INTERNATIONAL LAW STUDIES
Published Since 1895

Cyber Attribution and State Responsibility

William Banks

97 INT'L L. STUD. 1039 (2021)

Volume 97

2021

Published by the Stockton Center for International Law

ISSN 2375-2831

Cyber Attribution and State Responsibility

*William Banks**

CONTENTS

* Board of Advisers Distinguished Professor, professor of law, professor of public administration emeritus, Syracuse University College of Law, Maxwell School of Citizenship & Public Affairs. The author thanks Kristen Boon, Laura Dickenson, MJ Durkee, Sarah Haan, James Gathii, Ingrid Wuerth, and participants in The Law and Logics of Attribution: Constructing the Identity and Responsibility of States and Firms, September 2020, American Society of International Law, Dean Rusk International Law Center, and the School of Law, University of Georgia. He also thanks Jacob Saracino, J.D., Syracuse University College of Law, 2021, for excellent research assistance.

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

What does attribution mean in cyberspace? Is attribution of a cyberattack required by international law? When hackers use cyberspace to engage in espionage or cyber theft or disrupt valuable infrastructure, how can we know whether those acts should be attributed to a State? What are the legal consequences of attribution? At international law, we might expect that attribution requirements are significant in framing the legal responsibility of States and the boundaries of responsive actions by victim States. As it turns out, however, there is little international law of cyber attribution, and what law there is exists largely by implication. Likewise, there is only a murky and highly contested law of State responsibility that theoretically constrains the vast majority of State-sponsored cyberattacks.

For example, a State that has suffered a cyberattack may want to respond in kind with countermeasures. Because victim States cannot engage in countermeasures unless they attribute a cyberattack to a State, attribution can serve simultaneously to constrain and empower a victim State. However, the lack of a common understanding about whether cyber attribution is required—much less what evidence suffices for attribution of a cyberattack for international law purposes—combined with the absence of consensus legal rules to limit cyber intrusions, has helped render the entire international legal response to cyberattacks weak and largely ineffective. Going forward, States and the international community should support public cyber attributions and address in a sustained manner what legal or evidentiary standards must be met to attribute responsibility for a cyberattack to a State. A viable cyber attribution regime is a missing but key component for States to overcome the Wild West cyber environment that we live in.

In the decade since the 2010 Stuxnet and Olympic Games cyberattacks on a thousand Iranian nuclear centrifuges first brought to the world's attention that cyber tools could be weaponized to cause considerable destructive harm,[1] a long list of apparently State-sponsored cyberattacks have ricocheted

1. Marc Ambinder, *Did America's Cyber Attack on Iran Make Us More Vulnerable?*, THE ATLANTIC (June 5, 2012), https://www.theatlantic.com/national/archive/2012/06/did-americas-cyber-attack-on-iran-make-us-more-vulnerable/258120/ (calling the U.S. cyberattack a "history-making development" and "the most sophisticated state-sponsored cyber attack in the history of civilization").

across the globe.[2] Despite their impact—sometimes destructive (Stuxnet) and perhaps strategic game-changers (2016 election interference), at other times merely disruptive but costly (Office of Personnel Management (OPM) and Sony Pictures hacks)—little has been done to bring legal consequences to bear for what in a kinetic realm would likely be unlawful acts at international law. Over the last decade, at least thirty-eight States—including Russia, China, North Korea, Iran, the United Kingdom, and the United States—have allegedly carried out or supported significant cyberattacks that impacted governments, populations, and infrastructures.[3] The accused States, effectively hiding behind nameless agents, deny the accusations, blame someone

2. *See* Council on Foreign Relations, *Cyber Operations Tracker* (2020), https://microsites-live-backend.cfr.org/cyber-operations; *see also Significant Cyber Incidents*, CSIS, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited July 13, 2021); Catalin Cimpanu, *A Decade of Hacking: The Most Notable Cyber-Security Events of the 2010s*, ZD NET (Dec. 12, 2019), https://www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s/ (detailing forty-three cyber security breaches that occurred between 2010 and 2019, including State-sponsored cyberattacks and hacks attributable to individuals).

3. *See* Council on Foreign Relations, *supra* note 2; *see also Significant Cyber Incidents*, *supra* note 2; John S. Davis II et al., *Stateless Attribution: Towards International Accountability for Cyberspace*, RAND (2017), https://www.rand.org/pubs/research_reports/RR2081.html; Dan Efrony & Yuval Shany, *A Rule Book on the Shelf?* Tallinn Manual 2.*0 on Cyberoperations and Subsequent State Practice,* 112 AMERICAN JOURNAL OF INTERNATIONAL LAW 583, 594 (2018) (eleven case studies of State-sponsored cyber operations). The total number of accusations, including those made more privately, is likely much higher.

else, or decline to comment.[4] They show few signs of changing behavior.[5]

Gradually, some States have begun to publicly attribute cyberattacks against them, usually without accompanying evidence. Extensive cyberattacks in Estonia in 2007, Georgia in 2008, and Kyrgyzstan in 2009 were widely suspected as being perpetrated by Russia, yet none of them were publicly attributed.[6] The United States broke the attribution silence episodically. In 2014 the Justice Department indicted[7] five People's Liberation Army officers on economic espionage charges. Unsurprisingly, at least in part because the suspects could not be brought to trial in the United States and because the Chinese government understood that the threat of prosecution was empty,[8] the attributions did not include evidentiary support, and the

4. Przemyslaw Roguski, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, JUST SECURITY (Mar. 6, 2020), https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/ (citing twenty States accusing Russia of cyber operations against Georgia as evidence that "more—especially European—States are willing to adopt public attributions"); *see also* David E. Sanger & Marc Santora, *U.S. and Allies Blame Russia for Cyberattack on Republic of Georgia*, NEW YORK TIMES (Feb. 21, 2020), https://www.nytimes.com/2020/02/20/world/europe/georgia-cyberattack-russia.html ("Neither the United States nor its allies released any evidence used to establish how they tied the attacks to the G.R.U. That made it easier for the Russian Foreign Ministry to deny that Moscow was behind the assault."); Davis II et al., *supra* note 3, at 2; Thomas Grove & Ann M. Simmons, *Russian Agency at Center of U.S. Hacking Indictment Has Long Operated in the Shadows*, WALL STREET JOURNAL (July 14, 2018), https://www.wsj.com/articles/russian-agency-at-center-of-u-s-hacking-indictment-has-long-operated-in-the-shadows-1531599417#:~:text=Russian%20Agency%20at%20Center%20of%20U.S.%20Hacking%20Indictment,a%20visit%20to%20its%20Moscow%20headquarters%20in%202006.

5. *See, e.g.*, Jack Goldsmith, *Uncomfortable Questions in the Wake of Russia Indictment 2.0 and Trump's Press Conference With Putin*, LAWFARE (July 16, 2018), https://www.lawfareblog.com/uncomfortable-questions-wake-russia-indictment-20-and-trumps-press-conference-putin. The United States and China did reach an understanding in 2015 prohibiting commercial cyber espionage following the U.S. indictment of five People's Liberation Army officers for such behavior. China's commitment, however, appears to have been more a response to domestic politics, and was—in any case—short-lived.

6. Andrzej Kozlowski, *Comparative Analysis of Cyberattacks on Estonia, Georgie and Kyrgyzstan*, 3 EUROPEAN SCIENTIFIC JOURNAL 237, 242–243 (2014); John Markoff, *Before the Gunfire, Cyberattacks,* NEW YORK TIMES (Aug. 12, 2008), https://www.nytimes.com/ 2008/08/13/technology/13cyber.html.

7. Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2018), https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy; Jonathan Kaiman, *China Reacts Furiously to US Cyber-Espionage Charges*, GUARDIAN (May 20, 2014), https://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

8. Goldsmith & Williams, *supra* note 7; Kaiman, *supra* note 7.

cyberattacks continued unabated, following additional indictments in 2017 and 2018.[9]

Outside the United States, some efforts at public attributions of cyberattacks began after a 2017 global ransomware attack. WannaCry malware rapidly spread to over 230,000 computers across more than 150 countries in May of 2017 and wreaked havoc on the U.K. healthcare system.[10] Disguised within a phishing email, once the ransomware infected a computer it worked to encrypt files and prevent the file owners from accessing the encrypted data unless they paid $300 in Bitcoin.[11] In the United Kingdom, affected hospitals had to cancel thousands of medical appointments, and a large number of ambulances and patients were diverted from accident and emergency departments that were rendered unable to treat patients as a result of the attack.[12] Other notable targets of the attack include the Russian Interior Ministry, a local authority in Sweden, and a number of large firms and companies in Spain, France, Portugal, and the United States.[13] The ransomware, built to exploit a weakness in Microsoft systems that the National Security Agency (NSA) had previously identified, employed stolen NSA tools that had been posted online for free public download by a group called the "Shadow Brokers."[14]

The United States response to WannaCry exemplified a State employing domestic criminal prosecution alongside sanctions to back up a public attribution of cyberattack. While press reports indicating that North Korea was responsible were quick to follow the attack, the official attributions took months.[15] In October 2017 British Minister of Security Ben Wallace, without

9. Goldsmith & Williams, *supra* note 7.

10. Matt Reynolds, *Ransomware Attack Hits 200,000 Computers Across the Globe*, NEW SCIENTIST (May 15, 2017), https://www.newscientist.com/article/2130983-ransomware-attack-hits-200000-computers-across-the-globe/; *see also* National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (Apr. 25, 2018), https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

11. *Massive Ransomware Infection Hits Computers in 99 Countries*, BBC (May 13, 2017), https://www.bbc.com/news/technology-39901382.

12. National Audit Office, *supra* note 10.

13. *Massive Ransomware Infection Hits Computers in 99 Countries*, *supra* note 11.

14. *Id.*

15. The *New York Times* purported to cite intelligence officials who felt that North Korea was responsible as soon as three days following the attack. Nicole Perlroth & David E. Sanger, *In Computer Attacks, Clues Point to Frequent Culprit: North Korea*, NEW YORK TIMES (May 15, 2017), https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

sharing any evidence, told the BBC that North Korea was responsible.[16] By mid-December, the United States, United Kingdom, Australia, Canada, New Zealand, and Japan issued coordinated statements attributing the WannaCry actions to North Korea.[17] In a press briefing, White House Homeland Security Advisor Thomas Bossert stated that the United States "do[es] not make this allegation lightly. We do so with evidence, and we do so with partners."[18] No affirmative actions were taken until June 2018, when the United States brought criminal charges against North Korean citizen Park Jin Hyok, who was alleged to be a member of "a government-sponsored hacking team."[19] Hyok was charged with working for "a North Korean government front company . . . to support the [North Korean] government's malicious cyber actions," which included those of WannaCry.[20] Three months after the charges were brought, the U.S. Treasury Department sanctioned Hyok.[21]

16. Dan Bilefsky, *Britain Says North Korea Was Behind Cyberattack on Health Service*, NEW YORK TIMES (Oct. 27, 2017), https://www.nytimes.com/2017/10/27/world/europe/uk-ransomware-hack-north-korea.html.

17. Thomas P. Bossert, *It's Official: North Korea Is Behind WannaCry*, WALL STREET JOURNAL (Dec. 18, 2017), https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537; Press Release, U.K. Foreign & Commonwealth Office, Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks (Dec. 19, 2017), https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks; Greta Bossenmaier, Communications Security Establishment, *CSE Statement on the Attribution of WannaCry Malware,* GOVERNMENT OF CANADA (Dec. 19, 2017), https://cse-cst.gc.ca/en/information-and-resources/announcements/cse-statement-attribution-wannacry-malware (noting Canada's agreement with attribution of WannaCry to North Korea); Joint Media Release, Australia Ministry for Foreign Affairs, Attributing the 'WannaCry' Ramsomware to North Korea (Dec. 20, 2017), https://www.foreignminister.gov.au/minister/julie-bishop/media-release/attributing-wannacry-ramsomware-north-korea; *New Zealand Concerned at North Korean Cyber Activity*, NATIONAL CYBER SECURITY CENTRE (Dec. 20, 2017), https://www.ncsc.govt.nz/newsroom/new-zealand-concerned-at-north-korean-cyber-activity/; Press Release, The U.S. Statement on North Korea's Cyberattacks, MINISTRY OF FOREIGN AFFAIRS OF JAPAN (Dec. 20, 2017), https://www.mofa.go.jp/press/release/press4e_001850.html.

18. White House, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017), https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

19. Criminal Complaint, United States v. Park Jin Hyok, No. MJ 18-1479 (C.D. Cal. June 8, 2018), https://www.justice.gov/opa/press-release/file/1092091/download.

20. *Id.*

21. Press Release, Treasury Targets North Korea for Multiple Cyber-Attacks, U.S. DEPARTMENT OF THE TREASURY (Sept. 6, 2018), https://home.treasury.gov/news/press-releases/sm473.

The following year, Treasury sanctioned additional North Korean entities for their involvement in the WannaCry attacks.[22]

In June 2017 the NotPetya cyberattack encrypted computers' master boot records and struck Ukraine before spreading worldwide, impacting major companies and causing $10 billion in damages.[23] Ukraine first accused Russia of responsibility in July 2017, and the United Kingdom and the United States specifically attributed NotPetya to the Russian military in 2018.[24] Also, in 2018, the United States and European governments coordinated to attribute to the Russian Main Intelligence Directorate (GRU) a series of cyberattacks against entities investigating Russian misdeeds, including the poisoning of a former Russian spy, the shooting down of Malaysia Airlines Flight MY17, and hacking U.S. and international anti-doping agencies.[25] Russia denied involvement in each instance.[26]

Part II of this article will briefly explain what makes cyber attribution challenging. Part III uses examples to tell the story. Part IV reviews the evolving technical and practical obstacles to timely attribution. Parts V–VII will show that sparse cyber attribution doctrine is part of a generally anemic and incomplete set of secondary international law principles that fail to provide a normative structure for cyber relations between States. The same incompleteness characterizes the law governing victim State responses, considered next. Among other shortcomings, there is little clarity on a standard

---

22. Press Release, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups, U.S. DEPARTMENT OF THE TREASURY (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774.

23. Nicole Perlroth et al., *Cyberattack Hits Ukraine Then Spreads Internationally*, NEW YORK TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

24. White House, Statement from the Press Secretary (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

25. David E. Sanger et al., *Russia Targeted Investigators Trying to Expose Its Misdeeds, Western Allies Say*, NEW YORK TIMES (Oct. 4, 2018), https://www.nytimes.com/2018/10/04/us/politics/russia-hacks-doping-poisoning.html.

26. *Former Russian Spy Poisoned by Nerve Agent on Door of Home in England, Police Say,* CNBC, https://www.cnbc.com/2018/03/29/ex-russian-spy-skripal-poisoned-by-nerve-agent-on-door-of-home.html (last visited July 13, 2021); Opinion, *Peeling Away Russia's Lies About the Downed Malaysia Airlines Flight*, WASHINGTON POST (June 20, 2019), https://www.washingtonpost.com/opinions/global-opinions/peeling-away-russias-lies-about-the-downed-malaysia-airlines-flight/2019/06/20/611a7a1c-92b6-11e9-aadb-74e6b2b46f6a_story.html; *Russian Envoy Rejects Reports of Cybercrimes*, ASSOCIATED PRESS Oct. 4, 2018, https://apnews.com/article/hacking-winter-olympics-ap-top-news-olympic-games-international-news-f267a56952704de6bdddadac6193f854?utm_source=twitter&utm_medium=ap&utm_campaign=socialflow.

of proof that States should meet in attributing a cyberattack to another State. While some States are taking steps to attribute significant cyberattacks, these accusations bring little or no legal consequences. Further, most of the world has not bothered with attribution, and the result is a combination of Wild West virtual landscape and a lot of cat and mouse games. The article will conclude in part VIII by reviewing reforms that could improve cyber attribution by tethering it more concretely to international law.

II. WHAT MAKES CYBER ATTRIBUTION CHALLENGING?

The international law on State responsibility specifies that attribution is "the operation of attaching a given action or omission to a State."[27] Although the technical capabilities for cyber attribution—identifying the machine or IP address of the attacking machine—have improved considerably in recent years, the law of cyberattack attribution has remained mostly undefined for various reasons.

One reason is continuing uncertainties and delays in achieving attributions. Attackers complicate attributions by deliberately obscuring their identities or by staging their cyberattacks to appear as though they were caused by someone else. Even with recent advances, knowing the machines or IP addresses responsible for the hack is often difficult, costly, and time-consuming, and knowing those things does not necessarily lead easily to the responsible State. Technical and on-the-ground intelligence and police work are often necessary to establish reliable attribution. Even extensive efforts do not always produce unequivocal proof.[28]

Apart from identifying the responsible actor, attribution has also failed to coalesce on what proof should suffice for cyberattack attribution, whether attributions should be public, and what consequences should follow from a successful attribution. More fundamentally, the lack of consensus on standards of proof, public attributions, and the legal consequences of attribution

27. Int'l Law Comm'n, *Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries*, 56 U.N. GAOR Supp. No. 10, art. 2, cmt. ¶ 12, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), https://legal.un.org/ilc/documentation/english/reports/a_56_10.pfd; *see also* Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31 EUROPEAN JOURNAL OF INTERNATIONAL LAW 969, 985–90 (2020).

28. Good background on the technical challenges of attribution may be found in Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 JOURNAL OF STRATEGIC STUDIES 4, 14–23 (2015).

have stymied efforts to clarify what international legal rules apply when cyber operations target civilians and their infrastructure below the use of force threshold and outside of armed conflicts.

As a result, some States use cyber tools to strike with impunity, knowing (or at least strongly suspecting) that their digital attacks will either not prompt a response or lead to a response that is no more than the "naming and shaming" that goes on in the diplomatic world and in the media. Meanwhile, the threats to infrastructure and extraction of data and intellectual property by cyber means continue at great cost to governments and private industry. We now know that increasingly sophisticated forms of offensive hacking are capable of causing more significant harm, even catastrophic damage, such as shutting down financial systems, sabotaging critical infrastructure, and scrambling communications.[29] These continuing threats make knowing and attributing the source of the cyber intrusion especially important so that States and the international community can respond accordingly.

In addition, the inability to identify the source of a cyberattack potentially increases the risks of confusion and escalation. When the United States released an unclassified summary of its Department of Defense Cyber Strategy in September 2018, attention focused on its commitment to "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[30] Yet some see "defending forward" as putting the U.S. military on an offensive, rather than defensive, footing. The recent shift in U.S. cyber policy deepens a cyber variant on a classic security dilemma between States: as one State takes steps to defend itself in cyberspace, it inadvertently threatens other States with what appears to be offensive action. In practice, "defending forward" can look like attacking forward to those experiencing an intrusion. One implication is an increased

29. *See*, *e.g.*, Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG (Dec. 10, 2014), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar; *10 Catastrophic Cyberattacks From 2019*, ARTIC WOLF (Dec. 23, 2019), https://arcticwolf.com/resources/blog/10-catastrophic-cyberattacks-from-2019 (listing significant cyberattacks in 2019).

30. U.S. Department of Defense, *Cyber Strategy Summary* 1 (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

tendency to escalate conflicts.[31] In an environment where escalation fears are on the rise, the possibility that cyber intrusions could spark destructive and even destabilizing conflicts between States places a premium on confident attribution of cyber intrusions and agreed-upon norms limiting cyber intrusions.

III. RECENT EXAMPLES

In July 2020, in the midst of the global coronavirus pandemic, the U.S., British, and Canadian governments accused Russia of using cyber means in attempts to steal intelligence on vaccines from universities, companies, and other health care organizations.[32] According to the NSA, the group of hackers known as both APT29 and Cozy Bear (the same group implicated in the 2016 Democratic National Committee break-ins into Democratic Party servers) attempted to exploit the chaos created by the pandemic.[33] The attacks were, of course, conducted in secret with malware that disguised its origins. Despite these new public accusations, the uncertain attribution of the cyberattacks to Russia made it easy for Russia to deny responsibility.

A few days later, the Justice Department accused two Chinese hackers of trying to acquire vaccine research on behalf of China's intelligence service.[34] Despite the outrage expressed in some quarters that the Russians and Chinese would use digital tools to hack Western research into coronavirus vaccines, cyber experts cautioned that this form of cyber espionage—even if clearly attributed (it has not been)—is neither authorized nor forbidden by international law.[35]

---

31. Ben Buchanan & Robert D. Williams, *A Deepening U.S.-China Cybersecurity Dilemma*, LAWFARE (Oct. 24, 2018), https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma; Robert Chesney, *An American Perspective on a Chinese Perspective on the Defense Department's Cyber Strategy and 'Defending Forward,'* LAWFARE (Oct. 23, 2018), https://www.lawfareblog.com/american-perspective-chinese-perspective-defense-departments-cyber-strategy-and-defending-forward.

32. Julian E. Barnes, *Russia is Trying to Steal Virus Vaccine Data, Western Nations Say*, NEW YORK TIMES (July 16, 2020), https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html.

33. *Id.*

34. Julian E. Barnes, *U.S. Accuses Hackers of Trying to Steal Coronavirus Vaccine Data for China*, NEW YORK TIMES (July 21, 2020), https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html.

35. In contrast, an executive order issued by President Trump in 2020 confers on the Central Intelligence Agency authorities that open the door to expansive hacking activities,

Meanwhile, in late June and early July of 2020 explosions did significant damage to advanced nuclear centrifuges at Natanz in Iran.[36] It remains unclear whether the destruction was caused by an explosive device planted in the heavily guarded facility or was instead the product of a cyberattack that triggered a gas line explosion. Although Iranian officials and many in the media assumed that Israel was behind this latest attack on the Iranian nuclear initiative, Israel denied involvement.[37] Like the 2010 Stuxnet malware, the 2020 attacks on Iranian centrifuges may have constituted a use of force at international law, and thus a clearer assignment of the rights and responsibilities of the involved States, whichever they turn out to be, is needed.[38] In any case, the absence of agreed-upon standards for attribution means that the perpetrator will not suffer legal consequences.

Around the same time, despite years of fears about potential life-threatening cyberattacks from Russia, Iran, or North Korea that could resemble a "cyber 9/11" or "cyber Pearl Harbor," the first cyberattack directly linked to a death came from common criminals. In September 2020 an ailing woman was turned away from a hospital in Dusseldorf, Germany, that was in the grips of a ransomware attack. She died on the way to another hospital.[39]

Then, further illustrating the technical and practical challenges in attributing cyberattacks, in January and February 2021 news media reported that Russia and China executed major cyber operations against the networks of U.S. companies and government agencies. Both were apparently espionage operations designed to give foreign intelligence agencies access to sensitive

---

including disrupting foreign elections, energy services, or financial transactions that run directly counter to international norms that the United States has long advocated for cyberspace. Zach Dorfman et al., *Secret Trump Order Gives CIA More Powers to Launch Cyberattacks*, YAHOO NEWS (July 15, 2020), https://www.yahoo.com/now/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html. The 2020 executive order implements broad authorization provided by Congress in 2018 to give the Central Intelligence Agency broad powers to conduct actions in cyberspace without White House prior approval when targeting Russia, China, Iran, and North Korea.

36. *Iran Nuclear: Natanz Fire Caused 'Significant' Damage*, BBC NEWS (July 5, 2020), https://www.bbc.com/news/world-middle-east-53300579.

37. Borzou Daragahi, *Israel Speculated to be Behind Mysterious Explosion at Iranian Nuclear Site*, INDEPENDENT (July 6, 2020), https://www.independent.co.uk/news/world/middle-east/iran-nuclear-explosion-israel-natanz-a9603976.html.

38. *See* Kristen E. Eichensehr*, The Law and Politics of Cyberattack Attribution*, 67 UCLA LAW REVIEW 520, 582 (2020).

39. *German Hospital Hacked, Patient Taken to Another City Dies*, AP NEWS (Sept. 17, 2020), https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

material of value to their governments. The Russian malware operation—SolarWinds—gained access to the networks of thousands of American companies and organizations and learned about supply chain vulnerabilities and backdoors. Through careful selection of the highest value targets, the Russians were able to remain undetected on those company networks for close to nine months.[40]

The putative Chinese operation, known as the Microsoft Exchange hack, was designed to use zero-day vulnerabilities in Microsoft Exchange email servers to gain access to the email servers of tens of thousands of businesses and local governments. Once Chinese hackers penetrated Microsoft Exchange, they attacked other corporate and local government organizations. Those businesses and local governments were then subject to pillage and ransom demands by the hackers, whether the original Chinese perpetrators or criminals that bought into the hack.[41] When Microsoft learned of the breach, it prepared a patch. The Chinese learned of the planned patch and automatically scanned the vulnerable Exchange servers before they could be patched.[42]

The common ingredient in the recent Russian and Chinese cyberattacks is that U.S. intelligence agencies did not discover them until the damage was done. Definitive attribution of SolarWinds by U.S. officials was made in April 2021.[43] The Biden administration formally accused the Chinese government of attacking the Microsoft Exchange email server software on July 19, 2021.[44]

---

40. David E. Sanger et al., *White House Weighs New Cybersecurity Approach After Failure to Detect Hacks*, NEW YORK TIMES (Mar. 14, 2021), https://www.nytimes.com/2021/03/14/us/politics/us-hacks-china-russia.html.

41. Nicholas Weaver, *The Microsoft Exchange Hack and the Great Email Robbery*, LAWFARE (Mar. 9, 2021), https://www.lawfareblog.com/microsoft-exchange-hack-and-great-email-robbery.

42. Sanger et al., *supra* note 40.

43. On April 15, 2021, the White House attributed the SolarWinds cyberattack to the Russian foreign intelligence service and announced the official response. White House, Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government (Apr. 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/;
Press Release, Treasury Sanctions Russia with Sweeping New Sanctions Authority, U.S. DEPARTMENT OF THE TREASURY (Apr. 15, 2021), https://home.treasury.gov/news/press-releases/jy0127.

44. Dmitri Alperovitch & Ian Ward, *The White House Responded to the Chinese Hacks of the Microsoft Exchange Servers This Week. Is It Enough?*, LAWFARE (July 21, 2021), https://

Lacking an international legal regime for attribution and thus for State responsibility, in recent years victim States have often retaliated for cyber intrusions with their own cyberattacks. For example, experts and U.S. government officials believe that as retaliation for suspected U.S. and Israeli cyberattacks, Iran has targeted American financial institutions, a major Las Vegas casino, a dam in the New York City suburbs, and the water supply system in Israel.[45] There has been no formal attribution of these attacks by Iran, just as the attacks on Iranian centrifuges were not attributed.

IV. ATTRIBUTION OBSTACLES—TECHNICAL AND PRACTICAL

As recently as 2010, then-Deputy Secretary of Defense William Lynn bemoaned the difficulties in attributing cyberattacks and wrote that "[t]he forensic work necessary to identify an attack may take months, if identification is possible at all."[46] By 2012 Secretary of Defense Leon Panetta declared that the United States had made "significant advances" in cyber attribution and that "potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions."[47] In September 2018 the Office of the Director of National Intelligence described cyberattack attribution as "difficult but not impossible."[48] The 2020

---

www.lawfareblog.com/white-house-responded-chinese-hacks-microsoft-exchange-servers-week-it-enough.

45. Tracy Connor & Tom Winter, *Iranians Charged With Cyber Attacks of U.S. Banks, Dam*, NBC NEWS (Mar. 24, 2016), https://www.nbcnews.com/news/us-news/iranians-charged-hacking-attacks-u-s-banks-dam-n544801; Jose Pagliery, *Iran Hacked an American Casino, U.S. Says*, CNN (Feb. 27, 2015), https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html; Joby Warrick & Ellen Nakashima, *Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran*, WASHINGTON POST (May 8, 2020), https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.

46. William F. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFFAIRS 97, 99 (2010).

47. Leon E. Panetta, U.S. Secretary of Defense, Remarks on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012), https://www.hsdl.org/?view&did=724128.

48. Office of the Director of National Intelligence, *A Guide to Cyber Attribution* 2 (Sept. 14, 2018), https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_ Cyber_ Attribution.pdf; *cf.* Jeremy Hunt, U.K. Foreign Secretary, Speech at Glasgow University: Deterrence in the Cyber Age (Mar. 7, 2019), GOV.UK, https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary ("Along with

SolarWinds and Microsoft Exchange attacks were not even detected by U.S. intelligence agencies for as long as nine months (SolarWinds),[49] and official attribution of SolarWinds was not announced until April 2021.[50]

In general, significant technological strides in attributing cyber events in the last decade have made the attribution task "more nuanced, more common, and more political than has typically been acknowledged."[51] The nuance involves combining experienced and disciplined technical operators with the intuition and judgment of intelligence professionals. The political aspect includes assessing what is at stake in making the attribution judgment, starting with the damage incurred, whether physical, financial, or reputational.[52] A prime example is the U.S. attribution of Russian interference in the 2016 election. Although an official attribution was made public in the last days of the Obama administration, more detailed and evidence-based attributions accumulated in U.S. intelligence agencies and Congress through President Trump's first term, culminating in the August 2020 release of a lengthy report of the Senate Select Committee on Intelligence detailing the Russian cyber intrusions.[53] As the 2016 election interference example illustrates, attribution is often expressed in degrees of certainty. It requires input from a range of actors and sources, including technical forensics, human intelligence, signals intelligence, history, and diplomatic relations.[54]

The declassified *Background to "Assessing Russian Activities and Intentions in Recent US Elections"* reminds us that intelligence analysis of cyber intrusions

---

our allies, we have improved our collective ability to detect those responsible for malign actions in cyberspace, including election interference.").

49. Sanger et al., *supra* note 40.

50. The SolarWinds attack was attributed to the Russian Foreign Intelligence Service on April 15, 2021. *See* White House, *supra* note 43; *see also* Kristen Eichensehr, *SolarWinds: Accountability, Attribution, and Advancing the Ball*, JUST SECURITY (Apr. 16, 2021), https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball/.

51. Rid & Buchanan, *supra* note 28.

52. *Id.* at 7 ("attribution is an art as much as a science").

53. S. REP. NO. 116-290, RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION (2020). For an in-depth look at the long saga of Russian interference in the United States and the history of attribution, see OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (Jan. 6, 2017), https://digitallibrary.utah.gov/awweb/awarchive?type=file&item=8353 .

54. *See* John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARVARD NATIONAL SECURITY JOURNAL 391, 396–97 (2016) (discussing the expertise required for complex attribution analysis).

seeks "to reduce the uncertainty surrounding foreign activities, capabilities, or leaders' intentions."[55] 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.[56] 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."[57]

At least in the most advanced States digital forensics and threat intelligence have evolved to the point that quick and reliable attribution of the machines responsible for cyber intrusions is the norm.[58] Of course, attribution in cyber is only possible if the attacks are detected. The SolarWinds and Microsoft Exchange hacks avoided sophisticated NSA detection capabilities by launching their tools from inside the United States, where NSA does not operate. At the same time, the advances in technical attribution may be matched by advances in the cyber attackers' capabilities to hide their identities, leading to an unending cat-and-mouse game.[59] Thus, identifying the persons, organizations, or States that are legally responsible for a cyberattack remains challenging.[60] The problems derive from technical means of deception and anonymity, but they are also due to the vagaries of the process of fixing responsibility for cyberattacks within the international community and the malleability and open-endedness of the few attribution rules that currently exist in international law.[61]

In the aggregate, understanding the technical and practical components of attribution is essential but not sufficient for shaping a legal and policy

---

55. *Id.*

56. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *supra* note 53.

57. *Id.* at 2.

58. 1 ROBERT S. MUELLER III, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 7 (2019), https://www.justice.gov/storage/report_volume1.pdf ("On October 7, 2016, . . . Wikileaks made its second release: thousands of John Podesta's emails that had been stolen by the GRU in late March 2016 . . . . That same day . . . the Department of Homeland Security and the Office of the Director of National Intelligence issued a joint public statement 'that the Russian Government directed the recent compromises of e-mails from US persons and institutions.'").

59. *See* Eichensehr, *supra* note 38, at 532.

60. *See, e.g.*, Carlin, *supra* note 54, at 416; Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, 70 JOURNAL OF INTERNATIONAL AFFAIRS 75, 82–83 (2016).

61. *See* William Banks, *State Responsibility and Attribution of Cyber Intrusions After* Tallinn 2.0, 95 TEXAS LAW REVIEW 1487, 1494–97 (2017).

strategy to deter harmful but below the use of force threshold for cyber intrusions in the future. Meanwhile, as cyber intrusions have proliferated in recent years, and despite the absence of a durable legal regime that punishes malevolent cyber intrusions, many States have invested in doing attribution well and, as a result, deterring or at least discouraging States and other cyber intruders. When attribution is done badly or not at all, States lose credibility and likely effectiveness in dealing with those who would harm the State and its citizens. These risks hold for State-on-State interactions across the spectrum of cyber operations—from espionage to destructive attacks on infrastructure. Yet even persuasive attribution does not make up for the absence of cyber-specific legal norms specifying what constitutes adequate attribution at international law. Nor have the technical advances in cyber attribution led to emerging cyber law in the area of State responsibility.

V. A PATH TO LEGAL CONSEQUENCES FOR CYBER ATTRIBUTION?

When the international community recognized nearly two decades ago that cyberattacks were becoming a new form of State-on-State warfare, government lawyers were challenged either to fit cyber conflict into the paradigm of kinetic war and armed conflict or to develop a new set of rules for cyber. The United States and its allies sought to reassure the international community that the *jus ad bellum* and *jus in bello* frameworks for kinetic warfare could and would provide an effective overlay for the new era of cyber warfare.[62] Over the last two decades, governments and scholars labored over the nuances in deciding when a cyberattack might amount to a use of force or armed attack and, thus, whether international humanitarian law applies in the cyber domain. When cyber weapons cause destruction or injury, the kinetic model works reasonably well in the cyber realm. However, because the vast majority of cyberattacks have less than destructive impacts, the law for con-

62. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf ("The development of norms for state conduct in cyberspace does not require reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."); *see also* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael N. Schmitt gen. ed., 2013); TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0].

trolling the vast majority of cyberattacks has foundered in the underdeveloped international law of State responsibility, sovereignty, countermeasures, and retorsion.

The law of State responsibility has long been an underdeveloped area of international law, even before layering on the cybersecurity context.[63] The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts are not codified, but many of its provisions reflect widely accepted customary international law.[64] The Draft Articles provide helpful and adequate guidance on when States may attribute cyberattacks to another State, including in situations where a State has exercised "effective control" over the cyber actions of a private actor.[65]

Unfortunately, the Draft Articles and customary international law are less helpful in prescribing the law of State responsibility that would say when States are *required* to attribute cyberattacks to another State.[66] Some States have taken tentative steps toward advancing a legal framework for cyber attribution and the attendant State responsibility. For example, the United States has suggested that certain cyber operations, such as the 2015 Sony hack[67] and 2016 election interference, violated "established international norms."[68] Of course, the U.S. statements are silent on which norms it believes were violated. Nor do the supposed norm violations carry with them any consequences.

Nonetheless, the U.S. accusations also served as an invitation to other like-minded States to express similar views on the appropriate norms of behavior. In the case of U.S. accusations about Russian election interference, foreign and security ministers from the G7 subsequently issued a joint state-

63. *See* Eichensehr*, supra* note 38, at 524.

64. Int'l Law Comm'n, *supra* note 27.

65. *Id.* at 47–48, 50.

66. *See* Efrony & Shany, *supra* note 3, at 654.

67. John Kerry, U.S. Secretary of State, Press Statement, Condemning Cyber-Attack by North Korea (Dec. 19, 2014), https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm (describing 2014 Sony hack as a violation of "international norms").

68. *See* The White House, Office of the Press Secretary, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (opposing "Russia's efforts to undermine established international norms of behavior and interfere with democratic governance").

ment denouncing foreign attempts to interfere in democratic processes, including "through cyber-enabled activities."[69] That norm was then endorsed by over one thousand governments, firms, universities, and civil society institutions who have signed the French government-led *Paris Call for Trust and Security in Cyberspace*.[70]

While States have continued mostly to muddle through their responses to cyberattacks, several scholars and groups of international lawyers have urged the adoption of norms that could be embraced by States in their public or non-public attributions of cyberattacks. For example, a 2015 consensus report of the UN Group of Governmental Experts on Information Security recommended norm candidates for good state cyber behavior,[71] and a set of best practices was promulgated by the Organization of Security and Cooperation in Europe in 2016.[72]

Several scholars evaluated alleged cyberattacks by Russia in the 2016 U.S. election and North Korea in the WannaCry malware attack in 2017. They accused both States of international law violations based on attribution that may be surmised from publicly available sources.[73] Even when not formalized or documented by States accusing other States of international law violations, attributions of cyberattacks and associated violations of international

69. G7, Joint Statement of Foreign and Security Ministers, Defending Democracy—Addressing Foreign Threats (Apr. 23, 2018), http://www.g8.utoronto.ca/foreign/180423-democracy.html.

70. Ministère de l'Europe et des Affaires Étrangères [Ministry of Europe and Foreign Affairs], *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace* (Nov. 12, 2018), https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (includes list of stakeholder signatories).

71. *See* Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 13, U.N. Doc. A/70/174 (July 22, 2015) (hereinafter 2015 GGE Report).

72. *See, e.g.*, Organization for Security and Co-operation in Europe, Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies (Mar. 10, 2016), https://www.osce.org/files/f/documents/d/a/227281.pdf.

73. *See, e.g.,* Michael Schmitt & Sean Fahey, *WannaCry and the International Law of Cyberspace*, JUST SECURITY (Dec. 22, 2017), https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/; Banks, *supra* note 61; Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEXAS LAW REVIEW 1579 (2017).

law in press briefings or diplomatic notes, or even media reports and scholarly analyses, can give rise to State practice that over time may develop as customary international law.[74]

At the same time, the informal accusations and claims of State attribution for a cyberattack can, by their public nature, serve to limit the chances that the offending State's behavior will be recognized as lawful. Good examples include Estonia's claims of Russian responsibility for the 2007 cyberattacks against Estonian government and private sector infrastructure, President Obama's criticisms of Chinese cyber-espionage,[75] the public claims by the United States, United Kingdom, and Australia that North Korea was responsible for WannaCry, and the Obama administration's criticisms of Russian election interference in 2016.[76]

Of course, public attribution brings along with it knowledge of the victim State's vulnerabilities. States will, of course, avoid advertising how to steal their protected data or shut down their electric grid. As such, attribution may be provided in only general terms. Similarly, the United States and other States tailor attribution to protect intelligence sources and methods. Because a major part of attributing a cyberattack involves human and technical intelligence work, States will work to preserve the anonymity of the intelligence so that it may be used again.

Despite the sporadic positive steps taken by some States to attribute cyberattacks, the public attributions over the past decade have not been tied to law violations. States typically accuse the attributed State of bad behavior ("malicious")[77] or of violating some normative standard,[78] without specifying which norm or ascribing consequences for the violation. An especially colorful attribution of a cyberattack was President Obama's reference to the

74. *See, e.g.,* James Stavridis, *How to Win the Cyberwar Against Russia*, FP (Oct. 12, 2016), https://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/; *see also* George Norman & Joel P. Trachtman, *The Customary International Law Game*, 99 AMERICAN JOURNAL OF INTERNATIONAL LAW (2005).

75. Cory Bennett, *Obama Calls Out China for Cyber Espionage*, THE HILL (Feb. 6, 2015), https://thehill.com/policy/cybersecurity/231998-obama-security-plan-highlights-chinese-cyber-espionage.

76. *See* Banks, *supra* note 61, at 1489–92.

77. *See, e.g.,* Press Release, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks, U.S. DEPARTMENT OF THE TREASURY (Mar. 15, 2018), https://home.treasury.gov/news/press-releases/sm0312; The White House, *supra* note 68.

78. Kerry, *supra* note 67 (describing the 2014 Sony hack as a violation of "international norms").

Sony Pictures hack as an act of "cyber vandalism"—an apt description of what the North Koreans did, perhaps, but a phrase utterly without normative or legal grounding.[79] While the United Kingdom accused the Russian GRU of international law violations in several of its cyberattacks directed at Britain, Ukraine, and the United States, it declined to say which laws were broken in any specific operation.[80]

VI. BUILDING THE INTERNATIONAL LEGAL CASE FOR STATE RESPONSIBILITY IN BELOW-THRESHOLD CYBERATTACKS

The Wild West environment for cyber exploitation persists in part because of a lack of agreed-upon and enforceable rules for attributing cyber intrusions to the responsible actor and then punishing the wrongdoing. Without attribution rules and practices that are transparent and widely shared, there is no incentive for attackers to stop what they are doing. 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.

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 Articles on State Responsibility. While not binding on any nation, the ILC articles were commended to member States by the United Nations General Assembly in 2012 and have been cited repeatedly by courts, tribunals, and other bodies.[81] The unsurprising threshold un-

79. The White House, Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea" (Jan. 2, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s; Sean Sullivan, *Obama: North Korea Hack "Cyber-vandalism," Not "Act of War,"* WASHINGTON POST (Dec. 21, 2014), https://www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/; Ellen Nakashima & Devlin Barrett, *U.S. Charges North Korean Operative in Conspiracy to Hack Sony Pictures, Banks*, WASHINGTON POST (Sept. 6, 2018), https://www.washingtonpost.com/world/national-security/justice-department-to-announce-hacking-charges-against-north-korean-operative-the-charge--stemming-from-the-2014-sony-pictures-case--is-the-first-against-a-pyongyang-spy/2018/09/06/f477bfb2-b1d0-11e8-9a6a-565d92a3585d_story.html.

80. *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*, NATIONAL CYBER SECURITY CENTRE (Oct. 3, 2018), https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

81. TALLINN MANUAL 2.0, *supra* note 62, at 79 n.112.

derstanding on State responsibility 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."[82] States should thus care a great deal about cyber attribution precisely because the absence of attribution precludes State responsibility.

In addition, a persuasive case may be made that international law *requires* that States attribute internationally wrongful acts in cyberspace if they expect to respond in ways that would otherwise violate international law, e.g., by using force or engaging in countermeasures. For a use of force to be lawful, it must respond to an armed attack.[83] If the responsive use of force is not, in fact, defensive, the putative victim State's use of force would be prohibited by the UN Charter.[84] Similarly, the Draft Articles state: "An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply" with its legal obligations.[85] At least by implication, attribution of a cyberattack is required before a State may lawfully engage in countermeasures.

Another potential contributor to international law attribution requirements in the cyber domain is State sovereignty. Two competing views command attention. Below the use of force threshold and absent a prohibited intervention, does international law bar violations of sovereignty? Or is sovereignty merely a background principle that informs customary international law?[86] Sovereignty becomes relevant and potentially important for cyber attribution to the extent that a cyberattack from one State that penetrates another State is viewed as an international law violation. If the incoming cyberattack violates a sovereignty rule, countermeasures may be available to the victim State and, as explained above, attribution of the attack may be required. In some instances, even cyber espionage may be unlawful at international law if sovereignty is treated as a rule.

A growing number of States, including France, Austria, the Czech Republic, Finland, Germany, Iran, the Netherlands, and New Zealand, have

82. *Id.* at 84 (rule 14).

83. Int'l Law Comm'n, *supra* note 27, art. 21.

84. *Id.*

85. *Id.* art. 49.

86. *See* Eichensehr*, supra* note 38, at 576 (Making the case that "States are coequal sovereigns in the international system, not usually subordinates governed by each other's domestic laws. Domestic legal standards—especially divergent ones—cannot reasonably be expected to generate cross-national agreement on the bounds of permissible state behavior any more than disparate policy choices can.").

signed on to the view that sovereignty is violated when one State's cyberattack causes "unwelcome effects" in another State.[87] Although the precise scope of a sovereignty rule remains unclear,[88] under such a rule States are responsible for the wrongful cyber-related acts of their own officials, agents, contractors, non-State actors, and other States, to the extent they actually control the operations.[89] States do not escape legal responsibility for internationally wrongful acts by perpetrating them through proxies. Taken to its logical extreme, such an approach to sovereignty could mean that virtually any nonconsensual cyber operation carried out by agents under the direction or control of one State in another State has violated sovereignty.[90] In practice, however, these "purist" sovereignty States have not followed their own purported doctrine and have instead followed the approach to sovereignty set forth in a recent German government position paper, which maintains that "negligible physical effects and functional impairments below a certain impact threshold cannot—taken by themselves—be deemed to constitute a violation of territorial sovereignty."[91]

The United Kingdom and the United States have questioned whether sovereignty is itself an enforceable rule or is instead a background principle

87. *See id.* at 575; Jack Kenny, *France, Cyber Operations and Sovereignty: The 'Purist' Approach to Sovereignty and Contradictory State Practice*, LAWFARE (Mar. 12, 2021), https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice.

88. *See* Eichensehr*, supra* note 38, at 576 ("Often, applying existing international law is sufficient, but in the context of the evidentiary standards for attribution, the underdeveloped nature of existing international law on evidence suggests that a mix of existing and new international law will be required.").

89. TALLINN MANUAL 2.0, *supra* note 62, at 17 (rule 4); MINISTÈRE DES ARMÉES, DROIT INTERNATIONAL APPLIQUÉ AUX OPERATIONS DANS LE CYBERSPACE [Ministry of the Armed Forces, International Law Applied to Cyberspace] 1.1.1 (Sept. 9, 2019) (Fr.); Dutch Minister of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace app. at 2 (July 5, 2019), https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

90. Kenny, *supra* note 87.

91. Federal Government of Germany, On the Application of International Law in Cyberspace, § II(a) (Mar. 2021), https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf; *see also id.*

that informs the content of other rules, such as the duty of non-intervention.[92] These disparate views on sovereignty could, in turn, lead to different understandings of when attribution is required. Consider the SolarWinds cyberattack. As has been reported, assume that the United States believes that the Russian government was responsible for SolarWinds. The United States may well wish to counter the Russian hack with an equivalent cyber operation targeting Russian firms. If sovereignty is an international law rule, Russia engaged in internationally wrongful acts and the United States is entitled to take countermeasures, but only if the United States attributes the incoming attack to the Russian government. If the Russian attack is not attributed, any counter cyber operation by the United States would itself violate sovereignty and international law, permitting countermeasures by Russia. If, instead, sovereignty is a background principle and not law, SolarWinds is not an internationally wrongful act, and neither attribution nor countermeasures are required.[93]

By implication, States that view sovereignty as a background principle and not enforceable international law could argue reasonably that many of its cyber actions—such as the United States' responses to SolarWinds—are retorsion and thus need not be preceded by attribution of the incoming cyberattack to a State.[94] For the United States and the United Kingdom, the defend forward and persistent engagement policies of actively pursuing cyber attackers globally do not require attribution of cyberattacks to a State

92. *See, e.g.*, 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/; Jeremy Wright, U.K. Attorney General, Speech at Chatham House Royal Institute for International Affairs, Cyber and International Law in the 21st Century (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. The General Counsel of the U.S. Department of Defense has expressed a similar view. Paul C. Ney, Jr., General Counsel, U.S. Department of Defense, 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/ ("For cyber operations that would not constitute a prohibited intervention or use-of-force [i.e., those that might be covered by a rule of sovereignty], the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory.").

93. *See* Eichensehr*, supra* note 38, at 556 ("an injured state may only take countermeasures against the state responsible for the internationally wrongful act, necessitating that the victim state identify the state responsible").

94. *Id.*

because below threshold attacks are not internationally wrongful acts. Meanwhile, as noted above, other States may consider such operations violations of their sovereignty.[95]

Beyond the overarching debate on sovereignty, cyberattacks that are "coercive" may also violate international law. Outside an armed conflict, international law forbids cyber intrusions that violate the prohibition on intervention.[96] Based on the principle of sovereignty, but different from it, the non-intervention principle forbids coercive intervention by cyber means.[97] The consensus among experts is that State-on-State cyber intrusions that are not coercive but are "detrimental, objectionable, or otherwise unfriendly" are not international legal violations.[98] As confirmed by the International Court of Justice (ICJ) in the *Nicaragua* judgment, "the element of coercion . . . forms the very essence of . . . prohibited intervention."[99] Yet, international law has never had a precise definition of coercion. According to a consensus among the cyber experts who contributed to *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."[100] A State compels another State by, for example, providing cyber training or supplying malware to a private group operating in the compelled State.[101]

---

95. The United Kingdom appeared to take an internally inconsistent position in 2018 when its National Cyber Security Centre issued a news release attributing multiple cyber campaigns to Russia's GRU, the State military intelligence service. The release claimed that the Russian operations were "conducted in flagrant violation of international law." *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*, NATIONAL CYBER SECURITY CENTRE (Oct. 3, 2018), https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed. However, if sovereignty is a background principle and not a rule of international law, the Russian intrusions were disturbing and perhaps repugnant but not unlawful. Jeffrey Biller & Michael Schmitt, *Un-caging the Bear? A Case Study in Cyber* Opinio Juris *and Unintended Consequences*, EJIL:Talk (Oct. 24, 2018), https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/.

96. TALLINN MANUAL 2.0, *supra* note 62, at 312 (rule 66(1)).

97. *Id.* at 312–13.

98. *Id.* at 85 (rule 15(7)).

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

100. TALLINN MANUAL 2.0, *supra* note 62, at 317 (rule 66(18)).

101. Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 FLETCHER SECURITY REVIEW 53, 60 (2014).

Defining the range of cyber conduct that qualifies as "coercion" has been more difficult. The International Group of Experts (IGE) that provided the analysis in *Tallinn 2.0* could only agree on the anodyne statement "that as a general matter, States must act as reasonable States would in the same or similar circumstances when considering responses to them."[102]

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."[103] The *Tallinn 2.0* experts similarly suggested that remotely altering electronic ballots to manipulate election results constitutes unlawful intervention.[104]

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. It concluded that military cyber activities that fall below the use of force threshold and do not violate the non-intervention principle are "largely unregulated by international law at this time."[105]

We should remain cautious about this coercion analysis, however, because State practice and resulting customary international law is based on examples from kinetic conflicts. The analogies to cyber are not necessarily conclusive. Consider Russian election interference in 2016. If we extrapolate from General Michael Hayden's metaphor that the Russians effectively "weaponized"[106] 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

---

102. TALLINN MANUAL 2.0, *supra* note 62, at 81.

103. Brian J. Egan, Legal Adviser, U.S. Department of State, Remarks at Berkeley Law School, California: International Law and Stability in Cyberspace (Nov. 10, 2016), *reprinted in* Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY JOURNAL OF INTERNATIONAL LAW 169, 178 (2017).

104 TALLINN MANUAL 2.0, *supra* note 62, at 313.

105. Memorandum from Jennifer M. O'Connor, General Counsel, U.S. Department of Defense, International Law Framework for Employing Cyber Capabilities in Military Operations, to Commanders of the Combatant Commands et al. (Jan. 19, 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.*

106. Nicole Gaouette, *Ex-CIA Chief: Russian Hackers Trying to 'Mess with our Heads*,' CNN (Oct. 18, 2016), https://www.cnn.com/2016/10/18/politics/hayden-russia-us-cyber-elections/index.html.

attributed State responsibility for the attacks. An official attribution did not occur until January 2017, two months after the election.

The OPM hack, for example, may have severely undermined U.S. national security at a scale not seen previously. Yet, from the perspective of international law, the OPM hack was an act of espionage, which international law either fails to regulate or affirmatively permits. As such, it is not surprising to see accusations against China avoid condemnation for the OPM hack in international legal terms.[107]

VII. DEVELOPING EVIDENCE FOR ATTRIBUTION AND VICTIM STATE RESPONSES

An attribution of a cyberattack can lead to significant consequences for the perpetrator State. If a State is victimized by an internationally wrongful act below the use of force threshold, the victim State may be entitled to take countermeasures.[108] Brian Egan, in his 2016 speech, stated that "the availability of countermeasures to address malicious cyber activity requires a prior internationally wrongful act that is attributable to another state,"[109] while U.K. attorney general Jeremy Wright added that in carrying out countermeasures, "the victim state must be confident in its attribution of that act to a hostile state before it takes action in response."[110] Countermeasures are victim State responses that otherwise would violate international law and are designed to prevent a responsible State from continuing its unlawful cyber intervention.[111] Countermeasures require prior notice to the offending State, and they must have as their purpose inducing compliance with international law.[112] Punitive countermeasures are forbidden.[113]

A significant impediment to successful cybersecurity law and policy in international law is that no evidentiary standard for proof of attribution of

107. *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VIRGINIA JOURNAL OF INTERNATIONAL LAW 291, 300 (2015).

108. *See* Ashley Deeks, *Defend Forward and Cyber Countermeasures* (Aegis Series Paper No. 2004, 2020), https://www.law.virginia.edu/system/files/faculty/Defend-Forward-Cyber-Countermeasures.pdf.

109. Egan, *supra* note 103.

110. Wright, *supra* note 92

111. The most authoritative articulation of countermeasures is the International Law Commission's 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts. *See* Int'l Law Comm'n, *supra* note 27.

112. TALLINN MANUAL 2.0, *supra* note 62, at 112.

113. *Id.* at 124.

cyberattacks has been established or agreed upon by States.[114] The ILC Articles on State Responsibility declined to address matters of evidence and proof of international law violations.[115] The ICJ has contributed only by suggesting that such standards vary depending on the severity of the offense.[116] The complexities of cyber attribution and the risks of misattribution argue for a high burden of proof. Kristen Eichensehr has argued that the sliding scale of evidence based on the severity of the cyberattack and anticipated response, as justified by the ICJ and the *Tallinn Manual 2.0*, is helpful only at the extremes of the scale—a cyber armed attack.[117]

For the vast majority of cyberattacks—those that could trigger countermeasures and lesser intrusions below the use of force threshold—Eichensehr argues that a minimum standard of *some* evidence may serve important purposes of promoting stability and avoiding conflict in the cyber domain.[118] She persuasively maintains that "providing sufficient technical details to all other potential attributors . . . to confirm (or debunk) an attribution will bolster the attribution's credibility."[119] Requiring that attributors "show their work" should lead to more careful and better attributions, too.[120] Eichensehr concludes that "*all* governmental attributions should provide sufficient evidence to allow other governmental and nongovernmental actors to confirm or debunk the attributions."[121]

States engaged in countermeasures following a cyberattack bear the burden of attributing the attack they wish to counter to the responsible State.[122] In other words, the victim State must persuade other interested States that it was victimized by an internationally wrongful act. The evidence described above would accomplish that task. The *Tallinn Manual 2.0* 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 . . . because the robustness of permissible self-help responses . . .

---

114. *See* Eichensehr, *supra* note 38, at 559–86 (discussing this matter in depth and suggesting a standard.).

115. Int'l Law Comm'n, *supra* note 27, at 72.

116. *See* Eichensehr, *supra* note 38, at 562 (*citing* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, 130, ¶ 210 (Feb. 26)).

117. *Id.* at 577.

118. *Id.* at 578.

119. *Id.*

120. *Id.*

121. *Id.* at 583.

122. Deeks, *supra* note 108, at 6.

grows commensurately with the seriousness of the breach."[123] However, according to the IGE, the severity of the cyber intrusion directed at an injured State is also relevant, so that 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."[124]

In a similar vein, the time it takes to produce a high confidence attribution judgment can limit the lawful responses to cyber operations. Mistaken attribution can lead to an unlawful response even if the State made a reasonable attribution judgment and implemented countermeasures.[125] If a State victimized by an internationally wrongful cyber intrusion engages in countermeasures and ends up being wrong about State attribution, the victimized State has committed an internationally wrongful act.[126] On the other hand, if the victim State waits until it has high confidence in its attribution of a State's responsibility for the intrusion, any countermeasures may be construed as punishment, a form of reprisal forbidden under international law.[127] As a result, cyber deterrence may be undermined because the legally less risky but weak self-help retorsion responses to an intrusion are unlikely to deter similar cyber intrusions in the future.

Nor is the failure of a State to provide persuasive proof of attribution itself an internationally wrongful act. The 2015 United Nations Group of Governmental Experts report noted that accusations of wrongful acts by States "should be substantiated,"[128] but the group gave no indication of which or how much evidence would suffice or even count. The U.S. view, as articulated by Brian Egan's 2016 speech, 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

123. TALLINN MANUAL 2.0, *supra* note 62, at 82. In support of its position, the IGE cited Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 33 (Nov. 6) (separate opinion of Higgins, J.); Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 17 (Apr. 9); Application of the Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶¶ 209–10 (Feb. 26); Application of Convention on Prevention and Punishment of Crime of Genocide (Croat. v. Serb.), 2015 I.C.J. 3, ¶ 178 (Feb. 3).

124. TALLINN MANUAL 2.0, *supra* note 62, at 82.

125. *Id.* at 82–83.

126. *Id.* at 118–20.

127. *Id.* at 116.

128. 2015 GGE Report, *supra* note 71, ¶ 24.

to taking appropriate action."[129] Thus, even when legally required, attribution need not be made public.[130]

States are likewise not obligated to provide evidence of attribution when responding to another State's cyber intrusions.[131] While the IGE acknowledged the value in such a disclosure requirement, it found insufficient State practice and *opinio juris* to recognize "an established basis under international law for such an obligation."[132] 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.[133] Fear of reckless or spurious accusations is also widespread and, indeed, among the norms agreed to by the 2015 UN Group of Government Experts was the following: "accusations of organizing and implementing wrongful acts brought against States should be substantiated."[134]

Although attribution is necessarily probabilistic, the process serves its purpose if it convinces the responsible State (and victim State's citizens) that a response to the cyber intrusion is called for.[135] 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 with more information.[136] Continuing investigation may reveal additional useful information, which may (or may not) reinforce attribution judgments made earlier.[137] Over time, an international consensus may develop on the minimum level of involvement needed to declare that a State is legally responsible for a cyberattack.

Legally enforceable attribution proof requirements could be imposed only on States that have been victimized by an internationally wrongful act. Short of countermeasures, victim States may respond to cyber intrusions through retorsions, acts that are "unfriendly" but lawful.[138] Examples include

---

129. Egan, *supra* note 103.

130. *See* Eichensehr*, supra* note 38, at 556 (confirming that attribution by victim States can be private, though acknowledging associated risks).

131. TALLINN MANUAL 2.0, *supra* note 62, at 83.

132. *Id.*

133. *Id.*

134. 2015 GGE Report, *supra* note 71, ¶ 28(f).

135. CLEMENT GUITTON, INSIDE THE ENEMY'S COMPUTER: IDENTIFYING CYBER ATTACKERS 66 (2017).

136. *Id.* at 151–62.

137. *Id.*

138. Int'l Law Comm'n, *supra* note 27, chapeau to ch. II of pt. 3, cmt. ¶ 3.

diplomatic protests, denying access to State resources, and economic sanctions.[139]

VIII. CONCLUSIONS

An attribution may be celebrated by some and condemned by others. The OPM hack was assailed in the United States as a significant breach of national security, but Director of National Intelligence James Clapper acknowledged that the Chinese behavior was acceptable among States.[140] Clapper also opined that the United States would have done the same thing if it could. So the efficacy of attribution depends on its purpose, context, and audience.

Public attribution of attacks in the cyber domain has long been thought to further deterrence—the exposed attackers will refrain from future attacks.[141] Deterrence through attribution has a poor record, however.[142] Yet even where a public attribution does not stop cyberattacks by a perpetrator State, it may enable victim States to improve their cyber defenses and thus

139. Thomas Giegerich, *Retorsion*, MAX PLANCK ENCYCLOPEDIAS OF PUBLIC INTERNATIONAL LAW (updated Sept. 2020), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983?rskey=gdXVnW&result=1&prd=MPIL.

140. *See* Jim Sciutto, *Director of National Intelligence Blames China for OPM Hack*, CNN (June 25, 2015), https://www.cnn.com/2015/06/25/politics/james-clapper-china-opm-hacking/index.html (quoting James Clapper as stating "[y]ou have to kind of salute the Chinese for what they did").

141. *See generally* Joseph S. Nye, Jr., *Deterrence and Dissuasion in Cyberspace*, 41 INTERNATIONAL SECURITY 44, 45 (2017) ("Deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."); *see also, e.g.*, Chimène I. Keitner, *Attribution by Indictment,* 113 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 207, 210 (2019) (identifying the goal of deterrence as one purpose of U.S. attributions-by-indictment).

142. Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASHINGTON 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-b5e4279b4501e8a6_story.html (quoting U.S. government sources); *see also* Rid & Buchanan, *supra* note 28, at 29 (observing that following Mandiant's APT1 report, China's hacking activity "first stopped for 41 days, then remained at lower-than-normal levels until nearly 160 days after exposure").

deter future attacks.[143] Public attribution also builds a record that may help legitimate cyber responses by the victim State.[144]

Because of the harm that States and their citizens continue to suffer as a result of cyberattacks, States should agree to make some difficult tradeoffs between secrecy and transparency and publicly identify some public infrastructure "red lines" and attribution benchmarks that can help create an international law roadmap for deterrence of harmful cyber intrusions.

As cyber international relations now stand, a few States 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. However, in general, those States are also the most vulnerable to cyber intrusions. Meanwhile, the disparity between States that are strong and weak at attribution results in the equivalent of an arms race between advances in detection versus detection evasion. Evasion is getting easier faster, so States that do not have advanced attribution capabilities can reliably invest in hiding themselves.[145]

As the most advanced cyber States recognize the risks of cyber escalation, those States have good reason to become more transparent about attribution in service of the mutual restraint that could be gained by sharing attribution information. But to date, State concerns about revealing intelligence sources and methods counsel against transparency.[146] However, "[u]nless a nation is able to effectively redress a cyber intrusion, it can be harmful or self-defeating to publicize it, since public knowledge of loss and the failure to respond effectively invite more attacks."[147]

---

143. *See, e.g.*, Martin C. Libicki, *Cyberdeterrence and Cyberwar* 7 (2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf ("If deterrence is anything that dissuades an attack, it is usually said to have two components: deterrence by denial (the ability to frustrate the attacks) and deterrence by punishment (the threat of retaliation)."); Nye, *supra* note 141, at 54 ("Classical deterrence theory rested primarily on two main mechanisms: a credible threat of punishment for an action; and denial of gains from an action.").

144. *See* Int'l Law Comm'n, *supra* note 27, art. 22 ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State . . . .").

145. BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD 54–55 (2018).

146. *Id.* at 54.

147. Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations* 3 (Aegis Series Paper No. 1806, 2018),

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 *Tallinn Manual* IGE concluded that "States may agree between themselves to a rule of responsibility specific to a cyber act or practice."[148] The result would be *lex specialis* to the extent the rule conflicts directly with general principles of State responsibility.[149]

States could also work collectively toward cyber attributions. In September 2019, twenty-seven States issued a "Joint Statement" that contemplated a set of unspecified collective actions with an aim to advance responsible state behavior in cyberspace.[150] In recent years, cyberattacks including WannaCry, NotPetya, and the Organization for the Prohibition of Nuclear Weapons hack illustrate that collective attributions might enhance the credibility of the claims made.[151] Over time a series of collective attributions could constitute a general practice that could be accepted as *opinion juris*.

Alternatively, the creation of an international institution to impartially attribute cyberattacks or advocate for the application of international law to address such attacks might allow States to advance the power of accusations.[152] Such an institution could collect attribution data from State and non-

---

https://www.hoover.org/sites/default/files/research/docs/381100534-strengths-become-vulnerabilities.pdf.

148. TALLINN MANUAL 2.0, *supra* note 62, at 80.

149. As per the traditional legal maxim "specific law prevails over general law." *See* Generalia Specialibus Non Derogant, BLACK'S LAW DICTIONARY (11th ed. 2014) ("The doctrine holding that general words in a later statute do not repeal an earlier statutory provision dealing with a special subject."); TALLINN MANUAL 2.0, *supra* note 62, at 81.

150. *See* Other Release, Joint Statement on Advancing Responsible State Behavior in Cyberspace*,* U.S. DEPARTMENT OF STATE (Sept. 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/ ("When necessary, we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law.").

151. *See, e.g.,* Roguski, *supra* note 4 (in February 2020, twenty States collectively accused Russia of conducting cyber operations against Georgia); *Russia Cyber-Plots: US, UK and Netherlands Allege Hacking*, BBC (Oct. 4, 2018), https://www.bbc.com/news/world-europe-45746837 (noting organized accusations by Canadian, Dutch, U.S., and U.K. officials against the GRU).

152. The CyberPeace Institute is a novel non-profit organization recently established in Geneva with a mission of "assistance, accountability, and advancement" to "enhance the stability of cyber space" by collaboratively analyzing cyberattacks by assisting victims whose digital security systems are deficient, coordinating resources to assign accountability, and

State actors reluctant to share it publicly.[153] This avenue has the potential to provide integrity to the currently muddled series of accusations and counter-accusations that typically characterize the aftermath of cyberattacks. Such an entity could supplement the currently disaggregated attribution efforts, while providing the opportunity to strengthen and perhaps eventually supplant them.[154] Further, such an organization could build and concentrate technical expertise that would be of particular benefit to States that lack the capacity to adequately attribute, broadening participation in the creation of new international norms. In essence, credible reports of attribution by neutral actors could act as a catalyst for States to coalesce around new international legal rules proscribing the sort of cyberattacks that currently evade meaningful repercussions.

In practice, attribution of cyberattacks in the United States is determined if and when the Secretary of the Treasury decides, in consultation with other officials, to freeze the foreign actor's U.S.-based assets. Proposals for improving U.S. attribution processes include centralizing the attribution function in a single agency—likely NSA[155]—although the secrecy of NSA and its firm anchor in the U.S. government limits the attractiveness of that idea. Other proposals would create a National Cyber Safety Board,[156] an attribution organization somewhere in the U.S. government. Such a model has

---

advocating for the exposure and bridging of legal and normative gaps in international law. To date, however, it is not clear that the institute is likely to make accusations on its own. *See* CYBERPEACE INSTITUTE, https://cyberpeaceinstitute.org/ (last visited July 13, 2021).

153. *See, e.g.,* Davis II et al., *supra* note 3, at 3; JASON HEALEY ET AL., ATLANTIC COUNCIL, CONFIDENCE-BUILDING MEASURES IN CYBERSPACE (2014), https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf; Brad Smith, President, Microsoft Corporation, Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention, MICROSOFT (Feb. 24, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

154. *See, e.g.*, Kristin E. Eichensehr, *Decentralized Cyberattack Attribution,* 113 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 213 (2019). For Eichensehr's argument that decentralized attribution should continue, see Eichensehr, *supra* note 38.

155. Glenn S. Gerstell, NSA General Counsel, Speech: How We Need to Prepare for a Global Cyber Pandemic, NSA|CSS (Apr. 9, 2018), https://www.nsa.gov/news-features/speeches-testimonies/Article/1611673/how-we-need-to-prepare-for-a-global-cyber-pandemic/.

156. Paul Rosenzweig, *The NTSB as a Model for Cybersecurity*, R STREET (May 9, 2018), https://www.rstreet.org/2018/05/09/the-ntsb-as-a-model-for-cybersecurity/.

promise inside the United States, but a domestic process does not get at the international dimensions—where the problems are.