THE LAW & POLITICS OF CYBERATTACK ATTRIBUTION

67 UCLA L. REV. __ (forthcoming 2020).

Kristen E. Eichensehr*

Attribution of cyberattacks requires identifying those responsible for bad acts, prominently including states, and accurate attribution is a crucial predicate in contexts as diverse as criminal indictments, insurance coverage disputes, and cyberwar. But the difficult technical side of attribution is just the precursor to highly contested legal and policy questions about when and how to accuse governments of responsibility for cyberattacks. Although politics may largely determine whether attributions are made public, this Article argues that when cyberattacks are publicly attributed to states, such attributions should be governed by legal standards. Instead of blocking the development of evidentiary standards for attribution, as the United States, United Kingdom, and France are currently doing, states should establish an international law requirement that public attributions must include sufficient evidence to enable cross-checking or corroboration of the accusations. This functionally defined standard harnesses both governmental and non-governmental attribution capabilities to shed light on states' actions in cyberspace, and understanding state practice is a necessary precondition to establishing norms and customary international law to govern state behavior. Moreover, setting a clear evidentiary standard for attribution in the cybersecurity context has the potential to clarify currently unsettled general international law on evidentiary rules. The Article also engages debates about institutional design for cyberattack attribution. Companies and think tanks have made several recent proposals for an international entity to handle attribution of state-sponsored cyberattacks. Although these proposals have much to recommend them, the Article argues that such an entity should supplement, not replace, the current decentralized system of attribution. Having a multiplicity of attributors—both governmental and non-governmental—yields a greater likelihood that public attributions will serve the goals that attributors aim to achieve, namely strengthening defenses, deterring further attacks, and improving stability in and avoiding conflict over cyberspace.

* Assistant Professor, UCLA School of Law. For helpful comments and conversations, thanks to Asli Bâli, Bill Banks, Ben Boudreaux, Beth Colgan, Stephen Gardbaum, Andy Grotto, Oona Hathaway, Duncan Hollis, Eric Jensen, Chimène Keitner, Máximo Langer, Susan Landau, Jon Michaels, Kal Raustiala, Richard Re, Michael Sulmeyer, David Thaw, and Eugene Volokh and to participants in workshops at the Duke-Virginia Foreign Relations Law Roundtable, Privacy Law Scholars Conference, UCLA School of Law, and Yale Law School Information Society Project. Thanks to Ariel Cohen and Kimberly Turner for excellent research assistance.

INTRODUCTION

Figuring out who's doing what to whom and publicly identifying those responsible for bad acts in cyberspace are key features of increasing efforts to hold those actors more accountable. Cyberattack attribution is the process of assigning responsibility for carrying out a cyberattack.[1] Accurate attribution of cyberattacks is a crucial predicate to a wide range of related or responsive actions; in particular, attribution *to a state* can set in motion different legal consequences. Criminal indictments are one example: in the United States, a criminal charge of economic espionage requires the involvement of a foreign government.[2] Another is insurance coverage.[3] Invoking an exclusion for cyberwar, insurance companies have denied claims made by companies that suffered hundreds of millions of dollars of damage in a cyberattack called NotPetya, which the United States and its allies have attributed

[1] Some use the terms "computer network exploitation" and "computer network attack" to denote intrusions aimed at spying and damaging or disruptive intrusions respectively, but the line between categories blurs in practice. *See, e.g.*, Bruce Schneier, *There's No Real Difference Between Online Espionage and Online Attack*, ATLANTIC, Mar. 6, 2014, https://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/; Kim Zetter, *Hacker Lexicon: What Are CNE and CNA?*, WIRED, July 6, 2016, https://www.wired.com/2016/07/hacker-lexicon-cne-cna/. I therefore use "cyberattack" throughout the Article in the colloquial sense as an umbrella term for malicious computer or network intrusions. Unless otherwise noted, the term is not meant to indicate that an intrusion is an "attack" for purposes of the international law governing the use of force.

[2] *See* 18 U.S.C. § 1831 (defining economic espionage to require theft of a trade secret with the perpetrator "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent").

[3] Yet another context where attribution may matter is cases where individuals sue for harm caused by data breaches. Judges have made assumptions about the identity of hackers—specifically that they are criminals intent on committing fraud—in assessing the risk of harm to plaintiffs for purposes of establishing the injury in fact required for standing. *See, e.g.*, Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) (finding a "substantial risk of harm" sufficient for standing because "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"). For data breaches attributed to government actors, however, judges' views about the likelihood or nature of potential harm might change. This issue recently came before the D.C. Circuit in a case involving the 2015 Office of Personnel Management hack, which a security firm has attributed to China. *See infra* note 125 and accompanying text. Despite the possible espionage-related motives for the breach, the D.C. Circuit held that the plaintiffs' risk of identity theft was sufficient for standing. In Re: U.S. Office of Personnel Management Data Security Breach Litig., 928 F.3d 42, 56-58 (D.C. Cir. 2019). In dissent, Judge Stephen Williams disagreed, discounting the likelihood of identity theft and calling the breach more likely "the handiwork of foreign spies looking to harvest information about millions of federal workers for espionage or kindred purposes having nothing to do with identity theft." *Id.* at 76 (Williams, J., concurring in part and dissenting in part). The court rejected the government's petition for rehearing en banc. *See* Order, In Re: U.S. Office of Personnel Management Data Security Breach Litig., *supra* (Nos. 17-5217 & 17-5232) (D.C. Cir. Oct. 21, 2019) (denying petitions for rehearing en banc).

to the Russian military.[4] Still other important examples involve cyber-based responses, ranging from taking foreign government-linked cyber infrastructure offline[5] to even forcible self-defense in response to an armed attack.

Cyberattack attribution has technical, legal, and political aspects.[6] The technical side of such attribution—identifying the source of a cyberattack at the machine or internet protocol address level—has improved substantially over the last few years. But attributing cyberattacks to individual perpetrators and especially to states that direct the attacks remains complicated because it involves unsettled legal and political issues. Questions about who should accuse governments of cyberattacks and when and how to make such accusations remain highly contested. These questions are becoming more urgent as the need for accurate attribution of cyberattacks spreads to more contexts.

Now nearly ten years after Stuxnet targeted Iranian nuclear centrifuges,[7] scholars and states have devoted significant attention to how the primary rules of international law should govern state behavior in cyberspace.[8] But legal issues surrounding attribution of state-sponsored cyberattacks have received comparatively little attention.[9] A major reason for this differential treatment may be the status of the

---

[4] *See* Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong*, N.Y. TIMES, Apr. 15, 2019, https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html (detailing ongoing litigation between insurance companies and claimants Mondelez International and Merck over damage from NotPetya); *see also* White House, Statement from the Press Secretary, Feb. 15, 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (attributing NotPetya to the Russian military).

[5] *See, e.g.*, Julian E. Barnes & Thomas Gibbons-Neff, *U.S. Carried Out Cyberattacks on Iran*, N.Y. TIMES, June 22, 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html (describing U.S. cyber operations targeting Iranian missile launch systems and an Iranian intelligence unit involved in mine attacks on tankers); Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST, Feb. 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html (describing Cyber Command operation against the Internet Research Agency, which "U.S. officials have . . . assessed . . . works on behalf of the Kremlin").

[6] *See infra* notes 20-27 and accompanying text.

[7] *See, e.g.*, David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (discussing the Stuxnet attacks against Iranian nuclear facilities).

[8] *See infra* notes 219-220 and accompanying text (discussing the difference between primary and secondary rules). For examples of literature on rules of state behavior in cyberspace, see, for example, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt gen. ed., 2017); Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEX. L. REV. SEE ALSO 145 (2017); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011).

[9] *See, e.g.*, William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 TEX. L. REV. 1487, 1493 (2017) (highlighting the "substantially underdeveloped customary

relevant non-cyber-specific international law. On questions about the primary rules of international law, such as what counts as an armed attack and how to apply the principle of proportionality, international law is well-settled and can be applied, with some modifications, to cyberattacks.[10] Attributing responsibility for cyberattacks to states, on the other hand, intersects with secondary international law rules regarding the evidence states must provide when accusing other states of internationally wrongful acts—an area of law that is notoriously underdeveloped even outside the cybersecurity context.[11] This results in a double challenge for those deciding how much and what kind of evidence to disclose to support a cyberattack attribution: simply borrowing *lex generalis* from the non-cyberspace context is hard to do, and *lex specialis* governing evidence for cyberattack attribution has not yet crystallized.[12] At the same time, the lack of existing standards presents an opportunity. Setting clear

---

international law on attribution of cyber operations"). One of the best treatments of the relationship between attributions and international law is a draft piece by Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347958 (draft of Mar. 6, 2019). Like this Article, Finnemore and Hollis make the point that public attributions (which they call "accusations") can contribute to the formation of international law about state behavior in cyberspace. *Id.* at 5. They do not, however, focus on setting an evidentiary standard for attributions, as this Article does, and instead flag the issue as one for future development. *Cf. id.* at 16 ("As accusations of cyber operations become more common, we expect demands for documentation to rise, along with efforts to normalize how much substantiation should accompany an accusation.").

[10] Of course, some modifications are necessary. *See, e.g.*, Kristen E. Eichensehr, *Cyberwar & International Law Step Zero*, 50 TEX. INT'L L.J. 357, 375-79 (2015) (discussing areas where cyber-specific law of war rules may be needed).

[11] *See, e.g.*, James A. Green, *Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice*, 58 INT'L & COMP. L.Q. 163, 164 (2009) ("One of the most pressing and fundamentally overlooked questions relating to the international legal regulation of self-defence is the standard of evidence to be applied in assessing the lawfulness of such a claim."); Jules Lobel, *The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan*, 24 YALE J. INT'L L. 537, 538 (1999) ("Questions involving the standards and mechanisms for assessing complicated factual inquiries are generally not accorded the same treatment given by the legal academy to the more abstract issues involved in defining relevant international law standards."); Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, 50 TEX. INT'L L.J. 233, 242 (2015) (noting that cyberattack investigations "are complicated by the absence of a uniform body of rules on the production of evidence in international law"). In contrast to this Article's focus on international law evidentiary standards in general and their relationship to domestic law standards, Roscini focuses narrowly on the evidentiary standards for "inter-state judicial proceedings seeking remedies for damage caused by cyber operations" and the International Court of Justice in particular. *Id.* at 242-43.

[12] The principle that the specific prevails over the general is common among legal systems and well-established as a matter of international law. *See, e.g.*, Int'l Law Comm'n, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, U.N. Doc. No. A/CN.4/L.682, at 36 (2006), *available at* http://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf (explaining that "[t]he idea that special enjoys priority over general has a long pedigree in international jurisprudence," citing Grotius); John F. Manning, *Separation of Powers as Ordinary Interpretation*, 124 HARV. L. REV. 1939, 2012 (2011) (referring to the "deeply rooted . . . 'specificity maxim,'" which "holds, quite simply, that 'the specific governs the general'").

evidentiary standards for states to follow in the cyberattack attribution context could help to clarify the evidentiary standards in international law more generally and to regularize the attributions made by non-governmental actors as well.

As both cyberattacks and cyberattack attributions increase in frequency,[13] it is important to understand who attributes, how, and why and to examine which answers to those questions will best further the goals that attribution is intended to serve. Attributors may intend attributions to deter further attacks by changing states' behavior, deter individual hackers within states, enable better network defenses, or serve as a legal prerequisite to responsive actions. Done carefully and transparently, public attributions can also further broader goals of promoting stability and avoiding conflict in and over cyberspace.

This Article provides the first comprehensive account of states' emerging practice of issuing coordinated cyberattack attributions and explores three themes regarding how cyberattacks are attributed to states.

First is the interrelationship between law and politics. Although the United States, United Kingdom, and most recently France have taken the position that publicly attributing state-sponsored cyberattacks is a political decision, not a legal one, the issue is more complicated. The decision to attribute *publicly* is partly political: a state could suffer a cyberattack, have extensive evidence identifying the perpetrator, and still say nothing publicly. But when a state chooses to make a public attribution against another state, it should substantiate the accusation, and in doing so, international law has a role to play. Evidentiary issues have legal underpinnings, and the U.S., U.K., and French efforts to block the development of customary international law on attribution are short-sighted.[14] Although existing international law does not set clear evidentiary requirements for how to make attributions, establishing an international law standard would have significant benefits in the cybersecurity context. And setting *lex specialis* for cyberattack attribution could spur clarification of other evidentiary standards in international law.

The second and related theme is the relationship between domestic and international law. If attributions are to be governed by law, the applicable law could be either domestic or international. Currently, domestic law, particularly in the United States, is doing some of the work to fill gaps in standards left by underdeveloped international law.[15] But although domestic law is a helpful stopgap, it will be insufficient in the longer term, making the development of international law on attributions increasingly important.[16] In some cases, where attribution mechanisms governed by domestic law, such as indictments and economic sanctions, are used to accuse governments of cyberattacks, international law may require states

[13] For the most comprehensive attempt to track cyberattacks attributed to states, see Council on Foreign Relations, Cyber Operations Tracker, https://www.cfr.org/interactive/cyber-operations (last visited Sept. 12, 2019) (collecting "publicly known state-sponsored incidents that have occurred since 2005").

[14] *See infra* Section II.B.i.

[15] *See infra* notes 224-229 and accompanying text.

[16] *See infra* notes 230-236 and accompanying text.

to meet a standard higher than the domestic law floor of probable cause or substantial evidence required to satisfy constitutional due process.[17]

The third and final theme relates to issues of institutional design.[18] To date, governments, companies, academic institutes, and non-profits have all attributed cyberattacks to state-sponsored actors. Despite some recent examples of coordinated attributions, the current attribution "system," such as it is, is messy and decentralized. Going forward, the optimal structure for attribution of cyberattacks depends on the purpose or purposes attribution is intended to serve—deterring future bad acts, enabling defense, laying the foundation for responsive actions, or promoting stability and avoiding conflict.

The Article proceeds in three parts. Part I first provides an overview of the practice of governmental and non-governmental parties in publicly attributing cyberattacks to states and then evaluates the purposes public attributions may serve. Part II turns to the law of attribution. After examining the underdeveloped state of existing international law on evidentiary standards for attribution both in general and in the cyberattack context, the Article argues for the importance of developing international law on evidentiary standards to govern cyberattack attribution in particular. Specifically, the Article proposes that international law should require governments that engage in public attributions of cyberattacks to other states to provide enough evidence to enable cross-checking or corroboration of their attributions. Part III turns to issues of institutional design. Companies and think tanks have made several proposals for an international entity to handle attribution of state-sponsored cyberattacks. Although these proposals have much to recommend them, the Article argues that such an entity should supplement, not replace, the current decentralized system of attribution. Having a multiplicity of attributors—both governmental and non-governmental—yields a greater likelihood that public attributions will serve the defensive and deterrent purposes attributors aim to achieve. And having an evidentiary standard to govern attributions, as this Article proposes, creates an alternative to centralization for ensuring the credibility of attributions.

I. THE PRACTICE & PURPOSES OF ATTRIBUTION

"Attribution" has multiple meanings relevant to cybersecurity. At the most general level, "attribution" refers to identifying the entity responsible for a cyberattack or intrusion. But what is meant by the responsible entity can vary. Scholars often speak in terms of three types of answers: the machine from which an attack was launched, the individual sitting behind the machine and carrying out an attack, and the individual or entity that directed the attack.[19] As Herb Lin has

[17] *See infra* text accompanying note 236.

[18] *See infra* Part III.

[19] *See, e.g.*, Herbert Lin, *Attribution of Malicious Cyber Incidents*, Hoover Institute Aegis Paper Series No. 1607, at 5 https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf

explained, "these three types of attribution are conceptually distinct," but "often related in practice."[20] In particular, "[k]nowing the machine from which the intrusion initially emanated may provide some clues that can help uncover the identity of the human perpetrator, and knowing the human perpetrator may provide some clues that can help identify the party ultimately responsible for setting the entire intrusion into motion."[21]

Nonetheless, the different types of attribution pose different sorts of challenges. Identifying the machine from which an attack was launched is largely a technical question.[22] When malicious activity is discovered, investigators consider indicators of compromise, such as internet protocol addresses, domain names, hashes of programs running on compromised computers, and styles of attack used in the intrusion.[23] The infrastructure and software used in an attack can also provide clues because hackers often reuse the same infrastructure and code in different attacks.[24] Other information, like the hackers' apparent work schedules, use of a words in a particular language, or language settings on computers used to write malware can yield circumstantial evidence about the hackers' identity,[25] but can be faked relatively easily in a false flag operation—a deliberate attempt by hackers to disguise their identity.[26]

("[T]he question of 'who is responsible?' can be answered in three ways, which are not mutually exclusive. The possible types of answers are a machine, a specific human being pressing the keys or otherwise setting the intrusion into motion, and an ultimately responsible party."); Nicholas Tsagourias, *Cyber Attacks, Self-Defense and the Problem of Attribution*, 17 J. OF CONFLICT & SEC'Y L. 229, 233 (2012) ("What is critical, then, is not only to trace back the attack to its source, for example to a computer, but to identify the person who operated the computer, and more importantly to identify the real 'mastermind' behind the attack . . . .").

[20] Lin, *supra* note 19, at 12-13.

[21] *Id.*

[22] For excellent overviews of the technical aspects of attribution, see JOHN S. DAVIS II ET AL., STATELESS ATTRIBUTION: TOWARD INTERNATIONAL ACCOUNTABILITY IN CYBERSPACE 9-16 (2017), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2081/RAND_RR2081.pdf; Lin, *supra* note 19. at 5-9; and Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRAT. STUD. 4, 14-23 (2015).

[23] Rid & Buchanan, *supra* note 22, at 15 (describing "atomic, behavioral, and computed" indicators of compromise).

[24] *See id.* at 17-18 (discussing reuse of infrastructure and software as means of attributing attacks).

[25] *See id.* at 19; *see also* Lin, *supra* note 19, at 13 (noting that the "language setting for the keyboard of a particular computer . . . is suggestive and raises the likelihood that the human perpetrator is from a nation in which the language is used").

[26] *See, e.g.*, Rid & Buchanan, *supra* note 22, at 19 (discussing potential use of language indicators in false flag operations). The best-known example of a false flag operation is a 2015 attack on a French television station, TV5Monde. A group claiming to be the "Cyber Caliphate" took credit and posted pro-Islamic State propaganda on the station's social media accounts, but the attack was later attributed to Russia. *See* DAVIS II ET AL., *supra* note 22, at 13; *see also* Gordon Corera, *How France's TV5 Was Almost Destroyed by Russian Hackers*, BBC, Oct. 10, 2016, https://www.bbc.com/news/technology-37590375 (discussing the attack and attribution to Russia).

Moving beyond technical attribution to a machine, identifying the entity that directed or masterminded the attack implicates political and legal considerations. When the entity that directs a cyberattack is a state, the international law on state responsibility governs the extent to which a state can be held legally responsible, and it uses "attribution" to mean "the operation of attaching a given action or omission to a State."[27]

While technical attribution capabilities have improved dramatically in recent years, the political and legal issues surrounding ultimate attribution to state actors remain unsettled and contested. Sections I.A and I.B track the evolution of attribution practice of states and non-governmental parties respectively, emphasizing both shifts in the capacities for technical attribution and emerging policy and legal positions. Section I.C then identifies several purposes that attribution can serve.

The following sections focus heavily, but not exclusively, on the United States, the United Kingdom, and France, as well as on U.S. companies and a Canadian research institute. This focus reflects the entities that have engaged in public attributions to date or publicly addressed the legal issues surrounding attribution. Other entities' views are discussed to the more limited extent they are publicly available. These include governments, like Australia, Canada, Japan, the Netherlands, and New Zealand, which have participated in coordinated attributions with the United States and United Kingdom, as well as countries like China and Russia, which have been on the receiving end of public attributions and have also communicated some views about evidence and attribution in multilateral fora. If this Article's prescriptions are taken up by governmental and non-governmental attributors, then a greater diversity of views may become publicly available going forward.

A. The Practice of States

The practice of states publicly attributing cyberattacks to other states is a recent phenomenon.[28] The first public accusation by the U.S. government came in

[27] Int'l Law Comm'n, Articles on Responsibility of States for Internationally Wrongful Acts 36 (para. 12) (2001), *available at* http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

[28] Russia is widely believed to have been responsible for distributed denial of service (DDOS) attacks on Estonia in 2007. After initially appearing to accuse the Russian government based on tracing some of the attacks to "servers of Russian state authorities," Prime Minister Andrus Ansip's Speech in Riigikogu, May 2, 2007, https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu, an Estonian official later stated that while Russian governmental offices' IP addresses were involved in the attacks, "'[t]here is not sufficient evidence of a governmental role, but it indicates a possibility.'" *Estonian Links Moscow to Internet Attack*, ASSOC. PRESS, May 18, 2007, https://www.nytimes.com/2007/05/18/world/europe/18estonia.html (quoting Estonian defense minister Jaak Aaviksoo); *see also* Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC, Apr. 27, 2017, https://www.bbc.com/news/39655415 (reporting that "on condition of anonymity," an Estonian government official "suggested the attack 'was orchestrated by the Kremlin, and malicious gangs then seized the opportunity to join in"). Georgian officials have similarly

2014, when the United States accused five members of the Chinese People's Liberation Army (PLA) of hacking into U.S. companies to steal intellectual property.[29] Attributions were almost exclusively a U.S. phenomenon until 2017,[30] when state-to-state attributions increased significantly.[31]

The move to publicly attribute cyberattacks to governments first required improvements in the technical capacity for attribution.[32] In a 2010 *Foreign Affairs* article, then-Deputy Secretary of Defense William Lynn signaled the difficulty of attributing cyberattacks, writing that "[t]he forensic work necessary to identify an attack may take months, if identification is possible at all."[33] Scholars at the time echoed the idea that attribution was difficult, if not impossible.[34] But U.S. officials soon began to signal that the U.S. government had significantly improved its attribution capabilities. In a 2012 speech, Secretary of Defense Leon Panetta

---

suggested Russian government involvement in DDOS attacks on Georgia in 2008. *See* Noah Shachtman, *Top Georgian Official: Moscow Cyber Attacked Us—We Just Can't Prove It*, WIRED, Mar. 11, 2009, https://www.wired.com/2009/03/georgia-blames/ (reporting a Georgian government official's allegation that the Russian government organized the cyberattacks).

[29] Indictment at 1-2, United States v. Wang, No. 14-118 (W.D. Pa. May 1, 2014), *available at* https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[30] This is especially true outside the context of an armed conflict. Georgia's accusation against Russia involved cyberattacks accompanying Russia's invasion of Georgia. *See supra* note 28. Similarly, since Russia's annexation of Crimea in 2014, *see* Steven Lee Myers & Ellen Barry, *Putin Reclaims Crimea for Russia and Bitterly Denounces the West*, N.Y. TIMES, Mar. 18, 2014, https://www.nytimes.com/2014/03/19/world/europe/ukraine.html, the Ukrainian Security Service has repeatedly accused Russia of hacks and attempted hacks, *see, e.g.*, Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED, Mar. 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ ("Ukraine's intelligence community has said with utter certainty that Russia is behind the [2015 power grid] attack, though it has offered no proof to support the claim."); SBU Prevents Hacking Attacks on State Authorities Related to Election Process, Security Service of Ukraine, Mar. 6, 2019, https://ssu.gov.ua/en/news/1/category/1/view/5808#.j3gzNk3Q.dpbs (accusing "Russian special services" of attempted hacks); SBU Blocks Russia's Special Services Attempt of Cyber-Attack on IT System of Ukraine's Judiciary, Dec. 4, 2018, https://ssu.gov.ua/en/news/1/category/1/view/5487#.2eoqCcaM.dpbs (same).

[31] *See infra* notes 67-94 and accompanying text; *see also* Chimène I. Keitner, *Attribution by Indictment*, 113 AM. J. INT'L L. UNBOUND 207, 207 (2019) (noting that the United States made ten attributions by indictment in 2018, which "suggest[s] that this practice is likely to continue and even intensify in the near term").

[32] For an overview of the evolution in the U.S. government's publicly articulated views about its attribution capabilities, see Lin, *supra* note 19, at 26-27.

[33] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOR. AFFS. 97, 99 (2010).

[34] *See, e.g.*, Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for A Growing Problem*, 42 GEO. J. INT'L L. 971, 982 (2011) (calling attribution capabilities "primitive at best" and arguing that "[s]ophisticated attacks by knowledgeable hackers . . . are nearly impossible to trace to their source"). Some scholars still advance this view. *See, e.g.*, Christian Payne & Lorraine Finlay, *Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack*, 49 GEO. WASH. INT'L L. REV. 535, 561 (2017) (noting the "extreme difficulty of establishing the basic facts surrounding technical attribution").

explained that over the prior two years, the Defense Department had "made significant advances" in attributing cyberattacks.[35] He warned, "Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions . . . ."[36] In 2015, Director of National Intelligence James R. Clapper told Congress that most hackers "can no longer assume that their activities will remain undetected. Nor can they assume that if detected, they will be able to conceal their identities. Governmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions."[37] In September 2018, the Office of the Director of National Intelligence characterized cyberattack attribution as "difficult but not impossible."[38]

The advances in technical attribution may be matched over time by advances in attackers' capabilities to mask their identities, creating a cycle of escalating offensive and defensive capabilities in which the two sides will alternate having the advantage.[39] This cat-and-mouse game will continue to make attributions challenging, but at the same time, hackers, like their targets, are fallible and often make mistakes that reveal their identity. Indeed, the U.S. Office of the Director of National Intelligence notes that "[a]lmost all cyber attribution successes have

---

[35] Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, Oct. 11, 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[36] *Id.*

[37] James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, Senate Armed Services Comm., Feb. 26, 2015, at 2, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

[38] Office of the Dir. of Nat'l Intell., A Guide to Cyber Attribution 2, Sept. 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf; *cf.* Jeremy Hunt, "Deterrence in the Cyber Age" Speech by the Foreign Secretary, U.K. Foreign & Commonwealth Off., Mar. 7, 2019, https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary ("Along with our allies, we have improved our collective ability to detect those responsible for malign actions in cyberspace, including election interference."); U.S. Dep't of Justice, Associate Deputy Attorney General Sujit Raman Delivers Remarks at the ABA Rule of Law Initiative Annual Issues Conference, May 21, 2019, https://www.justice.gov/opa/speech/associate-deputy-attorney-general-sujit-raman-delivers-remarks-aba-rule-law-initiative ("[T]he increasing number of national security cyber cases . . . reflect our increasingly sophisticated ability to attribute this criminal conduct to the individuals and states involved.").

[39] U.S. officials have expressed concern about such possibilities. *See* James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, Senate Armed Services Comm., Feb. 9, 2016, at 3, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf (noting that there will be progress in attribution capabilities but "improving offensive tradecraft, the use of proxies, and the creation of cover organizations will hinder timely, high-confidence attribution of responsibility for state-sponsored cyber operations."); Daniel R. Coats, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, May 11, 2017, at 4, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf (highlighting that advances in artificial intelligence may result in "difficulty in ascertaining attribution").

resulted from discovery and exploitation of the attackers' operational security errors."[40]

The United States has used its improved capabilities to make a number of public attributions in recent years.[41] Public attributions by the U.S. government take one of four forms: 1) criminal indictments; 2) economic sanctions; 3) technical alerts; and 4) official statements or press releases.

The U.S. Department of Justice handles criminal indictments. The first public attribution by the U.S. government came in the form of an indictment in 2014, when a grand jury in the Western District of Pennsylvania indicted five members of China's PLA Unit 61398, for hacking and conspiring to hack companies, including Westinghouse and U.S. Steel, to steal intellectual property.[42] As has become routine in *attributions-by-indictment*, the 56-page indictment alleges violations of the Computer Fraud and Abuse Act,[43] including conspiracy, unauthorized access to computers, and computer damage.[44] The indictment includes charges of economic espionage and trade secret theft, which are typical in cases involving theft of intellectual property.[45] Other indictments have followed. For example, in 2017, a federal grand jury indicted two Russian Federal Security Service (FSB) officers for their role in directing a hack that compromised 500 million Yahoo accounts.[46]

The second mechanism the United States has used for attribution is imposition of economic sanctions. These *attributions-by-sanctions* fall under the

---

[40] Office of the Dir. of Nat'l Intell., *supra* note 38, at 3; *see also* Lin, *supra* note 19, at 22-25 (rejecting the "conventional wisdom" that attribution is impossible and detailing various factors, such as mistakes in "tradecraft" or "operational security," like revealing user names or discussing operations on "insecure channels," that aid in technical attribution); Rid & Buchanan, *supra* note 22, at 32 (noting that "adversaries reliably make mistakes," and "[t]he perfect cyber attack is as elusive as the perfect crime").

[41] *See* SASHA ROMANOSKY & BENJAMIN BOUDREAUX, PRIVATE SECTOR ATTRIBUTION OF CYBER INCIDENTS, RAND, at 35-36 (Feb. 2019), https://www.rand.org/content/dam/rand/pubs/working_papers/WR1200/WR1267/RAND_WR1267.pdf (providing a table of public U.S. government attributions to states).

[42] Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[43] The Computer Fraud and Abuse Act is the main federal anti-hacking law in the United States. *See* 18 U.S.C. § 1030. It criminalizes accessing "without authorization" or "exceed[ing] authorized access" to a "protected computer"—defined as any computer "used in or affecting interstate of foreign commerce." *Id.* § 1030(a)(2)(c), (e)(2)(b). It also prohibits, among other things, damaging protected computers and threatening to cause damage to such computers in order to extort money, such as in ransomware attacks. *Id.* § 1030(a)(5), (a)(7).

[44] *See* Indictment, *supra* note 29, at paras. 1-50.

[45] *Id.* at paras. 54-57.

[46] U.S. Dep't of Justice, U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts, Mar. 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions; Indictment, United States v. Dokuchaev, No. CR17-103 (N.D. Cal. Feb. 28, 2017), https://www.justice.gov/opa/press-release/file/948201/download.

purview of the Treasury Department. Executive Order 13,694, issued in 2015, created a new cyber sanctions regime allowing the Treasury Secretary to block the property of individuals "engaging in significant malicious cyber-enabled activities," including interfering with critical infrastructure computers, engaging in trade secret theft, or being complicit in significant cyber-enabled theft of trade secrets.[47] In December 2016, the Obama Administration amended the Executive Order to include election interference.[48] The Administration promptly used the new authority to sanction—and thereby accuse—Russia's intelligence services, four Russian intelligence officers, and three companies for interfering in the 2016 election.[49] Attributions-by-sanctions are accompanied by a Treasury Department press release that makes explicit the allegation of foreign government involvement in or responsibility for a cyberattack. For example, the press release detailing sanctions imposed on North Korea for the 2014 Sony Pictures hack explained that the sanctions were "[i]n response to [North Korea's] numerous provocations, particularly the recent cyber-attack targeting Sony Pictures Entertainment and the threats against movie theaters and moviegoers."[50]

---

[47] Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, Exec. Order 13,694, 80 Fed. Reg. 18,077, 18,077-78 (Apr. 2, 2015). Sanctions under the Executive Order do not depend on foreign government involvement; Treasury has imposed sanctions for routine cybercrime issues as well. *See, e.g.*, Dep't of Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities, Dec. 29, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx (detailing sanctions against two Russian individuals for distribution of malware and associated theft of information). Treasury has also used country-specific sanctions regimes to attribute cyberattacks to foreign governments. *See, e.g.*, Dep't of Treasury, Treasury Imposes Sanctions Against the Government of The Democratic People's Republic of Korea, Jan. 2, 2015, https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx (detailing sanctions imposed against North Korean government and related entities for the hack of Sony Pictures). In May 2019, the European Union established a cyber-specific sanctions regime that, like the U.S. sanctions regime, permits imposition of travel bans and asset freezes for "persons or entities that are responsible for cyber-attacks or attempted cyberattacks, who provide financial, technical or material support for such attacks or who are involved in other ways." Council of the European Union, Cyber-Attacks: Council Is Now Able to Impose Sanctions, May 17, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

[48] Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, Exec. Order 13,757, 82 Fed. Reg. 1, 1 (Jan. 3, 2017) (adding authority to impose sanctions for "tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions").

[49] White House, Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment, Dec. 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and (detailing the basis for imposing sanctions against Russian government and associated actors); *see also* Exec. Order 13,757, *supra* note 48, at 3 (listing Russian individuals and entities designated).

[50] Dep't of Treasury, Treasury Imposes Sanctions Against the Government of The Democratic People's Republic of Korea, *supra* note 47.

The third mechanism the U.S. government uses for attributions is technical alerts issued by the Department of Homeland Security, specifically the Cybersecurity and Infrastructure Security Agency.[51] The alerts provide technical information, such as indicators of compromise and malware descriptions, to help system administrators defend against malicious activity.[52] *Attribution-by-alert* occurs when a technical alert includes an allegation that the threat actor behind malicious activity is a foreign government. For example, in June 2017, DHS issued an alert about "a malware variant, known as DeltaCharlie, used to manage North Korea's distributed denial-of-service (DDoS) botnet infrastructure."[53] The alert "provides technical details on the tools and infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally."[54] Similar attributions-by-alert have included, for example, accusations of North Korean government responsibility for malware that enabled fraudulent withdrawals from automated teller machines in dozens of countries.[55] Others have accused Russia of targeting the energy sector and collecting information on industrial control systems.[56]

The final mechanism the U.S. government has used for attributions to foreign governments is issuance of public statements or press releases. For example, in the wake of the Sony hack, the FBI issued a statement attributing the cyberattack to the North Korean government.[57] Similarly, DHS and the Director of National Intelligence issued a statement attributing the 2016 hack of the Democratic National Committee to the Russian government.[58] Often such *attributions-by-press release* are the first in a series of U.S. governmental attributions and responsive actions.

---

[51] For an explanation of the agency's role, see About Us, https://www.us-cert.gov/about-us (last visited Sept. 12, 2019).

[52] *See, e.g.*, Dep't of Homeland Sec., Alert (TA17-164A): Hidden Cobra—North Korea's DDoS Botnet Infrastructure, June 13, 2017, https://www.us-cert.gov/ncas/alerts/TA17-164A ("This alert contains indicators of compromise (IOCs), malware descriptions, network signatures, and host-based rules to help network defenders detect activity conducted by the North Korean government.").

[53] *Id.*

[54] *Id.*

[55] Dep't of Homeland Sec., Alert TA18-275A: HIDDEN COBRA—FASTCash Campaign, Oct. 8, 2018, https://www.us-cert.gov/ncas/alerts/TA18-275A.

[56] Dep't of Homeland Sec., Alert TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, Mar. 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

[57] FBI, Update on Sony Investigation, Dec. 19, 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (stating that "the FBI now has enough information to conclude that the North Korean government is responsible for" the actions against Sony Pictures).

[58] DHS Press Office, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, Oct. 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national ("The U.S. Intelligence Community . . . is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. . . . We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.").

The U.S government frequently deploys more than one mechanism to attribute a particular cyberattack, including rolling out different attribution methods over the course of months or even years. For the Sony hack, the U.S. government first attributed the attack to North Korea in the FBI statement,[59] and followed with attribution-by-sanctions a few weeks later.[60] Nearly four years later in September 2018, the United States also engaged in attribution-by-indictment, unveiling criminal charges against a North Korean citizen, Park Jin Hyok, for allegedly participating in a "government-sponsored hacking team" responsible for the Sony hack, among others.[61] The attribution of election interference to the Russian government followed a similar pattern. The United States followed the joint DHS-DNI statement[62] with sanctions several months later against the Russian Main Intelligence Directorate (GRU), the Federal Security Service (FSB), and individual GRU officers.[63] Then in July 2018, Special Counsel Robert Mueller presented and a grand jury returned an indictment charging twelve GRU officers with hacking-related offenses,[64] including conspiring to hack "into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election," and conspiring to hack "state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections."[65]

Although the statement-sanctions-indictment ordering has occurred in several high-profile instances, this ordering is not consistent across attributions. In accusing the Iranian government of involvement in distributed denial of service attacks against U.S. financial institutions, for example, an indictment came first, and sanctions followed more than a year later.[66]

---

[59] *See supra* note 57 and accompanying text.

[60] *See* Dep't of Treasury, Treasury Imposes Sanctions Against the Government of The Democratic People's Republic of Korea, *supra* note 47.

[61] U.S. Dep't of Justice, North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, Sept. 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
Formally this attribution was by criminal complaint, rather than criminal indictment, but I use attribution-by-indictment for consistency.

[62] *See supra* note 58 and accompanying text.

[63] *See supra* note 49 and accompanying text. Additional sanctions have followed. U.S. Dep't of the Treasury, Press Release, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks, Mar. 15, 2018, https://home.treasury.gov/index.php/news/press-releases/sm0312.

[64] Indictment, United States v. Netyksho et al., No. 18-cr-215 (D.D.C. July 13, 2018), https://www.justice.gov/file/1080281/download.

[65] *Id.* at 2, 25.

[66] *See* U.S. Dep't of Justice, Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector, Mar. 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged (detailing charges against Iranian defendants related to DDOS attacks on U.S. financial institutions); Indictment at 4, United States v. Fathi, No. 16-Crim-48 (S.D.N.Y. 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged (noting that the attacks began in 2011 and

The practice of governmental public attributions broadened significantly in late 2017 and has increased since then. The impetus for the uptick was a global ransomware attack known as WannaCry. In May 2017, WannaCry malware spread quickly, reaching "more than 230,000 computers in more than 150 countries" and hitting the U.K. National Health Service particularly hard.[67] The ransomware encrypted data on infected machines, locking victims out of their files unless they paid $300 in Bitcoin.[68] In the United Kingdom, some hospitals had to divert ambulances and patients, and nearly 7000 medical appointments were cancelled.[69] The attack also hit the Russian Interior Ministry and impacted companies including Spain's Telefonica, France's Renault, and FedEx.[70] Spread via phishing emails, the ransomware reportedly "us[ed] a hacking method that the N.S.A. is believed to have developed as part of its arsenal of cyberweapons"—a method that was stolen and posted online by a group called the "Shadow Brokers."[71]

Shortly after the attack, press reports indicated that North Korea was responsible,[72] but the official attributions came only months later. Britain started the ball rolling, with Minister of Security Ben Wallace telling the BBC in October 2017 that North Korea was responsible, but declining to explain the evidentiary basis of the attribution.[73] Then in mid-December, the United States, United Kingdom, Australia, Canada, New Zealand, and Japan issued coordinated statements attributing WannaCry to North Korea and denouncing the country's actions.[74] White House

---

continued until 2013); U.S. Dep't of Treasury, Treasury Targets Supporters of Iran's Islamic Revolutionary Guard Corps and Networks Responsible for Cyber-Attacks Against the United States, Sept. 14, 2017, https://www.treasury.gov/press-center/press-releases/Pages/sm0158.aspx (explaining designations and noting that the designated individuals were indicted in 2016).

[67] Ellen Nakashima & Philip Rucker, *U.S. Declares North Korea Carried Out Massive WannaCry Cyberattack*, WASH. POST, Dec. 19, 2017, https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html.

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

[69] NAT'L AUDIT OFF., INVESTIGATION: WANNACRY CYBER ATTACK AND THE NHS 14 (Apr. 25, 2018), https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[70] *Massive Ransomware Infection Hits Computers in 99 Countries*, *supra* note 68.

[71] Nicole Perlroth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, N.Y. TIMES, May 12, 2017, https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html.

[72] *See, e.g.*, Nicole Perlroth & David E. Sanger, *In Computer Attacks, Clues Point to Frequent Culprit: North Korea*, N.Y. TIMES, May 15, 2017, https://www.nytimes.com/2017/05/15/us/nsa-hacking-shadow-brokers.html (citing unidentified "[i]ntelligence officials" and noting that private experts from Symantec, Google, and Kaspersky agreed that North Korea was responsible).

[73] Dan Bilefsky, *Britain Says North Korea Was Behind Cyberattack on Health Service*, N.Y. TIMES, Oct. 27, 2017, https://www.nytimes.com/2017/10/27/world/europe/uk-ransomware-hack-north-korea.html.

[74] Thomas P. Bossert, *It's Official: North Korea Is Behind WannaCry*, WALL ST. J., Dec. 18, 2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537; U.K. Foreign & Commonwealth Off., Foreign Office Minister Condemns North Korean Actor for

Homeland Security Advisor Thomas Bossert explained in a press briefing that the United States "do[es] not make this allegation lightly. We do so with evidence, and we do so with partners," citing the support of allied countries and "[c]ommercial partners," including Microsoft and Facebook, which "act[ed] on their own initiative . . . without any direction by the U.S. government or coordination to disrupt the activities of North Korean hackers."[75] After the public attributions, additional actions took months. In June 2018, the United States criminally charged a North Korean citizen, alleged to be a member of "a government-sponsored hacking team," for working for "a North Korean government front company . . . to support the [North Korean] government's malicious cyber actions," including WannaCry.[76] The Treasury Department also sanctioned him in September 2018.[77]

Three significant coordinated attribution efforts have followed the WannaCry attributions.

One focused on NotPetya—a serious disruptive cyberattack in June 2017 that struck Ukraine and spread worldwide, crippling companies, including FedEx and Maersk, and ultimately causing more than $10 billion in damages.[78] NotPetya

---

WannaCry Attacks, Dec. 19, 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks (quoting Foreign Office Minister for Cyber, Lord Ahmad as stating: "The UK's National Cyber Security Centre assesses it is highly likely that North Korean actors known as the Lazarus Group were behind the WannaCry ransomware campaign . . . ."); Greta Bossenmaier, Chief, Communications Security Establishment, Govt. of Canada, CSE Statement on the Attribution of WannaCry Malware, Dec. 19, 2017, https://www.cse-cst.gc.ca/en/media/2017-12-19 (noting Canada's agreement with attribution of WannaCry to North Korea); Min. for. Affs. Julie Bishop, Dep't of Foreign Affs. & Trade, https://foreignminister.gov.au/releases/Pages/2017/jb_mr_171220.aspx (last visited Sept. 12, 2019) ("Based on advice from our intelligence agencies, and through consultations with our allies, we confirm that North Korea carried out the 'WannaCry' ransomware campaign."); New Zealand Nat'l Cyber Security Centre, New Zealand Concerned at North Korean Cyber Activity, Dec. 20, 2017, https://www.ncsc.govt.nz/newsroom/new-zealand-concerned-at-north-korean-cyber-activity/ (stating that New Zealand "support[s] the actions of our cyber security partners in calling out this sort of reckless and malicious cyber activity"); Statement by Press Secretary Norio Maruyama, The U.S. Statement on North Korea's Cyberattacks, Dec. 20, 2017, https://www.mofa.go.jp/press/release/press4e_001850.html ("Japan supports the announcement of the United States demonstrating its firm determination towards ensuring the security of cyberspace, and denounces North Korea's involvement behind the WannaCry incidents.").

[75] White House, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, Dec. 19, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

[76] U.S. Dep't of Justice, North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, Sept. 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and. The complaint was filed in June, but only unsealed in September. Criminal Complaint, United States v. Park, No. MJ 18-1479 (C.D. Cal. June 8, 2018), https://www.justice.gov/opa/press-release/file/1092091/download.

[77] U.S. Dep't of Treasury, Treasury Targets North Korea for Multiple Cyber-Attacks, Sept. 6, 2018, https://home.treasury.gov/news/press-releases/sm473.

[78] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED, Aug. 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-

initially looked like a ransomware attack similar to WannaCry,[79] but it "irreversibly encrypted computers' master boot records," rendering ransom payments "futile."[80] Ukraine accused Russia of responsibility in July 2017.[81] Coordinated attributions followed in February 2018, with the United Kingdom taking the lead in attributing NotPetya to the Russian military.[82] The United States seconded the U.K. attribution, calling WannaCry a "reckless and indiscriminate cyber-attack that will be met with international consequences,"[83] and other countries, including Australia, Canada, Estonia, Denmark, Lithuania, and New Zealand concurred.[84] The United States subsequently cited Russia's responsibility for NotPetya as among the bases for sanctioning the GRU and GRU officials.[85]

In October 2018, the Netherlands, United Kingdom, and United States led coordinated attributions to the GRU of cyberattacks on victims who were

---

code-crashed-the-world/ (providing a detailed account of the attack); Nicole Perlroth, Mark Scott & Sheera Frankel, *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. TIMES, June 27, 2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html (describing the attack and its immediate aftermath).

[79] Media reports highlighted another similarity. Mark Landler & Scott Shane, *U.S. Condemns Russia for Cyberattack, Showing Split in Stance on Putin*, N.Y. TIMES, Feb. 15, 2018, https://www.nytimes.com/2018/02/15/us/politics/russia-cyberattack.html ("The NotPetya attacks took advantage of vulnerabilities identified by the National Security Agency and then made public by a group calling itself the Shadow Brokers.").

[80] Greenberg, *supra* note 78.

[81] SBU Established Involvement of the RF Special Services Into Petya.A Virus-Extorter Attack, Security Service of Ukraine, July 1, 2017, https://ssu.gov.ua/en/news/1/category/2/view/3660#.9MJp6B36.dpbs (accusing the Russian Federation "special services").

[82] Foreign & Comm. Off., Foreign Office Minister Condemns Russia for NotPetya Attacks, Feb. 15, 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks ("The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017." (quoting Foreign Office Minister for Cyber Security Lord Tariq Ahmad of Wimbledon)).

[83] White House, *supra* note 4; *see also* Landler & Shane, *supra* note 79 (noting that the U.S. announcement, which had been planned to issue with the British attribution, was delayed due to the Parkland school shooting).

[84] *See* Greta Bossenmaier, Communications Security Establishment, CSE Statement on the NotPetya Malware, Feb. 15, 2018, https://www.cse-cst.gc.ca/en/media/2018-02-15 (Canada); Council on Foreign Relations, *supra* note 13, NotPetya, https://www.cfr.org/interactive/cyber-operations/notpetya (collecting attributions); New Zealand Gov't Communications Security Bureau, New Zealand Joins International Condemnation of NotPetya Cyber-Attack, Feb. 16, 2018, https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/ (noting that "international partners" have attributed NotPetya to Russia and condemning NotPetya); Angus Taylor, Min. for Law Enforcement & Cyber Sec., Australian Government Attribution of the 'NotPetya' Cyber Incident to Russia, Feb. 16, 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-attributes-notpetya-malware-to-russia.pdf (attributing NotPetya to "Russian state sponsored actors").

[85] U.S. Dep't of Treasury, *supra* note 63.

investigating Russian misdeeds.[86] The Netherlands and the United Kingdom accused the GRU of sending agents to the Netherlands to hack the Organization for the Prohibition of Chemical Weapons (OPCW),[87] which was investigating the poisoning of a former Russian spy, Sergei Skripal, and his daughter in the United Kingdom.[88] According to the Dutch government, investigation of hacking equipment seized from the GRU operatives in the Netherlands also revealed that one of the operatives had "target[ed] the investigation of Malaysia Airlines Flight MH17,"[89] which was shot down by a Russian missile over Ukraine in 2014, killing the nearly 300 people on board.[90]

Another facet of the attributions focused on the GRU's targeting of anti-doping agencies. The United States released an indictment accusing several GRU agents not just of targeting the OPCW, but also hacking numerous anti-doping agencies, including the U.S. Anti-Doping Agency, World Anti-Doping Agency, and the Fédération International de Football Association.[91] Russia allegedly targeted these organizations due to their "role in the investigation or public condemnation of Russia's state-sponsored athlete doping program."[92] Australia, Canada, New Zealand

---

[86] *See* David E. Sanger, Eileen Sullivan & David D. Kirkpatrick, *Russia Targeted Investigators Trying to Expose Its Misdeeds, Western Allies Say*, N.Y. TIMES, Oct. 4, 2018, https://www.nytimes.com/2018/10/04/us/politics/russia-hacks-doping-poisoning.html.

[87] Prime Minister's Off., Joint Statement from Prime Minister May and Prime Minister Rutte, Oct. 4, 2018, https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte. Canada confirmed the attribution. Gov't of Canada, Global Affairs Canada, Canada Identifies Malicious Cyber-Activity by Russia, Oct. 4, 2018, https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html.

[88] Amb. Peter Wilson, Minister for Europe Statement: Attempted Hacking of the OPCW by Russian Military Intelligence, Oct. 4, 2018, https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence (detailing OPCW role in investigating the ex-spy poisoning in the United Kingdom, as well as testing suspected chemical weapons used in Syria); *see also Russian Spy Poisoning: What We Know So Far*, BBC, Oct. 8, 2018, https://www.bbc.com/news/uk-43315636 (providing an overview of the Skripal poisoning).

[89] Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW, Oct. 4, 2018, https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw; *see also* Sanger, Sullivan & Kirkpatrick, *supra* note 86.

[90] *See* Anthony Deutsch, *Investigators Identify Russian Military Unit in Downing of Flight MH17*, REUTERS, May 23, 2018, https://www.reuters.com/article/us-ukraine-crisis-mh17/investigators-identify-russian-military-unit-in-downing-of-flight-mh17-idUSKCN1IP0TR ("Dutch prosecutors identified a Russian military unit on Thursday as the source of the missile that shot down Malaysia Airlines Flight 17 over eastern Ukraine in 2014, killing all 298 people on board.").

[91] U.S. Dep't of Justice, U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations, Oct. 4, 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and (detailing hacking charges); Indictment, United States v. Morenets, No. 18-263, at 2-3 (W.D. Pa. Oct. 3, 2018), https://www.justice.gov/opa/page/file/1098481/download.

[92] *Id.*

and the United Kingdom confirmed the doping-related attributions.[93] Australia, New Zealand, and the United Kingdom further piled on by attributing the 2016 DNC hack to the GRU.[94]

Another coordinated attribution in December 2018 garnered less attention. The U.S. Department of Justice charged two Chinese nationals with a decade-long campaign of hacking at the behest of China's Ministry of State Security,[95] and allied countries simultaneously confirmed the accusations.[96] The indictment alleges that the defendants directly hacked dozens of companies and government agencies to steal sensitive data,[97] and starting in 2014, they also hacked "managed service providers"—companies like cloud providers that store information for other companies—and used their unauthorized access to steal intellectual property and other data from the providers' clients.[98] According to press reports, the compromised companies include Hewlett Packard Enterprises, IBM, and Huntington Ingalls Industries, which builds nuclear submarines for the U.S. Navy.[99] Multiple private

[93] Prime Minister of Australia, Attribution of a Pattern of Malicious Cyber Activity to Russia, Oct. 4, 2018, https://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia; Gov't of Canada, Global Affairs Canada, Canada Identifies Malicious Cyber-Activity by Russia, Oct. 4, 2018, https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html; New Zealand Gov't Communications Security Bureau, Malicious Cyber Activity Attributed to Russia, Oct. 4, 2018, https://www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/; U.K. National Cybersecurity Centre, *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*, Oct. 4, 2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

[94] Prime Minister of Australia, *supra* note 93; New Zealand Gov't Communications Security Bureau, *supra* note 93; U.K. National Cybersecurity Centre, *supra* note 93. The governments also attributed several additional hacks to the GRU, including release of BadRabbit ransomware that caused disruption in Ukraine and hacking of a U.K. TV station. Prime Minister of Australia, *supra* note 93; New Zealand Gov't Communications Security Bureau, *supra* note 93; U.K. National Cybersecurity Centre, *supra* note 93.

[95] U.S. Dep't of Justice, Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information, Dec. 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion (describing charges); Indictment, United States v. Zhu, No. 18-Crim-891 (S.D.N.Y. Dec. 17, 2018), https://www.justice.gov/opa/press-release/file/1121706/download.

[96] Press Release, National Cyber Security Centre, UK and Allies Reveal Global Scale of Chinese Cyber Campaign, Dec. 20, 2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign; Hon. Marise Payne, Min. for. Affs., & Hon. Peter Dutton, Min. for Home Affairs, Attribution of Chinese Cyber-Enabled Commercial Intellectual Property Theft, Dec. 21, 2018, https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx.

[97] Indictment, *supra* note 95, at 3-4.

[98] *Id.* at 4.

[99] Jack Stubbs, Joseph Menn & Christopher Bing, *Inside the West's Failed Fight Against China's 'Cloud Hopper' Hackers*, REUTERS, June 26, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

cybersecurity firms had also identified and tracked the hackers for years,[100] publishing details about the defendants and their exploits.[101]

In addition to their practice in carrying out attributions to government actors, states have made some explicit statements regarding attribution-related evidentiary issues. The statement supported by the broadest range of countries came in a 2015 U.N. Group of Governmental Experts (GGE) report.[102] The GGE included Brazil, China, India, Russia, the United States, and United Kingdom, among others.[103] All of the states agreed that in the cybersecurity context "accusations of organizing and implementing wrongful acts brought against States should be substantiated."[104] But they did not agree on how much evidence or what kind of evidence would suffice to "substantiate" accusations.[105]

Since the 2015 report, Russia, China, and other countries have continued to push the position that accusations must be substantiated.[106] Having been on the receiving end of attributions, Russia and China of course have a strong interest in forcing accusing countries to disclose as much information as possible since doing so often reveals sources and methods used by law enforcement and the intelligence community. Moreover, China, Russia, and their allies may calculate that given the cost to sources and methods, establishing an evidentiary requirement may tamp down on the number of public attributions over all.

For their part and despite their practice of providing at least some evidence to accompany attributions, the United States and United Kingdom have advanced the

---

[100] The indictment notes the various names that private firms have given to the hacking group. Indictment, *supra* note 95, at 2; *see* Catalin Cimpanu, *US Charges Two Chinese Nationals for Hacking Cloud Providers, NASA, the US Navy*, ZDNET, Dec. 20, 2018, https://www.zdnet.com/article/us-charges-two-chinese-nationals-for-hacking-cloud-providers-nasa-the-us-navy/ ("The two hackers are part of a cyber-espionage group that's been on the radar of cyber-security firms all over the world under codenames such as APT10 (FireEye), Red Apollo (PwC), CVNX (BAE Systems), Stone Panda (CrowdStrike), POTASSIUM (Microsoft), and MenuPass (Trend Micro).").

[101] *See* Adam Kozy, Two Birds, One STONE PANDA, CrowdStrike Blog, Aug. 30, 2018, https://www.crowdstrike.com/blog/two-birds-one-stone-panda/ (including details about APT10 and Zhang Shilong).

[102] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. No. A/70/174, at 15-17, http://undocs.org/A/70/174 (2015) (listing countries participating).

[103] *Id.*

[104] *Id.* at 13.

[105] *See* Kristen Eichensehr, *"Your Account May Have Been Targeted By State-Sponsored Actors": Attribution and Evidence of State-Sponsored Cyberattacks*, JUST SECURITY, Jan. 11, 2016, https://www.justsecurity.org/28731/your-account-targeted-state-sponsored-actors-attribution-evidence-state-sponsored-cyberattacks/ (discussing the GGE report).

[106] For example, Russia and China, along with a number of other states, tabled a draft U.N. General Assembly resolution in October 2018, stating that, in the case of "information and communications technologies," "[a]ccusations of organizing and implementing wrongful acts brought against States should be substantiated." Developments in the Field of Information and Telecommunications in the Context of International Security, U.N.G.A., Doc. No. A/C.1/73/L.27/Rev.1, para. 10, https://undocs.org/A/C.1/73/L.27 (2018).

position that international law does not require disclosure of *any* evidence to support accusations. In a November 2016 speech, State Department Legal Adviser Brian Egan explained,

> [D]espite the suggestion by some States to the contrary, there is *no* international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action. There may, of course, be political pressure to do so, and States may choose to reveal such evidence to convince other States to join them in condemnation, for example. But that is a policy choice—it is not compelled by international law.[107]

In a May 2018 speech, U.K. Attorney General Jeremy Wright echoed the U.S. position about the absence of international law.[108] Wright argued, "There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based . . . ."[109] In September 2019, France articulated the same position.[110]

Scholars have noted the disagreement among states over the evidentiary issue.[111] In the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, a comprehensive attempt to restate existing international law as it applies to cyberspace, an international group of experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence acknowledged states'

---

[107] Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 177 (2017). Egan's speech was the first statement of the U.S. position on evidentiary issues. *Cf.* Sean Watts, *Cyber Law Development and the United States Law of War Manual*, *in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES 49, 55 (Anna-Maria Osula & Henry Roigas eds., 2016), *available at* https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch3.pdf ("[T]he [2015 U.S. Law of War] Manual makes no attempt to identify, clarify, or for that matter even reject the existence of any international legal standard with respect to attribution, or to develop a cyber norm regarding this issue.").

[108] Jeremy Wright QC MP, Attorney General, United Kingdom, 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.

[109] *Id.*

[110] Ministère des Armées, République Française, Droit International Appliqué aux Opérations dans le Cyberespace 11 (2019), https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf (noting that a state that suffers a cyberattack is not required to make a public attribution and if does make such an attribution, international law does not require a victim state to provide proof to support the attribution) (author's translation).

[111] *See* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 633 (2018) ("There is no established body of international law of evidence that clearly defines the legal criteria and standards of proof governing a determination of whether a given cyberoperation should be attributed to individuals, groups, or nations. . . . Nor is there an internationally accepted mechanism for legally attributing cyberoperations that victim states can resort to."); Roscini, *supra* note 11, at 241 n.58 ("Whether or not States have an obligation to make evidence public is a matter of debate.").

divergent positions on the existence of a legal requirement.[112] The experts concluded that "although [providing evidence] . . . may be prudent in avoiding political and other tensions, insufficient State practice and *opinio juris* (in great part because cyber capabilities are highly classified) exist to conclude that there is an established basis under international law for such an obligation."[113]

B. Attributions by Non-Governmental Actors

Governments are not the only entities that attribute cyberattacks to states. Cybersecurity companies, technology companies, non-profits, and an academic institute have also made numerous public attributions to governments in recent years.[114] As with the dominance of the U.S. government on the governmental side, most, but not all,[115] of the non-governmental entities that do public attributions are U.S.-based.[116]

In high profile instances, non-governmental attributions to governments have preceded government attributions. For example, in a detailed report issued in February 2013, the cybersecurity firm Mandiant identified one of the Chinese PLA officers whom the U.S. later indicted for intellectual property theft.[117] Similarly, in June 2016, Crowdstrike, which the DNC had hired to investigate security breaches, publicly accused the Russian government of hacking the DNC months before the U.S. government did.[118]

---

[112] TALLINN MANUAL 2.0, *supra* note 8, at 83 ("[A] few States have taken the position that there is a legal obligation to disclose evidence on which attribution is based whenever taking actions in response to cyber operations purportedly constitute an international wrongful act.").

[113] *Id.* at 83.

[114] *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 489-94 (2017) (discussing attributions by private cybersecurity companies); *id.* at 498 (discussing attribution to China in "Operation SMN" by companies including FireEye and Microsoft); *see also* ROMANOSKY & BOUDREAUX, *supra* note 41, at 6-10 (providing an overview of public attributions by private companies).

[115] The Citizen Lab, based at the University of Toronto, is a prominent non-U.S.-based attributor. About the Citizen Lab, The Citizen Lab, https://citizenlab.ca/about/ (last visited Sept. 12, 2019); *cf.* Eichensehr, *supra* note 114, at 493 (discussing a report by Qihoo 360, a Chinese Internet security company, that reported on a state-based hacking group, but without naming the state responsible).

[116] *See infra* note 135 and accompanying text (discussing Russian company Kaspersky, which has implicitly, though not explicitly, attributed attacks to the United States).

[117] *Compare* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 52-55 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (discussing Wang Dong), *with* Indictment, *supra* note 29, at 49 (identifying Wang Dong).

[118] Dmitri Alperovitch, Bears in the Midst: Intrusion into the Democratic National Committee, CrowdStrike Blog, June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. The first U.S. government attribution came in October 2016. *See* DHS Press Office, *supra* note 58.

Non-governmental attributions differ from government attributions in a number of ways.[119] First, the non-governmental attributions are often quite detailed, providing indicators of compromise and other technical information.[120] The publication of such details allows others to take actions to defend networks from further compromise, as well as to verify the attribution.[121]

Second, non-governmental attributions cover additional types of attacks beyond what governments have attributed. In some cases, this may be because governments are reluctant to attribute hacks of the sort that victim governments may also undertake.[122] For example, the U.S. government never formally attributed the hack of the Office of Personnel Management, which involved the compromise of security clearance information for 21.5 million people.[123] The closest the United States came was a statement by then-Director of National Intelligence James Clapper who, when asked about the hack, said, "'You have to kind of salute the Chinese for

[119] This discussion of differences between governmental and non-governmental attributions draws from Kristen E. Eichensehr, *Decentralized Cyberattack Attribution*, 113 AM. J. INT'L L. UNBOUND 213 (2019).

[120] *See, e.g.*, Mandiant, *supra* note 117, at 66-74 (providing information on technical appendices); Alperovitch, *supra* note 118 (providing indicators of compromise); LOOKOUT & ELECTRONIC FRONTIER FOUND., DARK CARACAL: CYBER-ESPIONAGE AT A GLOBAL SCALE (2018), https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf (attributing an espionage campaign focused on mobile devices to Lebanon's General Directorate of General Security and providing indicators of compromise); DARIEN HUSS, NORTH KOREA BITTEN BY BITCOIN BUG: FINANCIALLY MOTIVATED CAMPAIGNS REVEAL NEW DIMENSION OF THE LAZARUS GROUP, PROOFPOINT (2017), https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf (attributing to North Korea a cryptocurrency-focused hacking campaign and providing indicators of compromise).

[121] For example, numerous other companies and researchers endorsed Crowdstrike's attribution of the DNC hack to Russia. *See* Ellen Nakashima, *Cyber Researchers Confirm Russian Government Hack of Democratic National Committee*, WASH. POST, July 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 (discussing confirmation of Crowdstrike's attribution by cybersecurity companies Fidelis Cybersecurity, Mandiant, and ThreatConnect); Matt Tait, *On the Need for Official Attribution of Russia's DNC Hack*, LAWFARE, July 28, 2016, https://www.lawfareblog.com/need-official-attribution-russias-dnc-hack (discussing why the author and Prof. Thomas Rid agree with Crowdstrike's attribution).

[122] Relatedly, the victim government's own willingness to engage in similar behavior makes it more difficult to take the responsive actions often expected to accompany public attributions. *See infra* note 132 and accompanying text.

[123] *See* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES, https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html (noting that the "hackers stole 'sensitive information,' including addresses, health and financial history, and other private details, from 19.7 million people who had been subjected to a government background check, as well as 1.8 million others, including their spouses and friends").

what they did . . . .'"[124] Crowdstrike, on the other hand, attributed the attack to China.[125]

In other cases, non-governmental attributors have focused on different kinds of attacks. For example, the Citizen Lab at the University of Toronto has focused on nation-state espionage against civil society. Citizen Lab has published several reports on exploits sold by NSO Group, an Israeli company, to governments around the world and then used against civil society.[126] For example, Citizen Lab attributed an attempted compromise of the phone of a human rights activist based in the United Arab Emirates (UAE) to that country's government.[127] It similarly accused the Mexican government of targeting journalists and lawyers investigating government corruption and human rights abuses.[128]

Third and relatedly, non-governmental attributions have implicated a broader range of government attackers. Many of the attributions focus on the same countries that governmental attributions do, namely China, Iran, North Korea, and Russia.[129]

---

[124] *In Data Breach, Reluctance To Point The Finger at China*, NPR, July 2, 2015, https://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china (quoting Clapper).

[125] Shane Harris, *Security Firm: China Is Behind the OPM Hack*, DAILY BEAST, July 9, 2015, https://www.thedailybeast.com/security-firm-china-is-behind-the-opm-hack (quoting Dmitri Alperovitch from Crowdstrike, stating "'Based on indicators we received from the U.S. government and our own analysis, I can confirm that the intruders were affiliated with the Chinese government . . . .'").

[126] *See* Bill Marczak & John Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender*, Citizen Lab, Aug. 24, 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (discussing the NSO Group's sales of "mobile phone surveillance software to governments around the world").

[127] *Id.*

[128] *See* John Scott-Railton et al., *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, Citizen Lab, June 19, 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (detailing investigation and targets of spyware and noting that although there is "no conclusive evidence attributing these messages to specific government agencies in Mexico[,] . . . circumstantial evidence suggests that one or more . . . of NSO's government customers in Mexico are the likely operators"); *see also* Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. TIMES, June 19, 2017, https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html (reporting on the Citizen Lab report).

[129] *See, e.g.*, Alperovitch, *supra* note 118 (attributing DNC hack to Russia); HUSS, *supra* note 120 (attributing crypto-currency-focused hacking campaign to North Korea); Manish Sardiwal et al., New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit, FireEye, Dec. 7, 2017, https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html (attributing cyberespionage against a Middle Eastern government to hackers "work[ing] on behalf of the Iranian government"); THREATCONNECT & DEFENSE GROUP INC., CAMERASHY: CLOSING THE APERTURE ON CHINA'S UNIT 78020 (2015), https://threatconnect.com/camerashy/ (attributing espionage against Southeast Asian targets to the Chinese PLA).

But others have implicated different governments, including Lebanon, Mexico, and the UAE.[130]

Finally, the implications of making an attribution differ for governmental and non-governmental actors. To be sure, entities on either side of the state/non-state line could make themselves a target for retaliation by attributing a cyberattack to a state.[131] But governments that accuse other governments of cyberattacks face pressure to undertake follow-up actions against the identified perpetrators.[132] The difficulties of follow-on actions, such as indictments, sanctions, or covert or overt responsive actions, may discourage governments from making public attributions. Non-governmental entities are not responsible for responsive actions and therefore may feel somewhat freer to accuse governments in the first place. Put another way, the pressure on governments to combine the naming-and-shaming of public attribution with other responsive actions means that government attributions run a greater risk of escalation than non-governmental attributions.

Notably, not all cybersecurity companies are willing to make public attributions to governments or think such attributions are a good idea. A company called Dragos, which focuses on industrial control system cybersecurity, has a policy *against* publicly attributing intrusions to governments. In a *Washington Post* interview, Dragos CEO Robert Lee explained, "'[T]here's no value to our customers' in identifying their attackers,'" and called attribution a "political discussion," noting that "an inaccurate attribution of responsibility could escalate tensions between states."[133] Other companies, especially non-U.S. companies have attributed state-sponsored cyber operations obliquely, without explicitly naming the state involved.[134] In particular, Kaspersky Lab, a Russian cybersecurity company, has identified malware used by the "Equation Group," which is understood to refer to the

---

[130] *See, e.g.*, LOOKOUT & ELECTRONIC FRONTIER FOUND., *supra* note 120 (attributing cyberespionage to Lebanon's government); *supra* notes 127-128 and accompanying text (discussing hacks attributed to the UAE and Mexico).

[131] *See, e.g.*, Jim Finkle, *Mandiant Goes Viral After China Hacking Report*, REUTERS, Feb. 22, 2013, https://www.reuters.com/article/net-us-hackers-virus-china-mandiant/mandiant-goes-viral-after-china-hacking-report-idUSBRE91M02P20130223 (reporting that hackers "creat[ed] malicious versions" of Mandiant's APT1 report "infected with computer viruses" and "emailed the tainted reports . . . in a bid to wreak havoc under Mandiant's name").

[132] *See, e.g.*, Eric Lipton, David E. Sanger & Scott Shane, *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 (reporting on the Obama Administration's difficulties in formulating a response to Russian election interference); David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. TIMES, Oct. 7, 2016, https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html (noting that the U.S. government's attribution of the DNC hack to Russia "immediately rais[ed] the issue of whether President Obama would seek sanctions or other retaliation").

[133] Ellen Nakashima & Aaron Gregg, *They're on the Lookout for Malware That Can Kill*, WASH. POST, Apr. 27, 2018, https://www.washingtonpost.com/world/national-security/theyre-on-the-lookout-for-malware-that-can-kill/2018/04/27/33190738-32c1-11e8-8abc-22a366b72f2d_story.htm

[134] *See supra* notes 115-116 and accompanying text.

U.S. National Security Agency and other U.S. government entities, though Kaspersky has refrained from explicitly naming the United States.[135]

C. The Purposes of Attribution

Very often victims or government agencies may determine who conducted a cyberattack, but decline to make that information public. Because they are secret or at least not publicly known, non-public or internal attributions are of limited utility to entities other than the victim. The public attributions that this Article addresses, however, can serve more and broader goals. The purpose of an attribution can inform how it is conducted and the extent to which it should be governed by legal standards.

One of the most often-cited purposes of public attributions is *macro-level deterrence*.[136] The idea is that public naming-and-shaming of state-sponsored actors will cause the named states (and potentially other states that might be watching) to refrain from future attacks.[137] For example, in announcing an indictment of Iranian hackers for DDOS attacks on U.S. financial institutions, then-FBI Director James Comey explained, "By calling out the individuals and nations who use cyber attacks to threaten American enterprise, as we have done in this indictment, we will change behavior."[138] U.S. officials made similar claims about the cyber sanctions executive order. In announcing the new sanctions regime, the Obama Administration's Cybersecurity Coordinator, Michael Daniel called it "a new way of both deterring and imposing costs on malicious cyber actors wherever they may be"[139]

---

[135] *See, e.g.*, Nicole Perlroth & David E. Sanger, *U.S. Embedded Spyware Overseas, Report Claims*, N.Y. TIMES, Feb. 16, 2015, https://www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html (discussing Kaspersky Lab report on the Equation Group and noting the moniker "appears to be a veiled reference to the National Security Agency and its military counterpart, United States Cyber Command"); *see also* Gordon Corera, *Kaspersky Defends Its Role in NSA Breach*, BBC, Nov. 16, 2017, https://www.bbc.com/news/technology-42009599 (noting that "Equation Group" "is widely understood to be Kaspersky's codeword for the NSA").

[136] *See generally* Joseph S. Nye, Jr., *Deterrence and Dissuasion in Cyberspace*, 41 INT'L SEC. 44, 45 (Winter 2016/17) ("Deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."); *see, e.g.*, Keitner, *supra* note 31, at 210 (identifying deterrence as one purpose of U.S. attributions-by-indictment).

[137] Victim states can attempt deterrence without going public, instead communicating privately to the attacker in an attempt to convince or threaten the attacker into ceasing its behavior. The Obama Administration reportedly attempted such an approach with Russia in August and September 2016 in advance of publicly attributing the DNC and related hacks to Russia in October 2016. Greg Miller, Ellen Nakashima & Adam Entous, *Obama's Secret Struggle To Punish Russia for Putin's Election Assault*, WASH. POST, June 23, 2017, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.d5ada09b5d4f. Deterring *other* states, however, requires public attribution.

[138] U.S. Dep't of Justice, *supra* note 66; *see also* Hunt, *supra* note 38 (discussing public attributions as one piece of the United Kingdom's approach to cyber deterrence).

[139] White House, On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," Apr. 1, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/record-press-call-president-

Measuring the deterrent effect of attributions is difficult. Unlike nuclear deterrence, where effective deterrence meant zero use of nuclear weapons, deterrence in the cybersecurity sphere need not mean *no* cyberattacks, but rather no cyberattacks above a certain level. Defined in this more nuanced way, the macro-level deterrence concept has borne some fruit. After the first U.S. attribution-by-indictment—the charges against Chinese PLA officers for intellectual property theft—sources indicated that the Chinese military substantially scaled down its economic espionage activities.[140] But at the same time, state-sponsored hacks of many kinds have continued after indictments.[141] Jack Goldsmith and Robert D. Williams recently bluntly declared that with respect to intellectual property theft, "the Justice Department's deterrence-by-indictment efforts have failed. And the scale of the failure is large."[142] The Justice Department's own continued indictments bear witness to this: in December 2018, the United States released an indictment of hackers linked to the Chinese Ministry of State Security for wide-ranging intellectual property theft that *began* in 2014—the same year indictments were supposed to begin deterring such behavior by China.[143]

Expecting public attributions alone to deter states may be asking too much. But public attributions serve other purposes.

First, public attributions to *particular* foreign government-employed or sponsored individuals may create successful *micro-level deterrence*. Individuals charged in an indictment cannot travel to the indicting country or countries that have extradition treaties with the indicting country; if they do, they risk capture and transfer for trial.[144] Individuals subject to economic sanctions may have assets seized

---

s-executive-order-blocking-property-certain- (quoting Michael Daniel). U.K. Foreign Secretary Jeremy Hunt made similar points about the deterrent effect of the new EU cyber sanctions regime. Press Release, U.K. Foreign & Commonwealth Office, Cyber Criminals Face New EU Sanctions, May 17, 2019, https://www.gov.uk/government/news/cyber-criminals-face-new-eu-sanctions.

[140] 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 (quoting U.S. government sources); *see also* Rid & Buchanan, *supra* note 22, at 29 (noting decrease in China's hacking activity for a period of time after Mandiant's APT1 report).

[141] *See, e.g.*, John P. Carlin, *The 'Global Cybercrime Problem' Is Actually the 'Russia Problem'*, ATLANTIC, Dec. 16, 2018, https://www.theatlantic.com/ideas/archive/2018/12/how-trump-can-stand-russian-cybercrime/578185/ (suggesting that public attribution is insufficient to deter Russia).

[142] 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; *see also* Jack Goldsmith, *The DNC Hack and (the Lack of) Deterrence*, LAWFARE, Oct. 9, 2016, https://www.lawfareblog.com/dnc-hack-and-lack-deterrence (arguing that a "shame + threatened sanctions" approach has failed to deter cyberattacks).

[143] *See* Indictment, *supra* note 95, at 4.

[144] *See* U.S. Dep't of Justice, Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps, Mar. 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-

and cannot engage in financial transactions touching the United States or other sanctioning countries. These risks are real, and they are personal.[145] Individual-level deterrence may therefore be more effective than macro-level deterrence,[146] though its efficacy may vary by country. For example, losing the ability to travel to or store money in Western Europe may be less of a blow to North Korean hackers than to Russians.[147] The efficacy of individual punishments for government-backed hackers may also depend on the extent of coercion to which the hackers are subject in their home country. If their actions on behalf of their government are not voluntary, then the hackers will not alter their behavior in response to a threat of prosecution or sanctions by a foreign government.[148] Nonetheless, the indictments and sanctions may help to create workforce problems for at least some governments as individuals with the skills to engage in state-sponsored hacking consider other career options.[149]

---

behalf-islamic-revolutionary (quoting U.S. Attorney for the Southern District of New York Geoffrey S. Berman explaining that Iranian hacking defendants "are now fugitives from American justice, no longer free to travel outside Iran without risk of arrest"); *see also* Ellen Nakashima, *For Alleged Russian Hacker, a Visit to Amsterdam Is a Costly Trip*, WASH. POST, Jan. 30, 2015, https://www.washingtonpost.com/world/national-security/for-alleged-russian-hacker-a-visit-to-amsterdam-is-a-costly-trip/2015/01/30/1e240c96-a33c-11e4-9f89-561284a573f8_story.html (detailing arrest of Russian hacker, wanted for intrusions at multiple U.S. companies, while he vacationed in the Netherlands); *see also* Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW, *supra* note 89 (noting that the government publicized the Russian officers involved in order to "hamper any further attempts by them to operate internationally").

[145] A similar micro-level deterrence strategy may be influencing recently reported U.S. operations to alert individual Russian operatives that the United States is aware of their election interference-related actions. Julian E. Barnes, *U.S. Begins First Cyberoperations Against Russia Aimed at Protecting Elections*, N.Y. TIMES, Oct. 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html (reporting that U.S. Cyber Command targeted "individual Russian operatives to try to deter them from spreading disinformation to interfere in elections, telling them that American operatives have identified them and are tracking their work," and noting that "anyone singled out would know, based on the United States government's actions against other Russian operatives, that they could be indicted or targeted with sanctions").

[146] Even commentators skeptical of macro-level deterrence acknowledge the potential micro-level deterrent effect of public attributions. *See* Goldsmith & Williams, *supra* note 142 ("The indictments rarely result in prosecution but do expose the alleged wrongdoers publicly, prevent them from traveling and perhaps embarrass them in certain circles. These costs are not nothing; would-be state-sponsored cyber-intruders and their principals surely take them into account.").

[147] *See, e.g.*, Nakashima, *supra* note 144 (discussing arrest of a Russian hacker in the Netherlands).

[148] Relatedly, governmental and non-governmental attributors should consider the likely consequences to individual hackers outed in attributions; the consequences imposed by their national governments may be far worse than any by the attributing entity. *See* Eichensehr, *supra* note 114, at 530-31 (highlighting due process and privacy concerns stemming from attributions to particular individuals).

[149] *See, e.g.*, U.S. Dep't of Justice, *supra* note 38 (asserting that U.S. indictments "can make it more difficult for states to recruit the manpower and resources for cyber-attacks"). However, these tactics may backfire. *See America's Government Is Putting Foreign Cyber-Spies in the Dock*, ECONOMIST, Sept. 13, 2018, https://www.economist.com/united-states/2018/09/13/americas-

Another purpose public attributions serve is enabling so-called *deterrence-by-denial*—strengthening defenses to prevent attempted attacks from succeeding and thus convincing attackers that attacking is not worth the effort.[150] Attribution can bolster deterrence-by-denial by encouraging and enabling those responsible for network defense to better secure their systems.[151] This mechanism is particularly likely to work when the public attribution is accompanied by technical details that enable defensive actions. For example, a recent technical alert published by DHS "contain[ed] indicators of compromise . . . and technical details on the tactics, techniques, and procedures . . . used by Russian government cyber actors on compromised victim networks" and specifically noted that the alert aimed "to educate network defenders to enhance their ability to identify and reduce exposure to malicious activity."[152] Public attribution to a government is not necessary to enable such defenses, but it can be helpful.[153] Understanding who the attacker is can shed light on intruders' likely targets and goals. For example, a state is more likely to be interested in information with strategic and national security value—items unlikely to be of interest to run-of-the-mill cybercriminals seeking financial profit.

A third purpose of public attribution is *justifying responsive action*. This is perhaps obvious with respect to indictments and sanctions, which both identify specific objects of the charges or sanctions. It is, however, equally true of other responsive actions. As a matter of international law, a state that has suffered an internationally wrongful act may take countermeasures—actions that would be unlawful but for the prior unlawful act.[154] But an injured state may only take countermeasures against the state responsible for the internationally wrongful act,

---

government-is-putting-foreign-cyber-spies-in-the-dock (reporting that U.S. government hackers are concerned that U.S. indictments could prompt retaliation, such as arrests of U.S. government hackers).

[150] *See, e.g.*, MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 7 (2009), *available at* 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 136, 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.").

[151] *See, e.g.*, DAVIS II ET AL., *supra* note 22, at 16-17 ("[A] public attribution statement may encourage victims or other vulnerable populations to bolster network defenses."); Hunt, *supra* note 38 (explaining the U.K. strategy to accompany public attributions with details about "how [a cyber intrusion] was done, thereby helping the cyber security industry to develop protective measures"); Mandiant, *supra* note 117, at 6 (explaining publication of the APT1 report that attributed intrusions to China on the grounds that "we wanted to do our part to arm and prepare security professionals to combat that threat effectively").

[152] Dep't of Homeland Sec., *supra* note 56.

[153] *But see* Nye, *supra* note 136, at 54 (asserting that "deterrence by denial . . . is indifferent to attribution").

[154] *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 . . . .").

necessitating that the victim state identify the state responsible.[155] Such an attribution could be done privately,[156] but if so, the victim state would risk other states viewing its countermeasure as an initial wrongful act, rather than a lawful response. Thus, *public* attribution helps to ensure that other states, commentators, and the public more generally understand the tit-for-tat of states' actions and which states believe their actions are legally justified.

Finally, and somewhat relatedly, public attributions that are supported by evidence can help to *promote stability in and avoid conflict over cyberspace*. There is currently a lack of clarity about what states are actually doing in cyberspace. Such lack of clarity about facts is not unique to cyberattacks,[157] but it is exacerbated in the cybersecurity context because some cyberattacks do not cause observable real-world effects, state cyber capabilities are often classified, and even when attacks are observable, their technical aspects create barriers to public understanding. In some cases, the attribution of a cyberattack may provide the only indication to parties other than the victim that anything has happened.

Publicly providing evidence about state behavior can help not just to provide greater information about states' actions, but to foster *agreement* about the factual reality of what states are doing. Public disclosure of evidence allows for cross-checking or corroboration of attributions by both governmental and non-governmental actors, ensuring or potentially improving the accuracy of attributions.[158]

Development of international law, particularly customary international law, proceeds through the application by states of law to facts. The common understanding about factual reality that can come from public attributions enables states to undertake the process of applying principles to facts that leads to the creation of primary rules to govern state behavior either as norms or more robustly as customary international law.[159] As Martha Finnemore and Duncan Hollis have explained, attributions "serv[e] as an opening bid" and can "lay out the contours of

---

[155] *See id.* art. 49(1) ("An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act . . . ."); *see also* Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), 1997 I.C.J. 7, 52 (explaining that for a countermeasure to be lawful "it must be taken in response to a previous international wrongful act of another State and must be directed against that State").

[156] *See supra* note 137 (discussing private attributions).

[157] For example, the ICJ complained about the lack of agreement on and accessibility of factual evidence in the *Nicaragua* case. Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.), 1986 I.C.J. 14, 28 (para. 57) (noting that "[o]ne of the Court's chief difficulties in the present case has been the determination of the facts relevant to the dispute" because "there is marked disagreement between the Parties not only on the interpretation of the facts, but even on the existence or nature of at least some of them" and because some of the parties' conduct was conducted in secret).

[158] *See* Eichensehr, *supra* note 114, at 529-30 (discussing how public disclosure of attributions by companies promotes accountability for their accuracy).

[159] *Cf.* Lin, *supra* note 19, at 29 ("Determining factual reality—important as it is—is only the beginning of the attribution process from a policy perspective.").

'bad behavior' along with an argument about why, exactly, the behavior is undesirable"—an argument that other actors can then accept, reject, or accept in part.[160] Public attributions foster "interactions between the accuser, the accused, and third party audiences that—over time—may result in the creation of a new norm."[161] Translated into the language of customary international law, public attributions

> may serve as early evidence of a "usage"— that is, a habitual practice followed without any sense of legal obligation. If such accusations persist and spread over time, States may come to assume that these accusations are evidence of *opinio juris,* delineating which acts are either appropriate or wrongful as a matter of international law.[162]

To be sure, this process will not be quick or easy, but agreement on facts can help to shift disagreements into the realm of norms and law, and away from questions about simply who did what to whom.

Even absent or in advance of agreement on norms or law, there is value in having agreement on facts. States with divergent views about the permissible bounds of state behavior can nonetheless benefit from understanding how other states believe that norms or law apply to facts. Understanding the factual scenarios that other states will, for example, consider to violate international norms or international law promotes stability in the international system by helping states to tailor their actions to avoid what another state would perceive to be escalatory behavior.[163]

The purposes that attributors intend public attributions to serve can vary. And different purposes may require different levels of evidence, as discussed in the next Part.

---

[160] Finnemore & Hollis, *supra* note 9, at 10.

[161] *Id.* at 10-11. Finnemore and Hollis use the term "accusation" to encompass, among other things, what I discuss as public attributions. *Id.* at 4.

[162] *Id.* at 11-12.

[163] Goldsmith and Williams have acknowledged that public attributions "might also help generate a broader public understanding about Chinese hacking in the hope of galvanizing support among U.S. allies and the public for a diplomatic push against China." Goldsmith & Williams, *supra* note 142. They argue that these gains are "offset by the massive benefits reaped" by China. *Id.* But my argument focuses not just on the benefits of possible agreement among allies about application of law to facts. Rather, the factual clarity from public attributions helps to foster stability and to avoid conflict among cyberspace *adversaries* by making clear how states will apply law to facts and what behaviors they will regard as escalatory. Goldsmith and Williams make a separate point that "[p]ublic attribution via indictments and other mechanism without a material response . . . signal[s] to adversaries . . . that the United States is extraordinarily defenseless." *Id.* Although I am somewhat less pessimistic about the utility of public attributions alone, I generally agree that other actions are necessary. Public attributions are the starting point, not the end point, of beginning to limit hostile activity in cyberspace.

II. THE LAW OF ATTRIBUTION

Assuming that the technical side of cyberattack attribution is a surmountable challenge, the legal and policy aspects of attribution raise a number of questions. This Part addresses the extent to which attribution is currently governed by law and how international and domestic law interact. Although existing laws are somewhat unsettled and fragmentary, this Part argues that greater legalization of attribution at the international level will promote the goals that attribution is intended to achieve, particularly fostering stability in the international system.

A. International Law on Evidence-Giving & Attribution in General

International law on the standard of proof states must meet when accusing other states of internationally wrongful acts is unclear.[164] The law is most developed with respect to the high end of state action, namely the evidence a state needs to provide to justify forcible self-defense in response to a claimed armed attack. But even there, the law is unsettled.[165] For lesser internationally wrongful acts, international law remains very murky.

Some support exists for the idea that a state seeking to use force in self-defense must provide "clear and convincing" evidence that it has suffered an armed attack. The "clear and convincing" standard derives from suggestions in International Court of Justice (ICJ) opinions, as well as state practice.

Although the ICJ has held that the state claiming to act in self-defense bears the burden of proving that an armed attack occurred,[166] it has not explicitly determined the *standard* of proof that such a state must meet.[167] In the 2003 *Case Concerning Oil Platforms (Iran v. United States)*, Judge Rosalyn Higgins criticized the ICJ's lack of clarity on standards of evidence.[168] She noted that "in a case in which so very much turns on evidence, it was to be expected that the Court would

[164] Green, *supra* note 11, at 165 ("[I]nternational law does not have a clear benchmark against which the persuasiveness or reliability of evidence may be gauged for the purposes of attributing responsibility or assessing legal claims."); Mary Ellen O'Connell, *Evidence of Terror*, 7 J. CONFLICT & SEC'Y L. 19, 21 (2002) (lamenting the lack of "any well-established set of rules governing evidence in international law in general or in the case of self-defence in particular").

[165] *See* Green, *supra* note 11, at 163 ("[T]he evidentiary standards applicable to the law on the use of force, as with international law more generally, remain extremely unclear."); O'Connell, *supra* note 164, at 21 ("How much objective evidence is needed before responding with force [in self-defense to an armed attack] is largely an open question.").

[166] Case Concerning Oil Platforms (Iran v. United States), 2003 I.C.J. 161, 234 (para. 30) (separate opinion of Higgins, J.) ("That a litigant seeking to establish a fact bears the burden of proving it is a commonplace, well-established in the Court's jurisprudence." (internal citation omitted)).

[167] *See, e.g.*, Green, *supra* note 11, at 166 (noting that the ICJ "has avoided explicitly articulating a general standard with regard to its decisions" and "has employed different standards, depending upon the dispute before it"); Roscini, *supra* note 11, at 248 ("The ICJ has to date avoided clearly indicating the standards of proof expected from the litigants during the proceedings.").

[168] *Case Concerning Oil Platforms*, 2003 I.C.J. at 233 (para. 30) (separate opinion of Higgins, J.).

clearly have stated the standard of evidence that was necessary for a party to have discharged its burden of proof," but "neither here nor elsewhere does the Court explain the *standard* of proof to be met."[169] She critiqued the Court's prior opinions in *Corfu Channel* and *Military and Paramilitary Activities in and Against Nicaragua* as similarly unclear,[170] noting that in *Nicaragua*, "the Court did not even attempt to articulate the standard of proof it relied on, merely holding from time to time that it found there was 'insufficient' evidence to establish various points."[171] Higgins noted that "[b]eyond a general agreement that the graver the charge the more confidence must there be in the evidence relied on, there is . . . little to help parties . . . as to what is likely to satisfy the Court."[172]

The ICJ addressed the standard of proof more explicitly in the 2007 *Case Concerning Application of the Convention on the Prevention & Punishment of the Crime of Genocide (Bosnia & Herzegovina v. Serbia & Montenegro)*, which dealt with state responsibility for genocide.[173] The Court explained that "claims against a State involving charges of exceptional gravity must be proved by evidence that is fully conclusive."[174] In yet another verbal formulation, the Court explained that it must be "fully convinced" that genocide has occurred and that "[t]he same standard applies to the proof of attribution for such acts."[175] Although the *Genocide Convention* case did not address self-defense in particular, its evidentiary standard appears more broadly applicable, adjusting based on the gravity of the offense claimed.

While acknowledging and criticizing the ICJ's lack of definitive resolution of the standard of proof required in use of force cases, scholars have argued that the ICJ's case law supports an implied clear-and-convincing or clear-and-compelling evidence standard for self-defense.[176] Such a standard is less than the beyond-a-

---

[169] *Id.* at 234 (para. 30); *see also id.* at 286 (para. 41) (separate opinion of Buergenthal, J.) (critiquing the Court's opinion because it "never spells out what the here relevant standard of proof is" and querying "[w]hat is meant by 'insufficient' evidence? Does the evidence have to be 'convincing', 'preponderant', 'overwhelming' or 'beyond a reasonable doubt' to be sufficient?").

[170] *Id.* at 233-34 (para. 32).

[171] *Id.* at 233 (para. 32).

[172] *Case Concerning Oil Platforms*, 2003 I.C.J. at 233 (para. 33) (separate opinion of Higgins, J.)

[173] 2007 I.C.J. 47 (Feb. 26, 2007).

[174] *Id.* at 129 (para. 209).

[175] *Id.*; *see also id.* at 130 (para. 210) ("[T]he Court requires proof at a high level of certainty appropriate to the seriousness of the allegation.").

[176] *See, e.g.*, Green, *supra* note 11, at 172-73 (arguing that a close reading of the ICJ's decision in *Nicaragua* and *Oil Platforms* reveals "implicit standards of evidence," and specifically that the Court applies a "clear and convincing" standard of proof for claims of self-defense); O'Connell, *supra* note 164, at 24 (arguing that the ICJ's *Nicaragua* decision impliedly required convincing evidence); Roscini, *supra* note 11, at 249-50 (citing ICJ cases and arguing that "claims related to *jus ad bellum* violations . . . have been treated as requiring 'clear and convincing evidence.'"). *But see* Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILLANOVA L. REV. 569, 594 (2011) ("[I]nternational law sets no specific evidentiary standard for drawing conclusions as to the originator of an armed attack . . . ."); Tsagourias, *supra* note 19, at 235 ("International law does not lay down any specific standards of evidence with regard to issues involving the use of force or

reasonable-doubt standard employed in criminal law, and more than a preponderance of the evidence.[177] In essence, a "clear and convincing" standard requires "the party with the burden of proof . . . [to] convince the arbiter in question that it is substantially more likely than not that the factual claims that have been made are true."[178]

Scholars draw further support for the clear and convincing evidence standard from state practice, particularly U.S. practice.[179] Scholars have collected numerous examples of U.S. officials citing "'convincing' or 'compelling' evidence" to support forcible responses to terrorist attacks, including bombings of Libya in 1986, Iraqi intelligence headquarters in 1993, and Sudan and Afghanistan in 1998.[180] Perhaps most significantly, the United States appears to have deployed the clear-and-convincing standard to justify the use of force in self-defense after the 9/11 attacks.[181] In a letter to the President of the U.N. Security Council, then-U.S. Permanent Representative to the United Nations John D. Negroponte explained that the United States had "clear and compelling information" that Al Qaeda "had a central role in the attacks."[182] The "clear and compelling" phrasing similarly appeared in a statement by the NATO Secretary General confirming that NATO considered the 9/11 attacks to trigger NATO's collective defense provisions.[183] It is not clear, however, that the United States and NATO—to say nothing of states

---

self-defence."). It is unclear the extent to which an implicit "clear and convincing" evidence standard may have been disrupted by the Court's decision in *Case Concerning Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda), 2005 I.C.J. 168, which appears to use different evidentiary standards throughout the opinion. *See* Green, *supra* note 11, at 174-76 (detailing the ICJ's inconsistent use of evidentiary standards, including "clear and convincing," preponderance, and "prima facie evidence," in the *DRC v. Uganda* case).

[177] *See, e.g.*, Green, *supra* note 11, at 167 (explaining hierarchy of standards); Schmitt, *supra* note 176, at 595 ("'Clear and compelling' is a threshold higher than the preponderance of the evidence (more likely than not) standard used in certain civil and administrative proceedings and lower than criminal law's 'beyond a reasonable doubt.'").

[178] Green, *supra* note 11, at 167. Michael Schmitt equates the standard to a state's duty to act reasonably. Schmitt, *supra* note 176, at 595 ("In essence, it obliges a state to act reasonably, that is, in a fashion consistent with the normal state practice in same or similar circumstances. Reasonable states neither respond precipitously on the basis of sketchy indications of who has attacked them nor sit back passively until they have gathered unassailable evidence.").

[179] *See* Green, *supra* note 11, at 174 (noting the practice of the United States in apparently invoking a clear and convincing standard to justify its use of force in self-defense and arguing that the standard may "be an accurate reflection of an embryonic formalist approach to evidence with regard to self-defence claims more generally").

[180] O'Connell, *supra* note 164, 25-27; *see also* Green, *supra* note 11, at 174.

[181] *See* Roscini, *supra* note 11, at 241-42 (discussing U.S. practice with respect to 9/11); Schmitt, *supra* note 176, at 594-95 (same).

[182] John D. Negroponte, Letter Dated 7 Oct. 2001 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, U.N. Doc. No. S/2001/946, *available at* http://repository.un.org/bitstream/handle/11176/31401/S_2001_946-EN.pdf.

[183] Statement by NATO Secretary General, Lord Robertson, Oct. 2, 2001, https://www.nato.int/docu/speech/2001/s011002a.htm.

outside that bloc—regard provision of clear and convincing evidence to be a matter of legal obligation. That is, while there is some state practice to support a clear and convincing evidence standard, it is unclear whether there is *opinio juris* as required for customary international law.[184]

While the ICJ and state practice lend some clarity to the evidentiary standard for uses of force, the standard for lower level actions is even less clear. The International Law Commission's Articles on State Responsibility, the most authoritative treatment of state responsibility and, relatedly, countermeasures, does not address evidentiary issues. The Articles explicitly set aside evidentiary questions, noting, in the commentary, that "[q]uestions of evidence and proof of such a breach [of an international obligation] fall entirely outside the scope of the articles."[185] For its part, the ICJ has only suggested that evidentiary standards vary along a sliding scale based on the severity of the offense.[186] If the most serious international offenses, such as armed attacks and genocide, must be proven by clear and convincing evidence,[187] then presumably the standard for lesser wrongs is lower. But how much lower?

State practice in the cybersecurity context provides little additional clarity. Both the United States and the United Kingdom have made statements about the evidence question. The United States has taken the position that in the absence of explicit international law on the standard of proof, "international law generally requires that States act reasonably under the circumstances."[188] The United Kingdom has said only that "the victim state must be confident in its attribution of that act to a hostile state before it takes action in response."[189]

Turning from what states say to what they do, the practice of state cyberattack attributions described in Part I could lend additional clarity to the evidentiary standard. However, there has been significant variance in the amount of evidence states adduce when attributing cyberattacks. When the United States first

---

[184] *See infra* note 201 and accompanying text (discussing the requirements for customary international law).

[185] Int'l Law Comm'n, *supra* note 27, at 54 (para. 4); *see also id.* at 72 (para. 8) (noting that the Articles "do not deal with issues of evidence or the burden of proof"); *see* also Egan, *supra* note 107, at 177 ("The law of state responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution.").

[186] *See Case Concerning Application of the Convention on the Prevention & Punishment of the Crime of Genocide* (Bosnia & Herzegovina v. Serbia & Montenegro), 2007 I.C.J. 47, 130 (Feb. 26, 2007) (para. 210) (noting that when a state is accused of genocide "the Court requires proof at a high level of certainty appropriate to the seriousness of the allegation").

[187] *See id.* at 129 (para. 209) ("[C]laims against a State involving charges of exceptional gravity must be proved by evidence that is fully conclusive.").

[188] Egan, *supra* note 107, at 177. The *Tallinn Manual* provides additional gloss on the meaning of reasonableness: "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." TALLINN MANUAL 2.0, *supra* note 8, at 81-82.

[189] Wright, *supra* note 108.

attributed the Sony attack to North Korea, it released very limited evidence, contained in its entirety in an FBI press release.[190] Some states appeared to accept the attribution, issuing statements that denounced North Korea's actions.[191] But some in the cybersecurity community publicly doubted the attribution,[192] criticizing the U.S. government for providing limited and questionable evidence of North Korea's involvement.[193] In response, the FBI released slightly more detailed evidence, citing operational errors by the hackers that revealed their use of Internet Protocol addresses used solely by North Korea.[194]

Other attributions have included more details. Attributions-by-indictment in particular have been quite detailed, as have attributions-by-alert.[195] The WannaCry attributions, initially done through official statements,[196] were less detailed, but a subsequent indictment provided additional information.[197] Among the most detailed attributions to date were those to the GRU in October 2018. There, the Dutch investigation produced significant evidence due to the physical location of the Russian government operatives in the Netherlands,[198] and the U.S. indictment provided considerable detail, particularly with respect to the targeting of worldwide anti-doping organizations.[199]

---

[190] FBI, *supra* note 57 (citing as evidence supporting its attribution to North Korea, "similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks" to attacks known to have been carried out by North Korea, as well as "significant overlap between the infrastructures used" in the Sony hack and prior attacks "linked directly to North Korea").

[191] *See, e.g.*, Rt. Hon. Philip Hammond, Foreign & Commonwealth Off., Foreign Secretary Responds to FBI Reports into Cyber Attacks on Sony Pictures, Dec. 19, 2014, https://www.gov.uk/government/news/foreign-secretary-responds-to-fbi-reports-into-cyber-attacks-on-sony-pictures ("I unequivocally condemn these cyber attacks [on Sony] and am deeply concerned at the findings of the US investigation, which seems to provide further evidence of North Korea's blatant disregard for international norms and obligations.").

[192] *See, e.g.*, Bruce Schneier, *Did North Korea Really Attack Sony?*, ATLANTIC, Dec. 22, 2014, https://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/ ("I am deeply skeptical of the FBI's announcement on Friday that North Korea was behind last month's Sony hack. The agency's evidence is tenuous, and I have a hard time believing it.").

[193] *See, e.g.*, Jack Goldsmith, *The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance*, Dec. 19, 2014, https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance (noting that "the 'evidence' is of the most conclusory nature" and "on its face . . . shows only that this attack has characteristics of prior attacks attributed to North Korea," and raising the possibility that "some other nation is spoofing a North Korean attack").

[194] James B. Comey, Director, FBI, Addressing the Cyber Security Threat, International Conference on Cyber Security, Fordham University, New York, NY, Jan. 7, 2015, https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

[195] *See* Rid & Buchanan, *supra* note 22, at 27-28 (describing the 2014 PLA indictment as "exceptionally detailed," and noting that despite the fact that it "did not reveal a great amount of attributive evidence[,] . . . [t]he subtext was that the government could produce such specific IP addresses, emails, malware samples, and stolen documents").

[196] *See supra* notes 73-75 and accompanying text.

[197] *See supra* note 76 and accompanying text.

[198] *See supra* notes 87-90 and accompanying text.

[199] *See supra* notes 91-92 and accompanying text.

As a matter of customary international law, looking to state practice among the states that do state-to-state attribution of cyberattacks might suggest an emerging requirement to give at least *some* evidence.[200]

However, the U.S. and U.K. statements about attribution and evidentiary standards seem precisely designed to block the development of customary international law by denying the existence of one of the two requirements for custom. Customary international law requires both "general and consistent" state practice and *opinio juris*—that the state practice is undertaken out of a "sense of legal obligation."[201] Both states, plus France, have explicitly stated that international law does not require a state to reveal the evidence on which an attribution is based.[202] Deeming the decision to release evidence a mere "policy choice"[203] ensures that the recent U.S. and U.K. practice of giving at least *some* evidence to support attributions cannot be cited as having been done out of a sense of legal obligation.[204] In short, although their actions might begin to demonstrate consistent state practice, their words deny the existence of the *opinio juris* required for customary international law.

---

[200] *See* Efrony & Shany, *supra* note 111, at 635 ("Attribution claims constitute part of state practice, and they divulge, at times, *opinio juris.* Thus, they may generate international law . . . ."); *see also* Finnemore & Hollis, *supra* note 9, at 24 ("Where States are specially affected—either because they possess cyber operation capabilities that others do not, or because they have been the victim of cyber operations—international law may actually require the community of States to pay particular attention to their views on the state of customary international law."). Similarities in the types of evidence cited across different attributions might also suggest practical convergence on the *nature* of evidence required. For example, multiple indictments cite information about hackers' working hours as evidence of their location. *See, e.g.*, Indictment, *supra* note 29, at 12-13 (discussing how hackers' activity corresponded to working hours in Shanghai); Indictment, *supra* note 95, at 14 (noting that the defendants "typically engaged in hacking operations during working hours in China").

[201] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) & cmt. c (1987); *see id.* cmt. C ("[A] practice that is generally followed but which states feel legally free to disregard does not contribute to customary law.").

[202] *See* Egan, *supra* note 107, at 177 ("[T]here is *no* international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action."); Ministère des Armées, *supra* note 110, at 11 (noting that international law does not require disclosure of evidence supporting an attribution) (author's translation); Wright, *supra* note 108 ("There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based . . . ."); *see also* Dan Efrony, *Entering the Third Decade of Cyber Threats: Toward Greater Clarity in Cyberspace*, LAWFARE, June 13, 2019, https://www.lawfareblog.com/entering-third-decade-cyber-threats-toward-greater-clarity-cyberspace (noting that Wright's speech "negated . . . the obligation to disclose evidence justifying attribution").

[203] Egan, *supra* note 107, at 177.

[204] Int'l Law Comm'n, Draft Conclusions on Identification of Customary International Law with Commentaries, U.N. Doc. No. A/73/10, at 141 (2018, *available at* http://legal.un.org/docs/?path=../ilc/texts/instruments/english/commentaries/1_13_2018.pdf&lang=EF ("[T]he effect of practice in line with the supposed rule [of customary international law] may be nullified by contemporaneous statements that no such rule exists.").

B. Legalizing Cyberattack Attribution

Attribution should be governed by law, not treated merely as a matter of policy. To be sure, the decision of whether to make an attribution public is partly a political one—a victim state need not announce that it has been attacked or identify the perpetrator.[205] But when states do publicly attribute cyberattacks, how such attributions occur should not be left to policy. The next two subsections explain why law, not just policy, should govern the evidentiary standard for public attribution of cyberattacks and propose a customary international law standard for the amount of evidence states should provide.

1. Why Legalize?

At least for cyberattacks that do not rise to the level of an armed attack, the U.S., U.K., and French position that international law does not currently require evidence-giving appears to be correct. But that merely raises the question of whether international law *should* have such a requirement.

Given that the United States and other Western countries now typically give evidence to support public attributions, the question of whether to establish a legal standard to require such evidence-giving may seem superfluous. However, the reason states provide evidence—policy choice versus legal requirement—has significant consequences. Characterizing a practice as merely a matter of policy means that it can be changed at any time by the states that currently provide evidence, and other states that might begin to make public attributions could totally disregard it. Practices undertaken as a matter of legal requirement, on the other hand, are stickier. For states that recognize the legal obligation, changing practice would require a change in legal position that may be difficult or impossible to square with its past legal views.[206] And invoking a legal obligation to provide evidence also constitutes a normative claim about the appropriate behavior of *other* states.[207] States are under no obligation to agree with or abide by one another's policy choices, but

[205] *Cf.* Wright, *supra* note 108 ("There is no legal obligation requiring a state . . . to publicly attribute hostile cyber activity that it has suffered in all circumstances.").

[206] *Cf.* Rebecca Ingber, *The Obama War Powers Legacy and the Internal Forces That Entrench Executive Power*, 110 AM. J. INT'L L. 680, 684 (2016) ("[W]hen the administration takes a legal position, it is saying that it is bound to take or not to take a particular action, and bound by some external or fixed source. When the administration takes a policy position, it is saying that it has discretion to act in a variety of ways (within the bounds of the prior legal position) but that it is choosing to act in accordance with this particular policy pronouncement." (internal citation omitted)).

[207] *See* Pierre-Hugues Verdier & Erik Voeten, *Precedent, Compliance, and Change in Customary International Law: An Explanatory Theory*, 108 AM. J. INT'L L. 389, 411 (2014) ("[W]hen a state declares that a CIL rule exists, it signals its intent . . . to apply the rule consistently and universally and to expect others to do so as well.").

customary international law is a different matter. Once established, it binds all states, even those that did not specifically consent to its formation.[208]

Relegating evidence-giving to the policy category, as the United States, United Kingdom, and France have done, risks legitimizing future evidence-free attributions by those states or others. Such "trust us" attributions are problematic for any number of reasons. They may be false. They will be difficult to corroborate (or debunk) because of the lack of supporting evidence. They may foster greater consolidation of blocs with respect to Internet governance and cybersecurity issues because "trust us" will only work with allies. And they may skew the development of primary norms of state behavior. To understand how such skewing could occur, consider the following hypothetical: The power grid in a major State A city goes down. State A quickly and without providing evidence attributes the outage to a cyberattack by State B. Although the accusation is false, State A then uses the attribution, which State B cannot refute because of the lack of evidence to debunk, to claim that power grids are legitimate targets for cyberattacks. Establishment of an evidentiary standard may not stop State A from making a false accusation, but State A's failure to comply with the established evidentiary standard should make other states reluctant to credit State A's attempt to establish a permissive rule allowing targeting of power grids based on State B's practice.

From a purely self-interested perspective, perpetrator states should see value in requiring accusers to support their accusations.[209] This category undoubtedly includes the United States and United Kingdom, which are active players in cyberspace, and as such, are likely to be on the receiving end of attributions at some point.[210] States that are active in cyberspace can be accused of all manner of activity for which they are *not* responsible, and could have difficulty refuting such accusations because of the lack of supporting evidence to debunk. The requirement to provide evidence to support accusations acts as a deterrent to untruthful or ill-founded accusations.[211]

---

[208] Customary international law's universality is one of the "design features" that make it an attractive alternative to both treaties and soft law in certain circumstances. *See* Laurence R. Helfer & Ingrid B. Wuerth, *Customary International Law: An Instrument Choice Perspective*, 37 MICH. J. INT'L L. 563, 568-72 (2016).

[209] Of course, a perpetrator state might wish to keep knowledge of its tactics confined to as few people or entities as possible and thus prefer that even if a victim state discovers the identity of the attacker, the victim remain silent, rather than making a public attribution. But on the other hand, a perpetrator state might prefer to know what the victim knows, which would come out in the evidence given to support a public attribution. Knowing that certain techniques have been discovered and can be traced to the attacking state may have value in itself. The weighing of these competing values is difficult in the abstract and may change depending on the circumstances of particular activities.

[210] Arguably, the United States already has been, though not explicitly. *See supra* note 135 and accompanying text (discussing Kaspersky Lab's attributions to the "Equation Group"); *see also* ROMANOSKY & BOUDREAUX, *supra* note 41, at 27-28 (speculating about possible reasons for low rates of attribution to the U.S. government).

[211] Even a requirement to provide evidence is not a fool-proof deterrent. Evidence can be faked. *See, e.g.*, Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy*,

Given these downsides, why then would the United States and United Kingdom resist legalizing the evidentiary standard for attribution? Neither state has explained its reasoning in detail. The most likely explanations do not withstand scrutiny, however, and other incentives should counsel in favor of developing a legal standard.

First, governments often invoke the need to protect intelligence sources and methods. The United States in particular appeared concerned on this score when it initially attributed the Sony hack to North Korea with little public evidence.[212] Concern about sources and methods is undoubtedly legitimate, and the need to preserve sources and methods may mean that in some cases, states will not make public attributions. At the same time, however, the detailed attributions that the United States has made show that in many cases, it is possible to develop evidence without disclosing classified information, or while disclosing only enough information that the benefits of the attribution outweigh the costs of disclosure. The detailed evidence in the non-governmental attributions further shows that *government* sources and methods are not necessarily required for attributions. Drawing on non-governmental information and attributions may provide governments with an alternative to revealing their own classified sources and methods.

Second, the United States and United Kingdom may fear that a legal requirement to provide evidence would require more evidence than they and other attributing allies currently provide as a matter of policy. But the best way to ensure that does not come to pass is to use their first-mover advantage to stake out a claim about what the legal standard should be.[213] If the United States and United Kingdom fail to take the lead and use the attributions they make to set the evidentiary standard, they run the risk of having a legal standard set for them. The standard could be set by other states that get into the attribution business and announce evidentiary standards or successfully advocate for such standards in international fora.[214] Or the standard could be set indirectly by non-governmental attributors in a sort of "cyber *CSI* effect."[215] Pursuant to the so-called "*CSI* effect," the portrayal of high-tech investigations in shows like *CSI* has allegedly caused jurors in real-life criminal trials to have unreasonable expectations about the kinds and amount of evidence

---

Democracy, and National Security, 107 CAL. L. REV. __ (forthcoming 2019), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 (discussing the pernicious possible effects of deep fake video and audio recordings).

[212] *See* FBI, *supra* note 57 (noting that "the need to protect sensitive sources and methods precludes us from sharing all of this information" to support the attribution).

[213] *Cf.* Ashley S. Deeks, *Predicting Enemies*, 104 VA. L. REV. 1529, 1589-90 (2018) (urging the United States to be transparent about its legal and policy decisions on military use of algorithms in order to shape the direction of international law in the area).

[214] *See infra* notes 268-269 and accompanying text (discussing U.N. General Assembly resolutions).

[215] *See* Kristen Eichensehr, *Risky Business: When Governments Do Not Attribute State-Sponsored Cyberattacks*, NET POLITICS, Oct. 4, 2016, https://www.cfr.org/blog/risky-business-when-governments-do-not-attribute-state-sponsored-cyberattacks (proposing the "cyber *CSI* effect").

prosecutors can produce.[216] Non-governmental attribution reports could have a similar effect: the non-governmental parties' practice of publishing detailed evidence to support their attributions of cyberattacks to governments may shape public and states' expectations about the type and amount of evidence that governments should supply when making similar accusations. Non-state practice cannot, of course, directly create customary international law,[217] but non-governmental practice can shape expectations about evidence that, as a practical matter, states may be forced to meet if they wish their attributions to be believed. By foregoing the opportunity to set a legal standard through their attribution practice, the United States and United Kingdom risk having a higher standard set for them as a matter of norms and accepted practice.

Third, with respect to other cybersecurity-related issues, treaties or other agreements on state behavior have been hampered by problems of verification. The United States, among others, has rejected the idea of a cybersecurity treaty to hem in state behavior because of the inability to verify other states' compliance.[218] If deviations cannot be detected reliably, then agreeing to legal rules will restrict the freedom of action of law-abiding states, while doing nothing to restrict the actions of scofflaw states. But this concern does not apply to setting a legal requirement for evidence-giving. Compliance with a legal requirement to provide evidence to support public attributions requires transparency and publicity. Compliance with the standard is defined by disclosure, and so violation of the requirement is comparatively easy to monitor.

Finally, working for the progressive development of law to require evidence to support attributions could have significant positive systemic effects, supporting stability and helping to avoid conflict over cyberspace. Evidentiary rules are secondary rules,[219] but establishing evidentiary rules for attributions would help to

---

[216] *See, e.g.*, Tom R. Tyler, *Viewing CSI and the Threshold of Guilt: Managing Truth and Justice in Reality and Fiction*, 115 YALE L.J. 1050, 1052 (2006) (describing the "CSI effect" as occurring when "people who watch the series develop unrealistic expectations about the type of evidence typically available during trials, which, in turn, increases the likelihood that they will have a 'reasonable doubt' about a defendant's guilt").

[217] *See* Int'l Law Comm'n, *supra* note 204, at 130 (noting that assessing the existence of "a general practice" for purposes of customary international law "refers primarily to the practice of States" and sometimes to "the practice of international organizations," while "[c]onduct of other actors is not practice that contributes to the formation, or expression, of rules of customary international law, but may be relevant when assessing the practice" of states). *But see id.* at 131 (explaining that in some circumstances the conduct of non-state and non-international organization entities like corporations "may have an indirect role in the identification of customary international law, by stimulating or recording the practice and acceptance as law (*opinio juris*) of States").

[218] *See, e.g.*, Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INST. (2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf (discussing hurdles, including verification, to cybersecurity treaties).

[219] *See* H.L.A. HART, THE CONCEPT OF LAW 94 (3d ed., 2012) (explaining that "while primary rules are concerned with the actions that individuals must or must not do, these secondary rules are all concerned with the primary rules themselves" and determine, among other things how violation of primary norms can be "conclusively determined").

foster the establishment of primary rules about acceptable state behavior in cyberspace—an avowed goal of the United States and its allies.[220] This point may seem counterintuitive. Setting a legal requirement for evidence-giving raises the cost to states of making an attribution, which might suggest that states will make fewer public attributions. It is certainly possible that requiring evidence-giving or setting an evidentiary standard for attributions could decrease the absolute number of attributions. States and private parties may not be able to meet the evidentiary standard in some cases and so will refrain from making a public attribution that they would make absent an evidentiary standard.[221]

But setting the secondary rules of evidence may also increase the benefits of making a public attribution. Clarity about the amount and nature of evidence that other states and the cybersecurity community will expect for a credible attribution changes the calculus for states considering the costs of revealing sources and methods necessary to disclose evidence. In essence, clarity about the evidentiary standard helps to ensure that states undertaking the costs of disclosure will obtain the benefit of being believed by relevant actors.[222] Clarity about the evidentiary standard could change the calculus for non-governmental attributors as well. Although non-governmental parties are not directly bound by international law and thus wouldn't be required to comply with the evidentiary standard, meeting the standard could lend credibility—and consistency[223]—to the attribution practices of companies and other non-governmental attributors as well. Clarity about what an attributor must do to obtain the benefits of attributions may spur additional attributions.

In any event, even if setting an evidentiary standard decreases the total number of public attributions, having fewer *credible* attributions is preferable to a greater number of ill-founded or unfounded attributions. For purposes of promoting knowledge about states' behavior and development of norms to govern it, public attributions must be accurate and credible. Deterring unsubstantiated attributions is a

---

[220] *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 8, at 80 ("Primary rules are those that set forth international law obligations. Breach of them results in State responsibility. Secondary rules lay out the general conditions for a State's responsibility, as well as the consequences of violating a primary rule."); Int'l Law Comm'n, *supra* note 27, at 31 (distinguishing between the primary rules that "define the content of international obligations, [and] the breach of which gives rise to responsibility" and "the secondary rules of State responsibility").

[221] Setting an evidentiary standard may differentially affect states, making it more difficult for states that have less sophisticated cyber capabilities to make public attributions. This possibility does not undermine the need for an evidentiary standard, but it does highlight one important role an international entity for cyberattack attributions could play, namely, ensuring that less sophisticated victims have access to *pro bono* assistance in investigating cyberattacks. *See infra* notes 295-297 accompanying text (discussing the role of an international entity in assisting victims).

[222] *Cf.* Efrony & Shany, *supra* note 111, at 636 (making the converse point that currently "[t]he legal uncertainty surrounding the attribution process may also tip the balance, at times, toward maintaining silence and ambiguity concerning cyberoperations"); *see also infra* note 270 and accompanying text (discussing how the proposed evidentiary standard can level the playing field for provision of evidence).

[223] *See infra* note 294 and accompanying text (discussing a new attribution entity as a way to standardize private attributors' methodologies).

feature, not a bug, of creating a customary international law standard for evidence to support public attribution of state-sponsored cyberattacks.

2. Law for Cyberattack Attribution

If evidentiary standards for attribution should be *legal* standards, which law should do the work—domestic or international? Although domestic legal standards currently govern some attributions, this Section argues that such standards are insufficient, and international law must be developed. What may begin as *lex specialis* on evidence for cyberattack attributions has the potential to crystallize the murky *lex generalis* of international law on evidence.

i. The Insufficiency of Domestic Law

Some of the mechanisms that the United States uses for attributions are already governed by U.S. domestic legal standards. The role of domestic law is clearest with respect to attributions-by-indictment. Federal prosecutors present evidence to a grand jury, which "may return an indictment if there is probable cause to believe that a crime has been committed by the persons indicted."[224] A grand jury need not be convinced beyond a reasonable doubt that the defendant has committed a crime, but only that there is probable cause to believe that the defendant has committed the crime alleged.[225] The U.S. Supreme Court has explained that probable cause "is not a high bar: It requires only the kind of fair probability on which reasonable and prudent [people,] not legal technicians, act."[226]

---

[224] CHARLES ALAN WRIGHT ET AL., FED. PRAC. & PROC. CRIM. § 111 (4th ed.); *see also* U.S. DEP'T OF JUSTICE, JUSTICE MANUAL, § 9-11.101 (2018), *available at* https://www.justice.gov/jm/jm-9-11000-grand-jury#9-11.101 ("[T]he grand jury's principal function is to determine whether or not there is probable cause to believe that one or more persons committed a certain Federal offense within the venue of the district court.").

[225] *See* Admin. Off. U.S. Courts, Handbook for Federal Grand Jurors 5, http://www.ndd.uscourts.gov/jury/jury_handbook_grand_jurors.pdf (last visited Sept. 12, 2019) ("[T]he grand jury is not responsible for determining whether the accused is guilty beyond a reasonable doubt, but only whether there is sufficient evidence of probable cause to justify bringing the accused to trial."). If the grand jury returns an indictment, the prosecutor then chooses whether to sign it and proceed with the case, which would ultimately be determined based on the usual criminal standard of beyond a reasonable doubt. *See* WRIGHT ET AL., *supra* note 224, at § 101 (explaining that prosecutors have "ultimate veto power over a grand jury decision to indict"); U.S. DEP'T OF JUSTICE, *supra* note 224, § 9-27.200-.250, *available at* https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution#9-27.200 (discussing considerations prosecutors must take into account in deciding whether to proceed with a prosecution).

[226] Kaley v. United States, 571 U.S. 320, 338 (2014) (alteration in original; internal quotation marks omitted); *see also* Illinois v. Gates, 462 U.S. 213, 231-32 (1983) (discussing probable cause and noting that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules"). Although the U.S. indictments are among the most detailed attributions, the ICJ, for its part, has discounted the value of indictments in establishing international legal responsibility in other contexts. *See Case Concerning Application of the Convention on the Prevention & Punishment of the Crime of*

The standard for imposition of economic sanctions is also low. In consultation with other departments, the Treasury Department can impose sanctions if there is a "reasonable basis to determine that the target meets the criteria for designation" under the relevant statutory and administrative scheme.[227] The executive branch "acts as the functional prosecutor, fact finder and review board," subject only to highly deferential review by courts.[228] A court reviewing a designation "appl[ies] the [Administrative Procedure Act's'] 'highly deferential standard,' meaning that [it] may set aside Treasury's action only if it is 'arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.'"[229]

One might think that domestic law standards are sufficient to govern attributions. In particular, attributions are in many ways like indictments—they are essentially accusations of wrongdoing—so the probable cause standard might approximate the standard one would want international law to uphold. But although the domestic law standards are currently doing some of the work that an international law requirement for evidence-giving would do, they are insufficient.

Even in the United States, not all of the attribution mechanisms are governed by legal standards, and states are under no obligation to select ones that are. Attributions-by-alert often use "estimative language" from the intelligence community, deploying standards that are not legally defined or reviewable in court.[230] For example, a report by the U.S. Office of the Director of National

---

Genocide (Bosnia & Herzegovina v. Serbia & Montenegro, 2007 I.C.J. 47 (Feb. 26, 2007) (para. 217) (explaining that because "the claims made by the Prosecutor in the indictments are just that—allegations made by one party . . . , as a general proposition the inclusion of charges in an indictment cannot be given weight").

[227] Testimony of Daniel L. Glaser, Deputy Asst. Sec'y (Terrorist Financing and Financial Crimes), U.S. Dep't of the Treasury, Before the House Comm. on Fin. Servs. Subcomm. on Oversight and Investigations, at 5, May 26, 2010, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FINAL%20GLASER%20TESTIMONY%20ON%20CHARITIES%205-26-2010%20edited%20PDF.pdf; *see also id.* at 4-5 (describing the designation process).

[228] Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 340 (2014); *see also id.* at 341 & n.71 (noting that while most courts have upheld designations based on a "'reasonable relation' between the facts in the record and the designation determination," a few have required probable cause).

[229] Zevallos v. Obama, 793 F.3d 106, 112 (D.C. Cir. 2015); *see* Holy Land Found. for Relief & Dvpt. v. Ashcroft, 333 F.3d 156, 162 (D.C. Cir. 2003) (explaining that "if the [Treasury Department Office of Foreign Asset Control]'s actions were not arbitrary and capricious, and were based on substantial evidence, [the court] must affirm" the designation); *see also Zevallos*, 793 F.3d. at 109-10 (noting that although the case at hand involved the Foreign Narcotics Kingpin Designation Act, the same procedures apply to all designations, including those pursuant to the International Emergency Economic Powers Act).

[230] *See* U.S. NATIONAL INTELLIGENCE: AN OVERVIEW 2011, at 59-60 (2011) (providing an overview of "estimative language" used by the intelligence community); *see also* Office of the Dir. of Nat'l Intell., Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution 2, Jan. 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf ("Intelligence Community judgments often include two important elements: judgments of how likely it is that something has happened or will happen (using terms such as 'likely' or 'unlikely') and confidence levels in those judgments (low,

Intelligence on Russian election interference notes that the intelligence community "assess[es] with *high confidence* that the GRU relayed material it acquired from the DNC and senior Democratic officials to WikiLeaks."[231] Other governments use the same estimative language.[232] Attributions by press release or official statement may not articulate any standard at all.

Even if states relied solely on mechanisms governed by their domestic legal standards, domestic law would still be insufficient to govern attributions. States' domestic legal standards for things like criminal charges vary. In some countries, the standard for a criminal charge is very low. Moreover, existing domestic legal standards for attributions governed by such standards are not in practice subject to judicial review as they are in more run-of-the-mill cases. In the United States, indictments and sanctions are generally subject to at least some post hoc judicial review, but attributions-by-indictment or other mechanisms have generally escaped judicial review because the defendants are not in U.S. custody and have not appeared in U.S. courts to challenge sanctions.[233] These kinds of attributions may also serve as the predicate to countermeasures—responsive actions against an aggressor state that would violate international law but for the aggressor's prior wrongful act;[234] such countermeasures have also not been subject to judicial review.

In addition, even for the United States, one could reasonably argue that domestic law standards of probable cause for an indictment and reasonable basis for sanctions are insufficient when what is at stake is an accusation of wrongdoing by a foreign government. The domestic legal standards are tied to due process protections for the individuals and entities subject to indictment or sanctions, and as a matter of U.S. constitutional law, the standards are understood as sufficient to serve that purpose. But the attributions-by-indictment and attributions-by-sanctions are serving multiple purposes, and at least arguably, the dominant one is communicating to

---

moderate, and high) that refer to the evidentiary basis, logic and reasoning, and precedents that underpin the judgments."). ODNI's Guide to Cyber Attribution defines "high confidence" as "when analysts judge the totality of evidence and context to be beyond a reasonable doubt with no reasonable alternative," and defines "moderate confidence" as "when analysts judge the totality of the evidence and context to be clear and convincing, with only circumstantial cases for alternatives." Office of the Dir. of Nat'l Intell., *supra* note 38, at 4. Despite echoing the language of legal standards, it is not clear that these standards as used by the intelligence community mean the same thing as the same linguistic formulations used in courts. In any event, the intelligence community assessments are not subject to judicial review.

[231] Office of the Dir. of Nat'l Intell., Assessing Russian Activities and Intentions in Recent US Elections 3, Jan. 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf (emphasis added).

[232] *See, e.g.*, U.K. National Cyber Security Centre, *supra* note 93 (noting that the U.K. National Cyber Security Centre "assess[es] with *high confidence* that the GRU was *almost certainly* responsible" for the 2016 hack of the DNC and subsequent release of stolen documents).

[233] *But see* Raman, *supra* note 38 (asserting that cybercrime charges are "brought only when the facts and law justify" them and "we can prove them in a courtroom, using admissible evidence, at proof beyond any reasonable doubt").

[234] *See supra* note 155 (discussing requirements for countermeasures).

foreign governments what constitutes unacceptable behavior in cyberspace.[235] Domestic law sets a floor, but the amount of evidence necessary to satisfy constitutional due process may well be insufficient to serve the alternative purpose of fostering norms and customary international law about state behavior in cyberspace. Domestic and international evidentiary standards would not conflict in this circumstance; rather the international law evidentiary standard would simply require *more* detail and evidence in indictments that accuse foreign governments of cyberattacks.[236]

Additionally, reliance on varied domestic law standards to govern attributions is unlikely to generate consensus among states about how attributions should be made. For issues related to the permissibility (or not) of state behavior vis-à-vis other states, there is significant value in having *agreed* legal standards. 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.[237] That is the domain of international law.

ii. Customary International Law for Evidence-Giving & Attribution

The turn to international law raises a familiar dilemma in the cybersecurity context and in circumstances of new technologies more broadly about the extent to which the best approach is to apply general, existing international law or instead to develop new law.[238] 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.

What then should international law say about evidence to support cyberattack attributions?

---

[235] *Cf.* Finnemore & Hollis, *supra* note 9, at 10 (noting that public attributions "lay out the contours of 'bad behavior' along with an argument about why, exactly, the behavior is undesirable").

[236] There is an obvious workaround for instances in which a state seeks to indict or sanction an individual who engages in cyberattacks on behalf of a foreign state: indict or sanction the individual without naming the state. The indicting or sanctioning state could still apply its domestic law to the accused individual when it cannot meet the proposed international law evidentiary standard. This may seem like a formalism, but the distinction is important. Only the acts of states determine customary international law, so without an allegation of state involvement, the indictment or sanctions can be severed from the process of setting primary norms of international law. It remains simply a routine exercise of a state's law enforcement authority.

[237] *See supra* note 206 and accompanying text.

[238] *See* Eichensehr, *supra* note 10, at 358 (terming this the "international law step-zero question"); *see generally* Rebecca Crootof, *Regulating New Weapons Technology*, *in* NEW TECHNOLOGIES AND THE LAW OF ARMED CONFLICT (Eric Talbot Jensen ed., forthcoming 2019), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195980 (discussing various factors for determining when new international law is required to regulate new weapons technologies).

For the very high end of state action, namely forcible self-defense, some state practice supports a requirement that a victim state must meet a clear and convincing or clear and compelling evidence standard.[239] For cyberattacks that reach the level of an armed attack, states contemplating responsive actions would be governed by this standard, to the extent that it is a customary international law requirement. Setting a high standard for attributions involving the most severe cyberattacks would be consistent with the ICJ's suggestion of a sliding scale of evidence based on the severity of the offense: an attribution of a cyber armed attack to a state requires the strongest evidentiary basis.[240] The *Tallinn Manual* endorses a similar sliding scale approach, arguing that "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 (such as retorsion, countermeasures, a plea of necessity, and self-defence) grows commensurately with the seriousness of a breach."[241]

Adopting a sliding scale of evidence based on the severity of the cyberattack and anticipated response provides some guidance for the ends of the scale. But it provides little clarity for everything in between—the space where the vast majority of cyberattacks occur. Such attacks would fall within the countermeasures framework, and as explained above, there is no consensus on the evidentiary standards governing states' use of countermeasures beyond a very general requirement to act reasonably.[242]

Moreover, the sliding scale approach, at least as justified by the ICJ and the *Tallinn Manual*, relies entirely on *one* possible purpose of attribution, namely justifying responsive action. It says nothing about the quantum of evidence that might be required for *other* purposes attributions might serve, and it does not consider the extent to which an absolute evidentiary minimum standard might be required for such other purposes.

Take the systemic purpose of promoting stability in and avoiding conflict over cyberspace. To serve this purpose, attributions should be accompanied by at least *some* evidence. Unsubstantiated attributions do not promote stability, and they may in fact undermine it by creating chaos and increasing the risk of escalation of conflict among states. To foster stability, the amount of evidence should be sufficient

---

[239] *See supra* notes 166-183 and accompanying text.

[240] *See* Case Concerning Application of the Convention on the Prevention & Punishment of the Crime of Genocide (Bosnia & Herzegovina v. Serbia & Montenegro, 2007 I.C.J. 47, 129 (Feb. 26, 2007) (para. 209) ("[C]laims against a State involving charges of exceptional gravity must be proved by evidence that is fully conclusive.").

[241] TALLINN MANUAL 2.0, *supra* note 8, at 82. Ultimately, the *Manual* takes a very on-the-one-hand, on-the-other-hand approach. After suggesting that the graver the attack the more evidence will be required, the *Manual* then notes essentially the opposite logic: states facing severe cyberattacks may be less able to muster robust attribution evidence than states facing less significant attacks. *Id.*

[242] *See* Egan, *supra* note 107; TALLINN MANUAL 2.0, *supra* note 8, at 81 ("With respect to *ex ante* uncertainty as to the attribution of cyber operations, . . . States must act as reasonable States would in the same or similar circumstances when considering responses to them.").

to enable cross-checking or corroboration of the attribution. Providing sufficient technical details to allow other attributors—companies, governments, and academic experts—to confirm (or debunk) an attribution will bolster the attribution's credibility.[243] Improving the credibility of attributions in turn leads to greater agreement about the factual realities of states' behavior in cyberspace and may foster development of agreed norms or customary international law about permissible behavior.

Moreover, a requirement for attributors to "show their work" by providing evidence to support and explain the attribution should incentivize more careful and better reasoned attributions in the first place. This argument is familiar from numerous contexts,[244] including U.S. administrative law. There, the requirement that agencies explain the basis for their decisions so that they can be subject to review (by courts, in the administrative context) is understood to foster better decision-making ex ante,[245] and accountability for decisions ex post.[246]

The requirement of sufficient evidence to allow cross-checking would set a floor on the evidence needed to accompany an attribution. Importantly, this floor is independent of the type of responsive action the attributing state may or may not choose to undertake, unlike the sliding scale approach from the ICJ and the *Tallinn Manual*, which alters the evidence required based on the severity of the attack or anticipated response. The two approaches can be applied in tandem. For severe attacks and significant responses, the sliding scale approach would suggest *more* than just enough evidence to permit cross-checking, but for less severe incidents, the cross-checking requirement sets an evidentiary floor. That is, even in instances where a state's only response to a cyberattack is attempted naming-and-shaming through public attribution to the perpetrator state, that state would be required to provide sufficient evidence to enable cross-checking and corroboration.

Cross-checking could either take the form of *replication* of an attribution by others using evidence provided by the original attributor, or *corroboration* of the

---

[243] *Cf.* Rid & Buchanan, *supra* note 22, at 28 (arguing that when details about attribution "are made public, the quality of the attribution is likely to increase" and that publication "may generate new evidence and analysis").

[244] *See generally* Frederick Schauer, *Giving Reasons*, 47 STAN. L. REV. 633, 657 (1995)(discussing the "decision-disciplining function of giving reasons").

[245] *See, e.g.*, Martin Shapiro, *The Giving Reasons Requirement*, 1992 U. CHI. L. F. 179, 181 ("The reason-giving administrator is likely to make more reasonable decisions than he or she otherwise might . . . ."); Matthew C. Stephenson, *A Costly Signaling Theory of "Hard Look" Judicial Review*, 58 ADMIN. L. REV. 753, 762 (2006) (summarizing academic arguments in favor of hard look review, including that "hard look review encourages agencies to engage in superior (for example, more comprehensively rational or more deliberative) decisionmaking processes"); Cass R. Sunstein, *On the Costs and Benefits of Aggressive Judicial Review of Agency Action*, 1989 DUKE L.J. 522, 527 (arguing that the "*in terroram* effect of the prospect of judicial scrutiny" "serves as a powerful ex ante deterrent to lawless or irrational agency behavior").

[246] Jerry L. Mashaw, *Reasoned Administration: The European Union, the United States, and the Practice of Democratic Governance*, 76 GEO. WASH. L. REV. 99, 115 (2008) ("[T]he fundamental value of reason giving is political and legal accountability.").

initial attribution by combining evidence from the initial attributor with additional information in the possession of subsequent attributors. The gold standard for provision of evidence to support an attribution is Mandiant's APT1 report, which included detailed explanations of the evidence on which Mandiant relied in identifying members of the Chinese PLA and also provided technical appendices that other entities could use.[247] Crowdstrike's attribution of the DNC hack was also subject to cross-checking, with multiple firms analyzing malware samples and building on information, notably IP addresses, Crowdstrike provided to confirm the attribution.[248] Some government attributions, particularly U.S. attributions-by-indictment, have been quite detailed, although they do not include as many technical details as private sector attributions.[249] In some circumstances, this is a question of form. An indictment or press release does not lend itself to providing indicators of compromise. Nonetheless, the U.S. government in particular, however, has released technical details via DHS alerts in some cases, including those like WannaCry, where other attribution mechanisms are also deployed.[250]

Defining the standard of evidence in a functionalist manner based on its key feature of enabling cross-checking is more robust than simply trying to apply a formalist descriptor. Even in the U.S. domestic system, which employs numerous descriptors for evidentiary standards, there is confusion about the precise meaning of different linguistic formulations.[251] Choosing a single descriptor that would have to be translated internationally may cause further confusion. The cross-checking standard deliberately combines a requirement to disclose evidence with a minimum amount of evidence requirement. Such a standard furthers the goal of promoting stability in cyberspace because it suggests broad agreement about the truth of attributions, and it is the agreed factual reality promoted by credible attributions that

[247] *See supra* notes 117-121 and accompanying text.

[248] *See* Nakashima, *supra* note 121 (discussing confirmations by Fidelis Cybersecurity, Mandiant, and ThreatConnect).

[249] *Cf.* Rid & Buchanan, *supra* note 22, at 27-28 (describing the 2014 PLA indictment as "exceptionally detailed" despite the fact that it contained "very few forensic details" as compared to the Mandiant APT1 report on the same actors).

[250] *See, e.g.*, U.S. Dep't of Homeland Sec., Alert (TA17-132A), Indicators Associated with WannaCry Ransomware, May 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-132A (providing indicators of compromise related to WannaCry and noting that the alert was updated after the U.S. government attributed WannaCry to North Korea); *see also* U.S. Dep't of Homeland Security, *supra* note 56 (providing indicators of compromise and other technical details related to Russian government targeting of various critical infrastructure sectors). Release of technical details should be done carefully and in such a way as to cause neither undue alarm nor confusion. *See* ROMANOSKY & BOUDREAUX, *supra* note 41, at 2 (discussing criticism of the U.S. DHS/FBI Joint Analysis Report entitled "GRIZZLYSTEPPE" on hacking related to the 2016 election).

[251] *See, e.g.*, Addington v. Texas, 441 U.S. 418, 425 (1979) ("[T]he difference between a preponderance of the evidence and proof beyond a reasonable doubt probably is better understood than either of them in relation to the intermediate standard of clear and convincing evidence."); CHARLES ALAN WRIGHT ET AL., 21B FEDERAL PRACTICE & PROCEDURE § 5122 (2d ed. 2005) ("Attempts to define this [clear and convincing evidence] standard seem to fall flat. Nonetheless, courts keep trying." (internal citation omitted)).

fosters stability in and helps to avoid conflict over cyberspace. If one were to map an existing evidentiary standard onto the cross-checking requirement's amount of evidence threshold, it would likely be something akin to a preponderance of the evidence standard.[252] A preponderance is generally understood to mean that something is more likely than not to be true.[253] Thus the cross-checking standard's amount and disclosure requirements might be understood together as akin to a *verifiable preponderance standard*.

Adopting an evidentiary standard of sufficient evidence to enable cross-checking would also serve the other possible purposes of attribution.

Consider macro-level deterrence. For an attribution to foster macro-level deterrence requires at least an implied threat of punishment—a responsive action such as countermeasures. For countermeasures to be viewed as lawful requires the state contemplating taking them to convince other states that it was the victim of an internationally wrongful act. Providing sufficient evidence to allow other states to verify the attribution—and thus the accused state's wrongful act—would make the threat of countermeasures more credible, increasing the deterrent effect of the attribution.

Creating micro-level deterrence by imposing costs on particular government-sponsored hackers could also be accomplished by providing sufficient evidence to enable cross-checking. In the United States, indictments are governed by probable cause and sanctions require a reasonable basis. These domestic law standards could easily be satisfied by a requirement to provide sufficient evidence to enable cross-checking, though the reverse might not be true, as explained above.[254] Particularly with respect to economic sanctions, the evidence offered to date has been minimal. Although likely sufficient to meet the domestic law standard, more detail would be required to enable cross-checking. For criminal indictments that proceed to trial, the domestic law standard could outpace the international one: evidence sufficient to prove an individual's criminal responsibility beyond a reasonable doubt could exceed the international law requirement to provide sufficient to enable cross-checking. International law would then provide merely a floor, while domestic due process requirements would push the evidentiary standard higher at the time of trial.

Finally, consider attributions aimed at improving network defenses. Attributing an attack to a particular state is not necessary for hardening defenses, which can be accomplished with provision of indicators of compromise and other technical details without a public attribution. If an attribution-by-alert attributes simply to *a state*, without naming a *particular* state, then it does not constitute a public attribution and would not in any event be captured by a requirement of

[252] *See, e.g.*, WRIGHT ET AL., *supra* note 251, at § 5122 (discussing the preponderance of the evidence standard in comparison to other evidentiary standards).

[253] *See, e.g.*, MCCORMICK ON EVIDENCE 661 (7th ed. 2013) (defining "proof by a preponderance" as "proof which leads the jury to find that the existence of the contested fact is more probable than its nonexistence").

[254] *See supra* text accompanying note 236 (discussing how domestic law provides an evidentiary floor for some mechanisms used to attribute cyberattacks to states).

sufficient evidence to enable cross-checking.[255] If, however, an attribution that is aimed at spurring network defenders to harden their systems does name a particular state, then the evidence sufficient for cross-checking requirement should apply. Even if the attribution is primarily intended to have defensive benefits, it also constitutes an accusation against a state, whose behavior and the state-based response to it are both constitutive of customary international law. Although at least some of the defensive benefits may accrue without sufficient evidence to enable cross-checking, the broader systemic benefits of clarity and conflict avoidance require providing evidence.

The legitimacy of establishing an international law standard for the quantum of evidence required for cyberattack attribution is perhaps most obvious with respect to the high-end of state action and possible victim response—cyberattacks that constitute an armed attack. But establishing an international law standard is desirable in other contexts too, and indeed may have a greater beneficial effect.

Some cyberattacks below the armed attack threshold will constitute a use of force or another violation of international law, such as a violation of the principle of non-intervention.[256] There, the attribution involves an allegation of a violation of international law, and allegations of lawbreaking should be supported with evidence to enable cross-checking of the allegation by, for example, other states and the United Nations. If the victim reasonably alleges a violation of international law, then it will be entitled to take countermeasures.[257] The allegation of wrongdoing changes the legal relationship between the states involved. In such a circumstance, evidence to support the existence of and attribution of the initial wrongful act is crucial to enable assessments of the legality of the victim state's subsequent countermeasures.

For attributions that do not involve an allegation of violating existing international law, an international law evidentiary standard is, paradoxically, perhaps even more desirable. From the perspective of progressively developing customary international law or at least norms to govern state behavior in cyberspace, it is most important to clarify state practice in the gray area where the primary rules governing what states may and may not do are currently unclear. Public attributions supported by evidence can foster greater understanding and agreement on what state practice is,

[255] *See* Eichensehr, *supra* note 90 (discussing the low evidentiary basis needed for private-sector notifications to account holders targeted by state-sponsored actors when the notifications do not identify a particular state). That is not to say that more evidence is undesirable: additional evidence up to or exceeding the level of enabling cross-checking would still serve the systemic purpose of promoting stability.

[256] For discussions of, for example, whether election interference violates the prohibition on intervention, see Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SEC. (Jan. 5, 2017), https://www.justsecurity.org/35999/international-law-response-russian-election-interference; Duncan Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention*, OPINIO JURIS (July 25, 2016), http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention.

[257] *See supra* notes 154-155 and accompanying text (discussing countermeasures).

and from state practice, norms or customary international law to govern behavior can evolve.

Importantly, establishing an evidentiary standard for public attribution of state-sponsored cyberattacks is not the same as setting an evidentiary standard for accusations related to activity that clearly does *not* violate international law. Traditional espionage is a good example. International law is generally understood *not* to prohibit espionage, although espionage violates states' domestic law.[258] In expelling alleged spies, states often provide no evidence to support their actions. And establishing a *lex specialis* in the context of cyberattacks would not require a change in this practice. Rather, for all of the reasons discussed above,[259] setting a standard in the cybersecurity context is particularly important and useful. At least some of the state-sponsored behavior at issue in public attributions made to date will likely come to be viewed as violating norms or customary international law governing state behavior—it is just not clear now *which* activities will fall in that category.[260]

The process for establishing the proposed international law requirement for evidence-giving is fairly straightforward.[261] Customary international law requires general state practice supported by a sense of legal obligation (*opinio juris*). Practice among states that have done state-to-state attributions, including the most recent coordinated attributions, has in some cases come close to providing sufficient evidence to permit cross-checking or corroboration.[262] Going forward, *all* governmental attributions should provide sufficient evidence to allow other governmental and non-governmental actors to confirm or debunk the attributions. This may mean combining attributions by indictment, sanctions, or press release with attributions-by-alert where technical details can be included more easily.

That leaves the second component of customary international law, namely *opinio juris*. The United States, United Kingdom, and France, as explained above,

---

[258] *See, e.g.*, Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 300-15 (2014) (discussing the reasons for the traditional view that international law either affirmatively permits or at least does not prohibit espionage and why those reasons may be under pressure).

[259] *Supra* notes 157-162 and accompanying text.

[260] *See id.* (discussing the iterative process of norm-creation through attributions).

[261] This Article focuses on creating an evidentiary standard through the development of norms and customary international law, but the standard could also be set by treaty. The prospects for such a treaty, however, seem dim as no cybersecurity treaties have yet garnered the kind of worldwide participation—that is, participation of both accusers and accused—that would make them most useful, and negotiations at the U.N. GGE broke down over issues of the application of international law to cyberspace. *See* Elaine Korzak, *UN GGE on Cybersecurity: The End of an Era?*, THE DIPLOMAT, July 31, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (discussing disagreement in the 2017 GGE over international law). In the immediate term, norms and customary international law appear more promising vehicles because states can begin to set state practice and *opinio juris* unilaterally and in smaller groups, and such progress does not require agreement of other states.

[262] *See, e.g.*, *supra* notes 249-250 and accompanying text (discussing technical details and government attributions).

have made statements disavowing a legal obligation.[263] That should change. And it can change quickly and easily. One of the clearest types of evidence of *opinio juris* is "an express public statement on behalf of a State that a given practice is permitted, prohibited or mandated under customary international law."[264] States could begin including references to customary international law in statements they issue announcing attributions or in statements supporting attributions made by other states. Importantly, to establish a rule of customary international law, "[i]t is not necessary to establish that all States have recognized (accepted as law) the alleged rule," but rather "it is broad and representative acceptance, together with no or little objection, that is required."[265] Such representative acceptance seems within reach if the attributing states alter their stance.[266] States more often on the receiving end of attributions have called most insistently (and opportunistically) for provision of evidence.[267] States making the attributions should do so as well. In addition, states that do not themselves engage in attributions or wish to comment on particular attributions could contribute to the formation of customary international law through voting and participation on deliberations on U.N. General Assembly resolutions dealing with attributions and the evidentiary standard.[268] Such resolutions could help both to constitute customary international law and reflect that such law has already crystallized by revealing the existence of *opinio juris* for a broad range of states.[269]

Taken together, the development of consistent and uniform state practice with respect to evidence giving and *opinio juris* reflecting a felt obligation to provide such evidence can help to level the playing field with respect to the evidentiary basis of attributions. In international politics, the credibility of the state offering evidence and that state's relations with other states can affect the amount of evidence required for a state to be believed.[270] Establishing a legal standard of sufficient evidence to enable

---

[263] *See supra* notes 201-204 and accompanying text.

[264] Int'l Law Comm'n, *supra* note 204, at 141.

[265] *Id.* at 139.

[266] The proposed customary international law rule would instantiate several of the features that Laurence Helfer and Ingrid Wuerth suggest make the formation of custom more likely, including having "powerful states (or groups of like-min[d]ed countries) advance new rules that respond to emerging global problems or seek to overcome distributional differences by promoting rules with compelling normative content." Helfer & Wuerth, *supra* note 208, at 609.

[267] *See supra* note 106 and accompanying text (discussing a U.N. resolution proposed by Russia and China, among other countries, stating that claims of state conduct of cyberattacks "should be substantiated").

[268] U.N. General Assembly resolutions generally require the vote of a "majority of the members present and voting." Gen. Assembly of the United Nations, Rules of Procedure, Rules 85-86, https://www.un.org/en/ga/about/ropga/plenary.shtml (defining the voting rules).

[269] *See* Int'l Law Comm'n, *supra* note 204, at 147-48 (discussing the role of resolutions of international organizations in constituting and reflecting international law, and noting that U.N. General Assembly resolutions deserve "[s]pecial attention" because the Assembly is "a plenary organ of the United Nations with virtually universal participation, that may offer important evidence of the collective opinion of its Members").

[270] *See, e.g.*, Finnemore & Hollis, *supra* note 9, at 16 ("Reputation and credibility matter greatly in the latitude an accuser has in disclosing supporting details when making accusations. If the accuser

cross-checking of an attribution decreases the role of reputation and makes the assessment of an attribution's accuracy and veracity more objective—a feature sorely needed in an international realm increasingly divided into adversarial blocs over the governance of cyberspace and many other issues.

Although international law directly binds only states, non-governmental attributors should consider abiding by the international law standard for evidence-giving as well. Indeed, many non-governmental attributions already meet the proposed standard of providing sufficient evidence to enable cross-checking, so the proposed standard would require little to no change in behavior by many non-governmental attributors. Nonetheless a commitment by non-governmental attributors to provide sufficient evidence to enable cross-checking of their attributions would be beneficial. It would both establish an industry-standard practice for other non-governmental attributors to meet[271] and ensure that non-governmental attributions contribute to shared and agreed knowledge about state behavior in cyberspace, along with the stability and conflict-avoidance benefits such clarity would foster.

* * *

Although the paucity of existing international law on evidence presents immediate challenges for cyberattack attribution, it also provides an opportunity to create an evidentiary *lex specialis*, tailored to the cybersecurity context. Adoption of and advocacy for the evidentiary standard by even a few states with significant cyberattack capabilities or high-profile victim states could begin the process of establishing a norm that could then, over time, harden into customary international law.[272] Some of the benefits of an evidentiary standard—including providing clarity about what's required for credible attributions, fostering transparency about states' behavior in cyberspace, and setting out markers for impermissible state behavior—could manifest even while the standard is merely a norm. Others, especially *mandating* evidence-giving by recalcitrant states, would require the standard to crystallize into customary international law.

Although the proposed evidentiary standard of providing sufficient evidence to enable cross-checking is particularly important in the cybersecurity context where so little is publicly known about what states are actually doing and where significant resources for verifying attribution claims exist outside of governments, the cross-

---

has a record of veracity and has technical capacity for sophisticated forensics and good intelligence, accusations with less detail may still be widely credible.").

[271] *Cf. infra* note 294 and accompanying text (noting private attributors' divergences in methodology).

[272] *See, e.g.*, Christine Chinkin, *Normative Development in the International Legal System*, *in* COMMITMENT AND COMPLIANCE: THE ROLE OF NON-BINDING NORMS IN THE INTERNATIONAL LEGAL SYSTEM 21, 30 (Dinah Shelton ed., 2003) (identifying "[e]mergent hard law" as "principles that are first formulated in non-binding form with the possibility, or even aspiration," that they will "harden into binding custom through the development of state practice and *opinio juris*" (footnote omitted)).

checking standard may have broader utility. It is essentially a standard founded on the idea of "trust, but verify," with a heavy emphasis on verification. Setting an evidentiary standard that enables and promotes verification by governmental and non-governmental entities alike of states' claims about cyberattack attribution would help to ensure the accuracy of states' accusations of wrongdoing and encourage broader acceptance of claims that are made. The *lex specialis* in the cybersecurity context has the potential to morph into *lex generalis*, bringing clarity to the evidentiary issues that states have muddled through in non-cybersecurity contexts, including, for example, evidentiary questions surrounding Iranian responsibility for mining tankers and shooting down a U.S. drone.[273] The potential for *lex specialis* to transform into *lex generalis* raises the stakes for developing a robust and widely agreed evidentiary standard for attributing cyberattacks.

The next Part turns from the legal standard for cyberattack attributions to questions of institutional design.

III. DESIGNING ATTRIBUTION

Setting an evidentiary standard for credible attributions could help to routinize attributions, but the question remains: attributions by whom? The current attribution system is decentralized, featuring a mix of governmental and non-governmental attributors and of attribution mechanisms. Diverse entities in recent years have proposed that attributions instead be centralized in a new international entity. These proposals have much to recommend them as additions to the attribution landscape. However, if this Article's proposed evidentiary standard were adopted, centralization would be less crucial, and moreover, preserving some amount of decentralization and a multiplicity of attributors may be the optimal design for attributing state-sponsored cyberattacks. Having a proliferation of credible attributors and mutually reinforcing attributions is more likely to maximize stability and foster development of primary norms of state behavior than resting attribution responsibilities in any single entity.

This Part first provides an overview of proposals to centralize attribution in a new international entity and then argues for some underappreciated virtues of preserving a measure of decentralization.

The problem of credibly attributing state-sponsored cyberattacks has prompted several recent proposals to centralize responsibility for attribution. The proposals differ in the extent to which the proposals' authors believe states should be involved in attribution judgments.

At one end of the spectrum, the Atlantic Council, a Washington, D.C.-based think tank, proposed a Multilateral Cyber Attribution and Adjudication Council

[273] *See, e.g.*, Jasmin Johurun Nessa, *Self-Defense in International Law: What Level of Evidence?*, JUST SEC., July 8, 2019, https://www.justsecurity.org/64796/self-defense-in-international-law-what-level-of-evidence/ (discussing the Iran examples and debates about the standard of evidence required for self-defense).

consisting, as the multilateral title suggests, of states.[274] The Council would "provide an international mechanism for arriving at a consensus attribution of illegal cyber campaigns by states and a formal process for adjudicating associated interstate disputes."[275] The proposal contemplates that "[w]hen attribution is high confidence, the defendant state would be given an opportunity to present exculpating evidence and arguments,"[276] and the Council can "issue a recommendation on steps to deescalate the malicious activity," as well as "rule on damages" that the perpetrator owes to the victim.[277]

At the midpoint of the spectrum, in a 2016 white paper, Microsoft proposed the establishment of an international institution for attribution of state-sponsored cyberattacks that would feature a mix of governmental and non-governmental actors.[278] Microsoft suggests modeling the body on the International Atomic Energy Agency and making it multistakeholder, "consist[ing] of technical experts from across governments, the private sector, academia, and civil society."[279] Microsoft envisions that the organization would produce a "technical analysis of the attack and evidence of attribution," which it would sometimes publish.[280] Microsoft acknowledges that the institution would need representatives from a "diverse set of nation-states and geographic regions," including "[a]t a minimum . . . representatives from countries that are permanent members of the United Nations Security Council."[281] The white paper further suggests that attribution reports "can be subject to peer review, improving the quality of the results."[282]

At the other end of the spectrum are proposals that deliberately exclude governments. Researchers at the RAND Corporation, in a report funded by Microsoft, went further than the Microsoft proposal.[283] RAND proposes the establishment of a "Global Cyber Attribution Consortium" and emphasizes that the Consortium must have "broad membership across geopolitical lines to foster a diversity of perspectives and to minimize the possibility that its findings are tainted by political influence."[284] But crucially, the RAND researchers specifically argue

---

[274] JASON HEALEY ET AL., CONFIDENCE-BUILDING MEASURES IN CYBERSPACE, ATLANTIC COUNCIL 10 (2014), https://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.

[275] *Id.*

[276] *Id.*

[277] *Id.* at 11.

[278] *See* Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 690 (2019) (discussing the Microsoft proposal).

[279] SCOTT CHARNEY ET AL., FROM ARTICULATION TO IMPLEMENTATION: ENABLING PROGRESS ON CYBERSECURITY NORMS 11 (2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

[280] *Id.*

[281] *Id.* at 12.

[282] *Id.*

[283] DAVIS II ET AL., *supra* note 22, at vi.

[284] *Id.* at 27.

that state representatives should *not* be part of the Consortium.[285] They argue that the Consortium's membership should be drawn from "(1) technical experts from cybersecurity and information technology companies, as well as academia, and (2) cyberspace policy experts, legal scholars, and international policy experts from a diversity of academia and research organizations."[286] They argue that state participation is not necessary in light of the "significant expertise" outside the government, and that state participation creates difficulties because states are often unwilling to disclose evidence on which attributions are based, states might try to "shape the Consortium's findings to serve their national interests," and states would try to direct the Consortium away from investigations that "might shed light on or otherwise threaten their own cyber operations."[287] A report published by researchers at the University of Washington's School of Public Policy has similarly proposed an international attribution organization that would exclude governments,[288] consisting instead of private sector representatives.[289]

The proposals to centralize attribution respond to problems with the current, decentralized system. Some of these problems stem from the inherent features of the current attributors, which raise serious questions about their credibility and objectivity. Government attributions may be politically motivated and lacking in transparency.[290] Private sector attributions, on the other hand, may be driven by companies' business incentives, which can lead to a rush to attribute, or by ties to governments that want the company to issue an attribution.[291] An international entity with diverse geographic representation that issues careful, transparent attributions and lacks financial or political incentives to skew results would address these concerns.

Another set of concerns with the current system focuses on the confusion caused by having a proliferation of attributors, each of which has its own naming convention and techniques for identifying threat actors, often the *same* threat actors. For example, the Russian GRU is "known as Sofacy by Kaspersky, as APT28 by FireEye, Strontium by Microsoft, and Fancy Bear by Crowdstrike."[292] Having a centralized attribution entity could address this by "creat[ing] a formal nomenclature system so that the attacks can be universally referenced in future investigations."[293] It

---

[285] *Id.* at 29.

[286] *Id.*

[287] *Id.* at 29-30.

[288] JUSTIN COLLINS ET AL., CYBERATTACK ATTRIBUTION: A BLUEPRINT FOR PRIVATE SECTOR LEADERSHIP, UNIV. OF WASH., 26 (2017), https://jsis.washington.edu/wordpress/wp-content/uploads/2017/07/ARP-2017-Report-FINAL.pdf (arguing that including governments "would undermine the organization because government involvement brings lack of transparency and issues of credibility").

[289] *Id.* at 28 (proposing that the organization be "private sector run").

[290] *See, e.g.*, DAVIS II ET AL., *supra* note 22, at 22 (discussing problems with government attributions).

[291] *See, e.g.*, *id.* at 23 (discussing weaknesses of private sector attributions).

[292] *Id.* at 20 (capitalization omitted).

[293] *Id.* at 19.

could also "help standardize diffuse methodological approaches and confidence metrics that would advance shared understanding in cyberspace and promote global cybersecurity."[294]

Finally, having an international attribution entity could improve access to attribution resources among victims. Cyberattack victims often "either cannot afford cyber attribution assistance or do not know where to turn for help."[295] This holds true for non-governmental victims, but also for states that have less advanced intelligence and cybersecurity capacities.[296] An international entity could help by providing a clear point of contact for victims and bringing to bear the resources of sophisticated cyber actors to help victims that lack resources to do the attribution themselves or to hire private companies to investigate for them.[297] This function would become especially important if states take up this Article's proposal for setting an evidentiary standard for public attributions of state-sponsored cyberattacks. One potential downside of the proposal is its possible differential impact: states with sophisticated cyber capabilities will have an easier time meeting any evidentiary standard, while those with less sophisticated capabilities may nonetheless be victims of cyberattacks and yet unable to meet the evidentiary standard required to make a public attribution to the perpetrator. An international attribution entity could help to mitigate this differential impact by making attribution resources available to less sophisticated states.

The proposals, particularly those that preserve an important or even dominant role for non-governmental attributors, have much to recommend them. At the same time, there are significant risks to relying on a centralized attribution model.

First, and most importantly, centralizing attributions makes the credibility of attributions dependent on the credibility of a single entity. The proposals attempt to address this issue by calling for diverse geographic representation among participants in the new attribution entity. But that will be difficult to achieve. Major cyber powers, particularly China, have repeatedly (and opportunistically) suggested that "attribution is nearly impossible."[298] Gaining participation from such countries and their allies will be difficult, and without it, the credibility of the entity will be undermined for a large swath of the world.

---

[294] *Id.* at 27.

[295] *Id.* at 19.

[296] *Id.*; HEALEY ET AL., *supra* note 274, at 10.

[297] *Cf.* HEALEY ET AL., *supra* note 274, at 10 (noting that the proposed Council "can help raise the expected attribution for states with lower attribution capacity by leveraging that of advanced cyber powers").

[298] Michael Sulmeyer & Amy Chang, *Three Observations on China's Approach to State Action in Cyberspace*, LAWFARE, Jan. 22, 2017, https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace (reporting on comments made by Chinese officials during a dialogue held by U.S. and Chinese think tanks); *see, e.g.*, Jason Healey, *China is a Cyber Victim, Too*, FOR. POL'Y, Apr. 16, 2013, https://foreignpolicy.com/2013/04/16/china-is-a-cyber-victim-too/ ("[Chinese officials] argue that the cyberattacks are too hard to trace to know with any certainty who perpetrated them.").

Second, an international attribution entity would likely be resource-constrained. Resource constraints could limit the number of cyberattacks the entity could investigate, raising the need for other attributors to pursue additional investigations. Resource constraints could also manifest in a different way, namely that attaining high confidence on particular attributions might require the all-source intelligence resources of powerful states—resources that quite likely would not be available to the new entity. The international attribution entity then could not cover the field of cyberattacks in need of attribution.[299]

A new attribution entity faces fundamental hurdles. Bringing governments into the organization risks corrupting the attribution process. Leaving them out risks hampering the entity's access to necessary intelligence information and preventing it from making attributions in particularly significant cyberattacks. And having some governments in and some governments out may exacerbate the perception that the entity's attributions are politicized or that its choice of cases to investigate is skewed.[300]

All of these challenges suggest that while there is value to creating an entity in some form, it should become an *additional* participant in the current decentralized attribution system—centralization within decentralization as it were. This is effectively an argument for what Heather Gerken has called "second-order diversity."[301] An international attribution entity might achieve "first-order diversity," mirroring the landscape of entities involved in cyberattacks and cyberattack attribution,[302] but additional benefits flow from having the "interorganizational heterogeneity" entailed by second-order diversity.[303] The decentralized attribution system, with its various forms of attributors, has a number of virtues that have gone un- or under-appreciated.[304]

First, if attributors adopt this Article's proposed evidentiary standard for attributions, the need for a centralized attribution entity would decrease. Instead of relying on a single entity's epistemic authority to ensure the credibility of attributions,[305] the evidentiary standard provides a means of diffusing credibility:

---

[299] DAVIS II ET AL., *supra* note 22, at 4 (noting that for some cases, an international attribution entity "will likely be . . . ill equipped to produce an attribution decision without the insights that government intelligence agencies may be able to provide").

[300] In a future project, I plan to address how best to structure an international entity to minimize the risks identified here and to maximize the beneficial role such an entity could play in a decentralized attribution system.

[301] Heather K. Gerken, *Second-Order Diversity*, 118 HARV. L. REV. 1099, 1102 (2005).

[302] *Id*.

[303] *Id.*; *see also id.* at 1108 ("[T]he democratic process may benefit from decisionmaking bodies that reflect a wide range of compositions.").

[304] The following arguments in favor of decentralization draw on Eichensehr, *supra* note 119.

[305] *See* Guy-Uriel E. Charles, *Colored Speech: Cross Burnings, Epistemics, and the Triumph of the Crits?*, 93 GEO. L.J. 575, 610 (2005) ("[E]pistemic authority is invoked when one accepts a factual assertion as true because someone else—someone with epistemic authority—says that it is true.").

attributions will be deemed credible not based on who makes them,[306] but rather based on their compliance with the evidentiary standard and consequent ability to be verified and corroborated. A new attribution entity could contribute to the parade of evidence-supported attributions, but it need not be the only game in town. The proposed evidentiary standard fosters credibility *because of* decentralization and the promise of multiple attributors verifying attributions.

Second, decentralization can foster transparency about states' actions more quickly. Different attributors can publicly accuse states whenever they, based on their own investigations, are satisfied that they have successfully identified the perpetrators. In many instances, this will mean a cascade of attributions over time. The overall credibility of an attribution is not set at a single early point in time, but builds along with confirmatory attributions. In other words, with a decentralized system, attributions need not be tied to the timetable set by the most hesitant attributor.

Numerous attributions bear out the transparency benefits of a multiplicity of attributors. For example, the Mandiant APT1 report accused Chinese PLA officers of IP theft more than a year before the U.S. government was ready to indict one of the same officers.[307] Perhaps the best example of the transparency benefits of rolling attributions is the process of attributing the DNC hack. The first attribution to Russia came from Crowdstrike, which investigated the hack for the DNC, in June 2016.[308] By July 2016, other security researchers confirmed Crowdstrike's claim.[309] These attributions provided crucial transparency about Russia's efforts to influence the U.S. elections, and they did so months before the U.S. government first attributed the cyberattacks to Russia only weeks before the election.[310] Responsive actions, at least in the form of sanctions, took additional months,[311] and an indictment charging Russian intelligence officials came only in July 2018.[312] The most recent additions are attributions of the DNC hack to Russia from Australia, New Zealand, and the United Kingdom, announced as part of a coordinated attribution campaign in October 2018.[313] If all of these attributors were to participate in an international attribution entity, it is doubtful that the attribution would have come as early as it did, and perhaps not even before the 2016 election. A centralized attribution entity

---

[306] *Id.* at 611 ("[W]hat we know depends upon whom we believe . . . . Whom we believe is a question of epistemic authority."); *cf.* Paul Horwitz, *Three Faces of Deference*, 83 NOTRE DAME L. REV. 1061, 1085 (2008) (explaining epistemic deference in the context of courts and noting that "courts defer to other institutions when they believe that those institutions know more than the courts do about some set of issues, such that it makes sense to allow the views of the knowledgeable authority to substitute for the courts' own judgment").

[307] *See supra* note 117 and accompanying text.

[308] Alperovitch, *supra* note 118.

[309] *See supra* note 121 and accompanying text (discussing confirmations of Crowdstrike's attribution).

[310] DHS Press Office, *supra* note 58.

[311] White House, *supra* note 49 (describing sanctions and other responsive actions).

[312] Indictment, *supra* note 64.

[313] *See* sources cited *supra* note 93.

could boost credibility by confirming attributions made at the earliest possible time by, for example, private cybersecurity companies. But relying solely on a centralized mechanism risks slowing accusations, at a significant potential cost to transparency in sufficient time to respond to or guard against the effects of ongoing bad acts.

Third, a multiplicity of attributors is likely to result in *more* and *different* attributions. A centralized entity would have to make choices about how to allocate scarce resources, but a decentralized system has the potential to foster a greater number of resources devoted to attributions overall. One risk of private attributions is that they are driven by companies' marketing concerns. But, on the other hand, the marketing benefits of attributing state-sponsored cyberattacks channels companies' business interests in the direction of more attributions. They get credit for outing state cyberattacks in a way that they likely would not by participating in a broad-based international entity.[314] An attribution by the entity would not redound to the business benefit of a particular company in the same way and thus could disincentivize companies to devote as many resources to publicizing attributions.

Decentralization also opens the door to different attributions. As noted above,[315] some non-governmental attributions have focused on espionage by governments that compromises human rights. Those sorts of attributions would be more difficult to do under the auspices of an international entity, at least one that included governments.

Fourth, the decentralized attribution system has the potential to enhance the credibility of attributions. In particular, having a multiplicity of attributors productively harnesses attributors' competitive instincts. Attributors have incentives to cross-check attributions publicized by others—an ability that would be fostered by the evidentiary rule proposed in Part II. Cross-checking resulted in confirmatory attributions by companies and governments with respect to the DNC hack.[316] It has also resulted in some attempted debunking of attributions. A significant attempt to debunk a government attribution occurred when Norse, a "cyber intelligence company," challenged the FBI's attribution of the Sony hack to North Korea and claimed to have evidence that a Sony insider perpetrated the attack.[317] After a briefing by Norse, the FBI reiterated its determination that North Korea was responsible,[318] and ultimately released more information about why it was confident that was the case.[319] To be sure, cross-checking could occur through more formalized peer review within an international attribution entity, serving the same purpose of potentially improving the quality and credibility of attributions.[320] But again, that

[314] *See* Finkle, *supra* note 131 (discussing public praise for Mandiant's APT1 report).

[315] *See supra* notes 126-128.

[316] *See supra* note 121 (discussing confirmations of Crowdstrike's attribution).

[317] Tal Kopan, *U.S.: No Alternate Leads in Sony Hack*, POLITICO, Dec. 29, 2014, https://www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866.

[318] *See id.*

[319] *See supra* note 194 and accompanying text (describing speech by James Comey providing additional details).

[320] *See, e.g.*, CHARNEY ET AL., *supra* note 279, at 12.

could be an addition to the ad hoc, competitively incentivized peer review currently occurring as part of the decentralized attribution system.

Another way the decentralized attribution system bolsters the credibility of attribution is by at least potentially broadening the audience of those who will credit attributions. Put simply, different attributors—or *different kinds* of attributors—may persuade different audiences. For example, cybersecurity researchers who are skeptical of government attributions without detailed evidence may nonetheless credit corporate attributions accompanied by indicators of compromise and other technical evidence. Or members of the cybersecurity community who previously worked for government intelligence agencies might credit even parsimonious attributions by former colleagues. Foreign governments might not put much stock in corporate attributions, but might, as appears to be the case, credit other governments' attributions, particularly if the attributing government shares the intelligence on which its attribution is based (even when it declines to do so publicly). Attributions can have a multiplicity of audiences—and thus having a multiplicity of attributors can be useful in ensuring that a wide swath of interested parties will credit at least one of the attributors of a particular attack, even if they would not believe others, at least acting alone.

Finally, the decentralized attribution system may create the potential for broader participation. Although the proposals for an international entity envision diverse participation, ad hoc information sharing on particular cases may be an easier way to promote diversity among attributors and to build trust. There are certainly costs to an ad hoc approach,[321] but many potential attributors may be more comfortable with a case-by-case approach to information sharing than with a standing information-sharing pool as envisioned in an international entity. For companies and experts in some regions of the world, it might be difficult or even dangerous to participate in what is likely to be (at least for now) a Western-led entity. But they might be able to participate in certain attribution projects. Think of a Chinese company that might participate in an ad hoc attribution to Russia, but not in one to the Chinese government. Or for that matter, a former U.S. intelligence official at a U.S. company who could participate in an attribution to North Korea, but not one to the United States. The ad hoc case-by-case collaboration approach allows for more tailored choices among experts about when to participate and when and with whom to share information.

The ad hoc approach leaves the door open for some of the benefits sought from an international entity, including standardization of nomenclature identifying threat groups and development of more consistent methodologies among attributors, and by bringing in a more diverse set of experts, it may help to promote a shared understanding of the factual reality of states' behavior in cyberspace. Ideally, diverse participation on particular cases could serve as a confidence-building mechanism

[321] *See, e.g.*, DAVIS II ET AL., *supra* note 22, at 19 (arguing that a "standing attribution entit[y]" would be better positioned to track threat actors over time than are "independent investigators coalescing in ad hoc cases")

that might help to foster more diverse participation in an attribution entity going forward.

All of the potential benefits of the decentralized attribution system would be bolstered in the short-term by greater proliferation of confirmatory attributions.[322] As discussed above, such attributions have begun to occur, but they are still quite limited. Among governments, confirmatory attributions have come mostly from the members of the Five Eyes intelligence sharing partnership (Australia, Canada, New Zealand, the United Kingdom, and the United States), plus a few other allies, such as Estonia, Japan, and the Netherlands. Similarly, the confirmatory non-governmental attributions have mostly come from Western companies and other entities. The decentralized attributions would have greater credibility if done by attributors diverse on a number of metrics—geography, political system, governmental/non-governmental status, etc.[323] The benefits of having a *broadly* shared understanding about the factual reality of states' behavior in cyberspace should weigh heavily in any calculus about the undoubtedly real costs of sharing intelligence more broadly or being more transparent about the evidence supporting an attribution.

Importantly, the diversity of attributors could come *after* an initial attribution in the decentralized system. As more attributors confirm an attribution and release more information, additional diverse attributors could pile on. The push for more diverse attributions by a greater number of attributors is thus a call both to those entities that are currently making public attributions to share more information and more broadly and to other governments, security companies, and experts around the world to join in, examine public evidence offered to support attributions, and issue statements of their own confirming (or disputing) public attributions.

CONCLUSION

Cyberattack attributions aren't just political. Politics may partly determine *whether* attributions are made public, but law should govern *how* public attributions are made. Although domestic law has a part to play with respect to some attribution mechanisms, the divergences in states' domestic legal standards and the fact that some frequently used attribution mechanisms are not subject to domestic law at all suggests that international law must step in to unify attribution requirements across states. The proposed functionally defined evidentiary standard requiring that attributors provide sufficient evidence to permit cross-checking will harness both

[322] *Cf.* Office of the Coordinator for Cyber Issues, Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats, U.S. Dep't of State, May 31, 2018, https://www.state.gov/s/cyberissues/eo13800/282011.htm (discussing deterrence of cyberattacks and noting that "[p]artner states could, on a voluntary basis, support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken following an incident, and/or actual participation in the imposition of consequences against perpetrator governments").

[323] *Cf.* Wright, *supra* note 108 ("If more states become involved in the work of attribution then we can be more certain of the assessment.").

governmental and non-governmental attribution capabilities to bring clarity about states' actions in cyberspace. The goals that public attributions are intended to achieve—from improving defenses, to deterrence, to improving stability in cyberspace—will be best served by maintaining a multiplicity of attributors, alongside any future international attribution entity.

Improving the quality, frequency, breadth, and scope of acceptance of attributions of state-sponsored cyberattacks can promote an agreed factual reality about states' behavior in cyberspace. Clarity on such facts can contribute to eventual legal clarity about permissible state behavior in the enormous and tremendously important gray zones below the level of an armed attack and outside armed conflict.