* and their commentary are as a result necessarily general in nature, sometimes ambiguous, and do not necessarily reflect settled international law. These limitations are not in any way due to shortcomings in the *Tallinn 2.0* project.

---

46. *See* Michael J. Adams, *A Warning About Tallinn 2.0 . . . Whatever It Says*, LAWFARE (Jan. 4, 2017), https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says [https://perma.cc/3H3V-GHVQ] (discussing the positive reception of the *Tallinn Manual* and similarly heightened expectations for the *Tallinn Manual 2.0*); Colonel Gary Corn, Tallinn Manual 2.0—*Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ [https://perma.cc/7LF6-AJL7] (noting the large and diverse audience in attendance at the standing-room-only D.C. launch of the *Tallinn Manual 2.0*).

47. Adams, *supra* note 46.

48. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael N. Schmitt ed., 2013).

49. *See* William Banks, *The Role of Counterterrorism Law in Shaping* ad Bellum *Norms for Cyber Warfare*, 89 INT'L L. STUD. 157, 161 (2013), *reprinted in* ISRAEL YEARBOOK ON HUMAN RIGHTS 45 (Yoram Dinstein & Fania Domb eds., 2013) (noting that a majority of cyberattacks were left unregulated by the *Tallinn Manual*); TALLINN MANUAL 2.0, *supra* note 45, at 1.

50. TALLINN MANUAL 2.0, *supra* note 45, at 3.

Indeed, the Director and IGE did excellent work in compiling what amounts to a general summary of the rules and principles that apply to cyber operations below the use-of-force threshold.

Tallinn 2.0 offers a nuanced and elegant application of the basic principles of State responsibility to below-threshold cyber operations and their attribution. In some instances, *Tallinn 2.0* clarifies unsettled areas of the law. Yet *Tallinn 2.0* and its near-contemporaneous release with the U.S. response to the Russian DNC hack bring into sharp relief the fact that international law on State responsibility for cyber operations and their attribution fails to provide prescriptive norms that will help deter malicious cyber operations.

The increasing stakes of below-threshold cyber operations are well-illustrated by the DNC hack. The Russian government actions profoundly impacted a presidential election,[51] our nation's most important democratic institution. Without better legal rules of the road, harmful features of cyber exploitation will only grow in importance. As will be developed below, the combination of unclear and unrealistic attribution requirements, countermeasures law that is not compatible with cyber operations, and ineffectual and ill-timed retorsion responses to cyber intrusions that provide little or no deterrence enable gray zones in cyber law that only incentivize harmful cyber intrusions.

Tallinn 2.0 reminds us that the customary international law of State responsibility and attribution is largely drawn from the work of over a half century of the International Law Commission (ILC) and its Rules on State Responsibility. While not a treaty, and thus not binding on any nation, the ILC rules were commended to member States by the United Nations General Assembly in 2012 and have been cited repeatedly by courts, tribunals, and other bodies.[52] The unsurprising threshold point on State responsibility emphasized in Rule 14 of *Tallinn 2.0* is that "[a] State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."[53] States care a great deal about cyber attribution precisely because the absence of attribution precludes State responsibility.[54]

---

51. *See* Richard Greene, *The Russian Hack Absolutely Affected the Outcome of the 2016 Election*, HUFFINGTON POST (Dec. 15, 2016), http://www.huffingtonpost.com/richard-greene/the-russian-hack-absolute_b_13656802.html [https://perma.cc/LS57-BSLQ] (arguing that Russian hacking had a palpable effect on the presidential election).

52. TALLINN MANUAL 2.0, *supra* note 45, at 79 n.112.

53. *Id.* at 84 (Rule 14).

54. *See, e.g.*, Phosphates in Morocco (It. v. Fr.), Preliminary Objections, 1938 P.C.I.J. (ser. A/B) No. 74, at 10, 28 (June 14) ("This act being attributable to the State and described as contrary to the treaty right of another State, international responsibility would be established immediately as between the two States."); United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 73, ¶¶ 29–30 (May 24).

Rules 15–18 of *Tallinn 2.0* summarize the customary international law of attribution of cyber operations in nuanced terms. Rule 15 states that "[c]yber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State."[55] Rule 15 may be reduced to an admonition that States are responsible for cyber-related acts of their own officials, agents, contractors, non-State actors, and other States to the extent they actually control the operations. Some explanation helps place application of the Rule in a few less obviously State-controlled settings.[56] One useful example from the IGE narrative concerns "spoofing," the practice of a representative of a State impersonating another State or its IP addresses and thereby feigning identity and sometimes its location.[57] Particularly when a cyber intrusion demands an immediate response from the victimized State, spoofing can completely flummox existing international law on attribution. The IGE counsels assessing the context of each such situation and expresses hope that patterns of cyber behavior, human intelligence, and a history of diplomatic relations between States will ameliorate the impacts of spoofing.[58]

Rule 16 states that "[c]yber operations conducted by an organ of a State that has been placed at the disposal of another State are attributable to the latter when the organ is acting in the exercise of elements of governmental authority of the State at the disposal of which it is placed."[59] The same practical application of State responsibility provides the basis for Rule 17, which states that "[c]yber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own."[60] In other words, States do not escape legal responsibility for internationally wrongful acts by perpetrating them through proxies. The extension of State responsibility to private actors that are acting under the direction and control of the State drives this Rule, which embraces the "effective control" formulation from the International Court of Justice in its *Nicaragua* and *Genocide* judgments.[61] One wrinkle that distinguishes attribution of non-State actors to States is that the *ultra vires* acts of non-State actors are generally not attributable to the State.[62] An example illustrates the

55. TALLINN MANUAL 2.0, *supra* note 45, at 87 (Rule 15).

56. *Id.* at 88–90.

57. *Id.* at 91.

58. *Id.* at 92.

59. *Id.* at 93 (Rule 16).

60. *Id.* at 94 (Rule 17).

61. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 108, ¶ 400 (Feb. 26).

62. TALLINN MANUAL 2.0, *supra* note 45, at 97.

limits of the principle of direction and control: a State instructs a non-State actor to introduce malware into another State's government networks and the non-State actor misappropriates the malware to target a third state. There is no attribution to the State because the non-State actor implemented the instruction in a way that was *ultra vires*.[63]

Finally, Rule 18 maintains that:

> [A] State is responsible for: (a) its aid or assistance to another State in the commission of an internationally wrongful act when the State provides the aid or assistance knowing of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it; (b) the internationally wrongful act of another State it directs and controls if the direction and control is done with knowledge of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it; or (c) an internationally wrongful act it coerces another State to commit.[64]

This rule simply imports noncyber considerations of State responsibility to the cyber domain.

II. Complying with International Law on Attribution: The Russia DNC Hack

Despite the persuasive criticisms of the U.S. responses to the Russian hack on the DNC, the U.S. government responses were carefully limited to comply with the current state of the law permitting only self-help responses under the international law of State responsibility and attribution. It bears emphasizing that attribution is a necessary precondition before responding to State-sponsored cyber intrusions. As the private security firm findings, intermediate agency reports, congressional briefings, and White House statements indicated, Russian involvement was suspected early on, before the publication of the materials began. However, the attribution report that the highest levels of the Russian government, including President Putin, directed and controlled the cyber hacking, exfiltration, and dissemination of private data in the United States was not delivered to President Obama's desk until much later.[65] Even then, rather than public attribution from the President, the White House ordered a relatively low-key release of the DHS/ODNI statement attributing the attacks to Russia on October 7.

As the January 6, 2017, *Assessing Russian Activities and Intentions* report indicated,

63. *Id.* at 98.
64. *Id.* at 100 (Rule 18).
65. Lipton et al., *supra* note 1.

> [a]n assessment of attribution usually is not a simple statement of who conducted an operation, but rather a series of judgments that describe whether it was an isolated incident, who was the likely perpetrator, that perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation.[66]

High confidence in State responsibility for the DNC hack required multiple agencies working their intelligence sources and methods, analysts' reviews of the evidence and judgments made on the evidence, and collective Intelligence Community judgments based on previous experience and the materials collected surrounding this case. Indeed, a unanimous Intelligence Community determination that military intelligence officials in the Russian government directed that the purloined e-mails be delivered to WikiLeaks was not achieved until sometime in December. In this instance attribution was aided by a parallel recent history of Russian hackers pursing political targets in Ukraine, Georgia, Estonia, and at North Atlantic Treaty Organization (NATO) installations.[67] A private security firm hired by the DNC also attributed the hacks to Russian State hackers.[68] That the Obama administration delayed formal State attribution to October, downplayed the announcement, and delayed implementation and a public statement of sanctions until the end of December was likely due to a combination of fear of escalation, a desire not to alienate Russia during Syria negotiations, and an expectation that Hillary Clinton would win the election in any case. Clearly, the Obama administration would have been reluctant to publicly announce sanctions against Russian hacking of the DNC and Clinton campaign before the election because of the appearance of punishing the Russians to benefit the Democratic candidate. In June or July, the sanctions that appeared too little, too late in December would have come across as aggressive and partisan.

Retired General and former NSA and CIA Director Michael Hayden helped place the U.S. response to the DNC hack in context by reminding us that the United States has only rarely officially attributed a malicious cyber operation to another State—China following widespread corporate espionage in 2014[69] and North Korea following the Sony hack in 2014[70]—and that when the United States makes such a public declaration "you can take it to the

66. ODNI REPORT RUSSIAN INTERFERENCE, *supra* note 26, at 2.

67. Lipton et al., *supra* note 1.

68. *Id.*

69. Robert Chesney, *DOJ's Summary of the Charges in the Chinese Economic Espionage Case*, LAWFARE (May 19, 2014), https://www.lawfareblog.com/dojs-summary-charges-chinese-economic-cyberespionage-case [https://perma.cc/KFN2-XYY4].

70. Herb Lin, *Learning from the Attack Against Sony*, LAWFARE (Jan. 23, 2015), http://www.lawfareblog.com/learning-attack-against-sony [https://perma.cc/6ZKP-5ZA2].

bank."[71] General Hayden also opined that Russia effectively "weaponized the information" they exfiltrated in an attempt to erode confidence in our democratic system.[72] Although General Hayden was not specifically critical of the Obama administration's actions in this instance, he suggested that other more aggressive geopolitical measures would have been appropriate.[73]

Retired Admiral James Stavridis, former head of NATO forces in Europe, offered a series of potential responses to the Russian DNC hack that he maintained would underscore U.S. determination to "respond with a firm hand."[74] Among other things, Admiral Stavridis argued that "the United States could use its own offensive cyber-tools to punish Russian hackers by knocking them off-line or even damaging their hardware."[75] Acknowledging that some would object that such a response may escalate the conflict, Admiral Stavridis admitted that "[t]he burden of proof for attribution would be higher" if we responded as above and "would be viable only if Washington had definitive information on the command and control centers that launched the hacking activity."[76] Admiral Stavridis's proposal to disconnect the hackers from Internet connectivity is likely not prohibited by international law unless doing so would require some kind of entry into the hackers' systems. Damaging the hackers' hardware would in all likelihood, however, be characterized as a forbidden use of force at international law.[77] Admiral Stavridis wisely recognized that any response to a responsible State requires attribution to that State. Yet Admiral Stavridis overstated international law attribution requirements. Applying the Rules on State responsibility and attribution compiled in *Tallinn 2.0*, there is no burden of proof or requirement that there exists "definitive information" on attribution. Although wise as a matter of policy, the failure to offer persuasive evidence of State attribution is not wrongful legally.

---

71. *Gen. Hayden on U.S. Response to Russian DNC Hack*, WALL ST. J. (Dec. 7, 2016), http://www.wsj.com/video/gen-hayden-on-us-response-to-russian-dnc-hack/54D57FC3-D99E-4864-B9C7-EE948791158A.html [https://perma.cc/GAW2-UXDC].

72. *Id.*

73. *Id.*

74. James Stavridis, *How to Win the Cyberwar Against Russia*, FOREIGN POLICY (Oct. 12, 2016), http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/ [https://perma.cc/WSX2-69L7].

75. *Id.*

76. *Id.*

77. *See* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 208–09 (2002) (arguing that cyberattacks against a nation's critical infrastructure should constitute an act of force giving rise to a right of proportionate self-defense under the United Nations Charter); TALLINN MANUAL 2.0, *supra* note 45, at 28 (noting that "interference with an object enjoying sovereign immunity constitutes a violation of international law," and that "[i]nterference includes, but is not limited to, activities that damage the object").

It is important to place the DNC hack in the larger context of cyber intrusions. The DNC hack clearly was not an armed attack or use of force.[78] Below the use of force threshold, States are responsible for a "cyber-related act . . . that constitutes a breach of an international legal obligation."[79] The breach may be a violation of a treaty or customary international law, or other "general principles of law."[80] Outside an armed conflict and below the use-of-force threshold, cyber intrusions constitute an international law breach by violating the prohibition on intervention.[81] The prohibition on intervention, based on the international law principle of sovereignty, forbids coercive intervention by cyber means.[82] *Tallinn 2.0* affirms that State-on-State cyber acts that are "detrimental, objectionable, or otherwise unfriendly"[83] are not breaches and do not trigger State responsibility. However, physical damage or injury is not necessary to render a cyber operation an internationally wrongful act "unless damage is an element of breach of the primary rule."[84] Nor is intent to cause harm generally a requirement of an internationally wrongful act.[85] Violations of domestic law cannot be the basis for an internationally wrongful act,[86] because the existence of a legal obligation is determined solely by international law.[87]

Based on the publicly available evidence, the DNC hack probably was not an unlawful intervention. In a November 2016 speech, Department of State Legal Adviser Brian Egan opined that "a cyber operation by a State that interferes with another State's ability to hold an election or that manipulates a State's election results would be a clear violation of the rule of non-intervention."[88] The *Tallinn 2.0* experts similarly suggest that remotely altering electronic ballots to manipulate election results constitutes an unlawful intervention.[89]

The core requirement of a prohibited intervention is coercion.[90] As confirmed by the International Court of Justice in the *Nicaragua* judgment,

78. *See* TALLINN MANUAL 2.0, *supra* note 45, at 107, 364–65 (discussing cyber operations that qualify as "armed attacks" and "uses of force").

79. *Id.* at 84 (Rule 14).

80. *Id.* at 84.

81. *Id.* at 312.

82. *Id.* at 313.

83. *Id.* at 85.

84. *Id.* at 86.

85. *Id.*

86. *Id.*

87. G.A. Res. 56/83, Articles on State Responsibility, art. 3 (Jan. 28, 2002).

88. Brian J. Egan, Remarks on International Law and Stability in Cyberspace at Berkeley Law School (Nov. 10, 2016), https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf [https://perma.cc/4DXB-9TNH].

89. TALLINN MANUAL 2.0, *supra* note 45, at 313.

90. *Id.* at 317.

"the element of coercion . . . forms the very essence of [] prohibited intervention."[91] As understood in *Tallinn 2.0*, coercion "is not limited to physical force, but rather refers to an affirmative act designed to deprive another State of its freedom of choice . . . to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[92] A January 2017 memorandum from the General Counsel of the Department of Defense to the Combatant Commands and other senior military and civilian lawyers in the Pentagon affirmed coercion as a prerequisite means for unlawful intervention, and concluded that military cyber activities that fall below the use of force threshold and do not violate the nonintervention principle are "largely unregulated by international law at this time."[93]

Measured against those customary international criteria, the Russian hack likely was not an internationally wrongful act. The Russians exfiltrated and disseminated private information but did not tamper with voting machines or change votes. According to the traditional measures, there was no coercion and no unlawful intervention. We should temper our confidence in this coercion analysis, however, because state practice and resulting customary international law are based on examples from kinetic conflicts. The analogies to cyber are not necessarily conclusive. If we extrapolate from General Hayden's metaphor that the Russians effectively "weaponized the information" they stole for the purpose of eroding confidence in the U.S. democratic system, the Russian exfiltration looks more coercive. In any case, the United States could not respond to Russia until it attributed State responsibility for the attacks.

III. The International Law Problems with Countermeasures in Cyber

For the sake of argument, assume that the Russian DNC hack was an unlawful intervention. What could the United States have done in response? Admiral Stavridis appeared to propose what international law refers to as countermeasures. Countermeasures are responses, whether cyber in nature or not, below the use-of-force threshold designed to prevent or mitigate a perpetrator State from continuing its unlawful cyber intervention.[94] Though

91. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

92. TALLINN MANUAL 2.0, *supra* note 45, at 317.

93. Dep't of Def., Memorandum for Commanders of the Combatant Commands, International Law Framework for Employing Cyber Capabilities in Military Operations (2017) (on file with author). The Memorandum acknowledges that the "exact contours of cyber activities that might violate the principle of non-intervention are not clear, and will continue to develop with state practice over time." *Id*.

94. *See* TALLINN MANUAL 2.0, *supra* note 45, at 111 ("Only available in response to internationally wrongful acts, countermeasures are actions or omissions by an injured State directed against a responsible State that would violate an obligation owed by the former to the latter but for

short of a use of force, countermeasures would be unlawful themselves but for the purpose of stopping the intrusion.[95] Because they respond to an internationally wrongful act, countermeasures require prior attribution and notice to the offending State that the victim State knows the source of the cyber intrusion.[96] International law also requires giving the aggressor State a chance to forbear.[97] In addition, the countermeasures must be proportional to the original intrusion[98] and they must have as their purpose "induc[ing] compliance with international law."[99] Punitive countermeasures are forbidden.[100]

In October 2014, the United States made a public submission[101] to the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, a group focused in recent years on identifying legal norms in cyberspace. Among other subjects, the U.S. submission noted the legal limits on exercising countermeasures in cyberspace, including the requirement of the injured State to call on the responsible State to comply with its international obligations before launching cyber countermeasures, except in exigent circumstances.[102]

Even if the Russian operation was an unlawful intervention, the long lag time between the hack and a confident State attribution rendered countermeasures unavailable. Countermeasures are designed to persuade the perpetrator to stop its unlawful actions, not as punishment or escalation. Putting aside the specifics of the DNC hack, cyber intrusions below the use-of-force level are normally quick-hitting, allowing insufficient time for the countermeasures regime to play out in a State-on-State setting. Following the countermeasures requirements of notice to the offender and giving them a chance to refuse to stop their actions is unrealistic in the cyber environment.

Although the technological aspects of attribution have advanced considerably in recent years,[103] settling on State responsibility involves more

---

qualification as a countermeasure."); Nicar. v. U.S., 1986 I.C.J. 14, ¶ 249; Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, ¶¶ 82–83 (Sept. 25).

95. TALLINN MANUAL 2.0, *supra* note 45, at 111.

96. *Id.* at 120.

97. *Id.*

98. *Id.* at 127 (Rule 23).

99. *Id.* at 112.

100. *Id.* at 124.

101. Applicability of International Law to Conflicts in Cyberspace, 2014 DIGEST OF U.S. PRACTICE IN INTERNATIONAL LAW, ch. 18, § A(3), at 13, https://www.state.gov/documents/organization/244486.pdf [https://perma.cc/5VDX-2M7X] [hereinafter 2014 U.S. SUBMISSION TO THE GGE].

102. *Id.* at 20.

103. *See* Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, J. INT'L AFFAIRS ONLINE (Mar. 9, 2017), https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents [https://perma.cc/2CTP-8Q6Z] (synthesizing various discussions of attribution, specifically as it relates to malicious cyber acts).

than technical attribution of the offending machine, or even the operator of the machine. If a State victimized by an internationally wrongful cyber intrusion engages in countermeasures too early and is wrong about State attribution, the victimized State has committed an internationally wrongful act.[104] If the victim State waits until it has high confidence in State responsibility for the intrusion, any countermeasures that are implemented may be construed as punishment, forbidden under international law.[105] As a result, cyber deterrence may be undermined because the limited available self-help retorsion responses to an intrusion like the DNC hack are weak and unlikely to deter similar cyber intrusions in the future.

Attribution can mean different things depending on a State's objectives. Attribution of malicious cyber activity can trace to a machine, to one or more persons operating the machine that initiates the cyber intrusion, and to a person or entity that is found to be ultimately responsible for that activity.[106] Attribution is determined by a wide range of facts, including technical forensics, human intelligence, signals intelligence, history, and diplomatic relations, among others.[107] The declassified *Background to "Assessing Russian Activities and Intentions in Recent US Elections"* reminds us that intelligence analysis of cyber intrusions seeks "to reduce the uncertainty surrounding foreign activities, capabilities, or leaders' intentions. This objective is difficult to achieve when seeking to understand complex issues on which foreign actors go to extraordinary lengths to hide or obfuscate their activities."[108] The Intelligence Community assessment reflects "a series of judgments that describe whether [the intrusion] was an isolated incident, who was the likely perpetrator, the perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation."[109]

Recognizing that customary international law has not developed a set of understandings or recognized State practice on what level of attribution is acceptable or necessary for establishing State responsibility for cyber actions, the IGE concluded that "States may agree between themselves to a rule of responsibility specific to a cyber act or practice."[110] The result would be *lex specialis* to the extent the rule conflicts directly with general principles of State responsibility.[111] Discerning no such rules or understandings among

104. TALLINN MANUAL 2.0, *supra* note 45, at 118–20.

105. *Id.* at 116.

106. Clark & Landau, *supra* note 39, at 532.

107. *See* Carlin, *supra* note 43, at 396–97 (discussing the various experts required for the complex attribution analysis).

108. ODNI REPORT RUSSIAN INTERFERENCE, *supra* note 26, at 1.

109. *Id.* at 2.

110. TALLINN MANUAL 2.0, *supra* note 45, at 80.

111. As per the traditional legal maxim "specific law prevails over general law." *See Generalia Specialibus Non Derogant*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("The doctrine holding that

States today, the IGE acknowledged the "uncertainty as to the attribution of cyber operations" and agreed "that as a general matter, States must act as reasonable States would in the same or similar circumstances when considering responses to them."[112] The IGE elaborated in this way:

> 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. These factors must be considered together. Importantly in the cyber context, deficiencies in technical intelligence may be compensated by, for example, the existence of highly reliable human intelligence.[113]

Reasonableness may also take into account "the severity of the cyber operations being directed against the State and the robustness of any possible response."[114] The IGE suggested that "as a general matter the graver the underlying breach . . . , the greater the confidence ought to be in the evidence relied upon by a State considering a response[115] . . . because the robustness of permissible self-help responses . . . grows commensurately with the seriousness of the breach."[116] At the same time, "the severity of the cyber operations directed at the injured State"[117] matters. A State confronted with "low-level cyber operations that are merely disruptive" may be expected to amass more evidence for attribution than a State victimized by "devastating cyber operations and needing to respond immediately to terminate them."[118] To put it slightly differently, the IGE acknowledged that all attribution judgments that determine State responsibility are necessarily accompanied by some measure of uncertainty. Because there is no accepted State practice, nor international agreement or domestic law on how much evidence suffices for attribution of State responsibility, the attribution bar is at present set very low by international law.

Nor is the failure of a State to provide persuasive proof of attribution itself an internationally wrongful act. There are no burdens of proof or

---

general words in a later statute do not repeal an earlier statutory provision dealing with a special subject."); TALLINN MANUAL 2.0, *supra* note 45, at 81.

112. TALLINN MANUAL 2.0, *supra* note 45, at 81.

113. *Id.* at 81–82.

114. *Id.* at 82.

115. *Id.* In support of its position, the IGE cited Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 33 (Nov. 6) (separate opinion of Judge Higgins); Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 17 (Apr. 9); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 108, ¶¶ 209–10 (Feb. 26); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croat. v. Serb.), 2015 I.C.J. General List No. 118, ¶ 178 (Feb. 3).

116. TALLINN MANUAL 2.0, *supra* note 45, at 82.

117. *Id.*

118. *Id.*

additional legal criteria for establishing attribution. The 2015 United Nations Group of Governmental Experts (GGE) report noted that accusations of wrongful acts by States "should be substantiated,"[119] but the GGE gave no indication of which or how much evidence would suffice or even count. The United States' view, articulated by State Department Legal Adviser Brian Egan in November 2016, is that "a State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. . . . [T]here is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action."[120]

States are likewise not obligated to publicly provide evidence of attribution when responding to another State's cyber intrusions.[121] While the IGE acknowledged the value in such a disclosure requirement, they found insufficient State practice and *opinio juris* to recognize "an established basis under international law for such an obligation."[122] The IGE noted that the highly classified nature of such attribution assessments is the primary reason for the absence of customary international law on this important point.[123] The October 2014 U.S. submission to the GGE is consistent with the IGE on all of these points.[124]

IV. Assessing the State of Attribution Law

Over time, an international consensus may develop on the minimum level of involvement needed to declare that a State is legally responsible for a cyber operation. But we are not there yet. In working to attribute an intrusion to a human perpetrator or an ultimately responsible State, technical forensics by themselves are generally inconclusive,[125] and the information they provide must often be combined with other sources to be genuinely useful.[126] The fact that attribution judgments draw on many different sources of information has one major temporal implication—early judgments made with less information are generally less believable than later judgments made

119. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 24, U.N. Doc. A/70/174 (July 22, 2015).

120. Egan, *supra* note 88, at 19.

121. TALLINN MANUAL 2.0, *supra* note 45, at 83.

122. *Id.*

123. *Id.*

124. *See* Michael Schmitt, *U.S. Transparency Regarding International Law in Cyberspace*, JUST SECURITY (Nov. 15, 2016), https://www.justsecurity.org/34465/transparency-international-law-cyberspace/ [https://perma.cc/UCY4-5VBT].

125. *See* Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 7 (2015) (noting that using technical forensics to attribute a cyber attack to a specific actor is more of an art than a science).

126. *See* Lin, *supra* note 103 (observing that the duration of the Sony investigation was due in part to an absence of other sources).

with more information. Continuing investigation may reveal additional useful information, which may (or may not) reinforce attribution judgments made earlier.

The lucid analysis by the IGE in *Tallinn 2.0* affirms that international law does not incentivize careful and thorough efforts at attribution in cyber operations. For example, there is no incentive at international law for a State planning self-help retorsion to be certain of State responsibility and refrain from responding to a cyber intrusion before all the facts are in so long as it does not engage in an internationally wrongful act. Meanwhile, the fact that attribution of State responsibility for an internationally wrongful cyber intervention may take a long time and thus defeat the countermeasures option creates a particularly unhelpful set of choices—to respond with countermeasures based on incomplete evidence and risk making a mistake that constitutes an internationally wrongful act or wait to implement countermeasures only after there is solid evidence of State responsibility. By such time, the original victimized State will have engaged in an internationally wrongful act because the international law criteria for a countermeasure are not satisfied and the putatively defensive measures will be seen as an attack.

One positive development in the attribution landscape in the past several years is the increasing involvement of private-sector firms in rendering attribution judgments. The 2015 Department of Defense Cyber Strategy notes that security firms reporting on attribution "can play a significant role in dissuading cyber actors from conducting attacks in the first place" and states that "[t]he Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution. This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time."[127]

For example, in February 2013 Mandiant issued an extensive report on Chinese cyber espionage that relied on detailed evidence of Chinese government attribution.[128] Mandiant found with a high degree of confidence that a specific unit of the People's Liberation Army (PLA) perpetrated hacks on many of the targeted industries in the United States, after first identifying the particular machines and operators involved in the espionage.[129] The Mandiant work helped pave the way for the May 2014 indictments by the

127. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 12 (2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [https://perma.cc/2LS5-CPCZ].

128. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [https://perma.cc/Q4WP-VQDG].

129. *Id.* at 3–7. Mandiant acknowledged the "unlikely possibility" that a group of private hackers had engaged in espionage similar to that conducted by the PLA. *Id.* at 6.

Justice Department of five PLA members on economic espionage charges.[130] In another example, after senior DNC executives learned from FBI officials that they had been hacked, the DNC hired CrowdStrike, a cybersecurity firm, to rebuild its computer security.[131] Within a day, CrowdStrike advised its client that the hacks originated in Russia.[132] Several other prominent examples of private security firms' involvement in attribution of cyber intrusions by States are noted below.[133]

On the one hand, private firms' cases for attribution of State responsibility are speculative. They can provide computer forensics and, at times, identify the operators of perpetrator machines.[134] But they lack the authority and means to collect the human intelligence necessary to reliably find State attribution. There is a big difference between saying that Russians hacked and Russia hacked. In addition, the companies have a self-interested stake in marketing their brand and encouraging further work on Internet security. The companies may lack the independence and rigor that we expect of government intelligence work.[135] On the other hand, private security firms can provide a public accounting of responsibility for malicious cyber actions with analytical and collection resources beyond those employed by States. The unclassified nature of their reports both provides a transparent airing of attribution and takes the pressure off government to share its sources and methods while allowing government to avoid responsibility for the attribution judgment.

From a policy perspective, the implications of these developments for cyber attribution are coming into sharper focus. A determination of

---

130. Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015), https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html?utm_term=.d21182d3328f [https://perma.cc/8UU5-X6H9].

131. Lipton et al., *supra* note 1.

132. *Id.*

133. *See* CROWDSTRIKE, CROWDSTRIKE INTELLIGENCE REPORT: PUTTER PANDA (2014), https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf [https://perma.cc/2FPF-GQ53] (concluding that Unit 61486 in the PLA was likely responsible for the cyber theft of trade secrets against entities in the satellite, aerospace, and communication industries); FIREEYE, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? (2014), http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf [https://perma.cc/BSG7-8WME] (presenting evidence that Russia was involved in espionage against private-sector and government actors); NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT (2014), http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf [https://perma.cc/UTX3-ESS6] (contending that the Chinese government was likely involved in cyber espionage against several private companies, governments, journalists, and prodemocracy groups).

134. *See* Biddle, *supra* note 7 (discussing a private security firm's forensic findings following the DNC hack).

135. Lin, *supra* note 103 n.62.

attribution is rarely definitive, and will usually be hedged with some degree of uncertainty.

The necessary degree of confidence in an attribution judgment depends on the nature of the malicious activity being attributed and the action that is contemplated in its aftermath. The audience that an attribution judgment seeks to persuade has a significant impact on how subsequent aspects of the attribution process unfold. The *Tallinn 2.0* experts recognize these variables and their importance.

V. The National Security Implications of the International Law on Attribution

States want to set responsibility for malicious actions in the cyber domain so that governments can decide what action to take in response and against whom. Technology may be sufficient for attribution in cyber if governments want to stop or impact the machine that is causing the harm. If instead governments want to prosecute a cyber perpetrator, different attribution from different sources will likely be required. Knowing the machine doesn't necessarily lead to the operator. If the goal is to fix State responsibility more may be required.

The sources and methods pursued to determine attribution in national security cyber cases are in some ways different and in some ways like those used in law enforcement. Much of the evidence of attribution is off-line and involves traditional interviews and the examination of equipment.[136] Much of the sleuthing is also vulnerable to efforts by adversaries to thwart or slow down investigations, often through cyber means such as spoofing on location and identity.

How much evidence of attribution is enough? As reflected in the commentary in *Tallinn 2.0*, international law requires a granular analysis, taking into account "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."[137] A State merely encouraging a non-State actor to undertake a malicious cyber intrusion is not sufficient for State responsibility.[138] In this respect, the nuance and detail offered in *Tallinn 2.0* is extremely valuable, showing how judicial decisions and analysis from customary international law sources can help in determining attribution.

The time it takes to produce an attribution judgment with high confidence can significantly impact the lawful responses to cyber intrusions. In some circumstances mistaken attribution can lead to an unlawful response

136. Carlin, *supra* note 43, at 414–15.

137. TALLINN MANUAL 2.0, *supra* note 45, at 82.

138. *Id.* at 97.

even if the victimized State made a reasonable determination of attribution and implemented countermeasures.[139] In national security contexts, the IGE opined that "as a general matter the graver the underlying breach . . . the greater the confidence ought to be in the evidence relied upon by a State considering a response."[140] More robust responses require more evidence, and the more severe the injury to the victim State, the less certain of attribution the State needs to be.[141] Similarly, low-level cyber intrusions that are disruptive but not destructive place victimized States "in a position to accumulate more evidence for attribution," suggesting a case-by-case evaluation of required attribution.[142]

Apart from the substantive attribution criteria, international law is unlikely to play an important role in contributing predictability and stability in cyberspace relations among States without greater transparency within and among States on their cyber norms and practices than now exists. Customary international law, after all, develops from a consistent practice of States followed out of a sense of legal obligation.[143] When States articulate their views on how international law applies to cyber operations, such public statements increase expectations of State behavior and thus contribute to greater predictability and stability in cyber operations.[144] Instances such as the Russian attempts to interfere with the 2016 election provide an opportunity for the United States to clearly and unequivocally delineate red lines, reinforced by a set of lawful responses that would follow their breach. That the Obama administration equivocated, delayed attribution, and then delayed ineffectual sanctions did not serve those important international law objectives.

Reacting in December 2016 to the Obama administration's relative public silence on the Russian DNC hacks, former acting director of the CIA Michael Morell opined that "[a] foreign government messing around in our elections is . . . the political equivalent of 9/11."[145] Morell pointed out that North Korea, China, and Iran are watching the U.S. reaction to the Russian

---

139. *Id.* at 82–83.

140. *Id*. at 82; *see also* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 108, ¶¶ 209–10, 400 (Feb. 26) (discussing the implicitly proportionate connection between the degree of one country's offense and another country's response); U.K. v. Alb., 1949 I.C.J. ¶ 17 (Apr. 9) (noting that a "charge of such exceptional gravity against a State would require a degree of certainty").

141. TALLINN MANUAL 2.0, *supra* note 45, at 82.

142. *Id.*

143. Egan, *supra* note 88, at 5.

144. *Id.* at 7.

145. Michael Morell & Suzanne Kelly, *Fmr. CIA Director Michael Morell: "This Is the Political Equivalent of 9/11"*, CIPHER BRIEF (Dec. 11, 2016), https://www.thecipherbrief.com/article/exclusive/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091 [https://perma.cc/QK8K-5X2X].

infiltration, and if the response is not visible, the deterrent effect is lost.[146] Transparency objectives are inhibited in cyber-operations law in part because the domain itself is still relatively new and evolving. There are also complications in implementing a geographic- and location-based legal structure alongside an incongruous Internet. Additional obstacles include the inevitable need for secrecy in carrying out most cyber operations and the attribution work that must occur regarding the cyber activities of our adversaries. Still, States should work toward norms of expected conduct in cyberspace, along with mutually agreed deterrents to harmful cyber intrusions. Such norms could supplement customary law on State responsibility, becoming *lex specialis* in the cyber domain.[147]

International law as summarized in *Tallinn 2.0* requires much less proof of attribution than lawyers traditionally expect.[148] Of course lawyers expect rigorous standards for proof in civil trials or criminal prosecution, not necessarily in national security investigations, depending on the investigative method. The proof necessary for attribution in cyber exploitation involving State responsibility certainly need not stand up in court. Indeed, the evidence of attribution may never be made public because of the sensitivity of the intelligence sources and methods utilized in the investigation.

Nonetheless, the international-law reasonableness approach and the absence of burdens or criteria for assessing attribution leave an unfortunate gap in the international law of cyber. Without more public accounting of State responsibility, governments and citizens are not likely to trust or accept cyber responses, leading to the escalation of cyber conflict and failures of deterrence. In the United States and much of the world, neither governments nor citizens will accept cyber operations without some credible attribution that is transparent to some degree.

Conclusions

States are better able to attribute cyber intrusions than they were a decade ago, but the technical environment is so dynamic that new tools constantly both improve and occlude attribution capabilities. Even though the attribution bar at international law is low, spoofing and other challenges can greatly complicate attribution and cyber response when an immediate response is required, particularly when a State is the suspected perpetrator. Attribution is in any case an all-source enterprise. States that are forced by international law to publicly express the proof of attribution to explain countermeasures or some other response run the risk of overstating their case,

146. *Id.*

147. *See supra* text accompanying notes 109–12 (discussing how States could develop specialized rules for State responsibility for cyber acts).

148. *See* TALLINN MANUAL 2.0, *supra* note 45, at 81 (asserting that States "must act as reasonable States would" in dealing with attribution uncertainty).

or not supporting it thoroughly, and thereby engage in an internationally wrongful act.

As cyber international relations now stand, a few States (the United States and likely Russia, China, North Korea, and Iran) benefit from the absence of express cyber norms on what suffices to attribute State responsibility for cyber exploitation because they have the most offensive cyber capabilities. Russian State involvement in the DNC hacks and the releases through WikiLeaks is a good example. Because it is unclear whether the Russian interference in the U.S. elections amounted to the coercion that is necessary to establish an international law violation, the Putin government could and did act with relative impunity. Establishing attribution of the hacks and dissemination to WikiLeaks to the Russian government was a multifaceted intelligence investigation that could not be completed with confidence in short order. Countermeasures could not be lawfully implemented, and the late-arriving self-help retorsion measures likely did nothing to deter further Russian cyber aggression.

The decision to delay formal attribution of the DNC hacks to Russia was a policy decision. As noted above, President Obama had declined to name Russian State involvement in cyber intrusions because of fear of escalating to cyberwar, and because of the presumed need for Russian cooperation in Syria negotiations.[149] Situation Room meetings on the Russian hacking began in July 2016, but no formal attribution report was forwarded to the President.[150] During August, a series of formerly secretive software tools that can be used for cyber surveillance or attack were published by a hacking group possibly affiliated with Russia. U.S. officials took the dissemination of the tools as a warning that Russia would respond with more releases of U.S. secrets if the United States retaliated for the DNC hack.[151] Reportedly, a series of meetings around the same time deliberated aggressive cyber counterstrikes, although none of those recommendations were formally presented to the President.[152] Officials worried that an aggressive U.S. response would undermine confidence in our voting system, and perhaps most importantly, should not be seen as trying to influence the election.[153] Instead, President Obama delivered his personal warning to Mr. Putin at the Group of 20 summit meeting and left the public attribution of Russia's role to the written statement from ODNI and DHS.

The States that benefit presently from the absence of rules in cyberspace are also the most vulnerable to cyber intrusions. As the most advanced cyber States begin to recognize the zero-sum aspects of cyber escalation, those

149. Lipton et al., *supra* note 1.
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*

States should become more transparent about attribution in service of the mutual restraint that could be gained by sharing attribution information.[154] Extensive diplomatic, intelligence, and public communication about attribution and potential uses of countermeasures in the below-threshold cyber domain will become part of emerging customary international law as lawyers and government officials engage in this especially important risk assessment project. States should strive to establish criteria or measures for State attribution in instances of cyber exploitation, then seek bilateral or multilateral agreements with other States, toward establishing more concrete customary international law for attribution. Similar steps could be taken to agree on measures of public transparency on State responsibility.

The lack of clear normative bases for governing cyber operations according to international law extends beyond problems of attribution, of course. The same inadequacy of lawful, defensive response options that reveal themselves in discussing attribution fare no better when responsibility for a cyber intrusion is known. For example, *Tallinn 2.0* regards State sovereignty as a binding rule of international law[155] that applies to the conduct of nonconsensual cyber operations of one State against cyber infrastructure located in another State. Under this admittedly widely held view of sovereignty, the Russian DNC hack probably violated sovereignty and thus international law. The fact that the United States responded with relatively nonthreatening self-help retorsion may indicate that the United States views the noncoercive hacks and exfiltration of data not as internationally wrongful acts, but instead as a species of espionage that is generally unregulated by international law.[156]

Given the architecture of the Internet, the traditional Westphalian stance on sovereignty embedded in customary law and reflected by the IGE in *Tallinn 2.0* may frustrate the development of workable norms for controlling below-threshold conflict in cyberspace.[157] Consider the simple example of a nonstate, transnational terrorist group spreading malware across several States. Although many States are equipped to disrupt botnets or malware impacts through straightforward, technical cyber operations, the sovereignty rule could stand in the way of State responses to the terrorists that cross national borders. Absent State consent, any cyber operation in response to

154. In the United States, domestic law authorizes covert action, including for cyber activities. 50 U.S.C. § 3093 (2012). The fact that a domestic law justification exists for secrecy does not impact existing or evolving international law.

155. TALLINN MANUAL 2.0, *supra* note 45, at 11.

156. Egan, *supra* note 88, at 11–12; TALLINN MANUAL 2.0, *supra* note 45, at 85.

157. The United States' view is that "remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a *per se* violation of international law." Egan, *supra* note 88, at 11. The U.S. view takes into account the importance of intelligence collection abroad through cyber means. *Id.* at 11–12.

this kind of intrusion that constitutes a prohibited intervention is unlawful. The barrier applies to responses to States and to nonstate actors.[158]

Tallinn 2.0 marks an important but early point in a conversation among States about the most important principles of international law in cyber. The conversation matters a great deal because so much of our international relations are now bound up in the cyber domain, and the existing rules of the road are riddled with gray areas and incomplete understandings.

158. Colonel Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ [https://perma.cc/7LF6-AJL7].