doi:10.1017/aju.2019.33

SYMPOSIUM ON CYBER ATTRIBUTION

DECENTRALIZED CYBERATTACK ATTRIBUTION

*Kristen E. Eichensehr**

Attribution of state-sponsored cyberattacks can be difficult, but the significant uptick in attributions in recent years shows that attribution is far from impossible. After several years of only sporadic attributions, Western governments in 2017 began attributing cyberattacks to other governments more frequently and in a more coordinated fashion.[1] But *non*government actors have more consistently attributed harmful cyber activity to state actors. Although not without risks, these nongovernmental attributions play an important role in the cybersecurity ecosystem. They are often faster and more detailed than governmental attributions, and they fill gaps where governments choose not to attribute. Companies and think tanks have recently proposed centralizing attribution of state-sponsored cyberattacks in a new international entity. Such an institution would require significant start-up time and resources to establish efficacy and credibility. In the meantime, the current system of public-private attributions, decentralized and messy though it is, has some underappreciated virtues—ones that counsel in favor of preserving some multiplicity of attributors even alongside any future attribution entity.

Private Attributions in Practice

Although the deterrent effect of cyberattack attributions is debated,[2] identifying cyberattack perpetrators can enable network administrators to defend against further attacks, and attribution is also a necessary precondition to many responsive actions, like countermeasures.[3] Governments do not have a monopoly on the accusation function.

Private attributions of state-sponsored cyberattacks burst onto the scene in 2013.[4] In February 2013, cybersecurity firm Mandiant published a detailed report accusing Unit 61398 of the Chinese People's Liberation Army of hacking 141 companies over seven years.[5] Other attributions have followed, accusing countries such as China, Iran, and North Korea.[6] Perhaps most famously, in June 2016, Crowdstrike accused the Russian government

* *Assistant Professor, UCLA School of Law.*

[1] *See infra* notes 35–36 and accompanying text.

[2] *See, e.g.*, Jack Goldsmith, *The Strange WannaCry Attribution*, LAWFARE (Dec. 21, 2017) (arguing that a naming-and-shaming strategy is ineffective at deterring state-sponsored cyberattacks).

[3] *Cf.* UN Int'l Law Comm'n, Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 49, UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10 (2001) ("An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act.").

[4] *See* Kristen Eichensehr, *The Private Frontline in Cybersecurity Offense and Defense*, JUST SECURITY (Oct. 30, 2014).

[5] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3 (2013).

[6] *See, e.g.*, CROWDSTRIKE, CROWDSTRIKE INTELLIGENCE REPORT: PUTTER PANDA 5 (2014) (accusing Chinese PLA Unit 61486 of hacking, among others, "satellite and aerospace industries"); Manish Sardiwal et al., *New Targeted Attack in the Middle East by APT34, a Suspected Iranian*

of hacking the Democratic National Committee (DNC).[7] In addition to the corporate attributors, noncorporate nongovernmental entities, including the Citizen Lab at the University of Toronto and the Electronic Frontier Foundation, have made public attributions.[8]

Nongovernmental attributions differ from governmental attributions in a number of ways. First, they tend to be faster. For example, Crowdstrike's attribution of the DNC hack to Russia preceded the first official U.S. government attribution by several months.[9] Second, nongovernmental attributions are often more detailed than governmental attributions and include indicators of compromise and other technical details that enable security professionals to defend systems against further attacks.[10]

Third, nongovernmental attributions have covered a broader range of alleged perpetrator governments and types of cyberattacks than governmental attributions have. Whereas governmental attributions have focused mostly on intellectual property theft and disruptive attacks, nongovernmental attributions have outed, for example, cyberespionage with privacy and human rights implications.[11] Relatedly, private attributions can fill an attribution gap, covering cases where governments decline to make attributions for political reasons or are wary of accusing other governments of activities similar to those that the victim state itself undertakes.[12]

Fourth, the motivations for private attributions and governmental attributions may differ. In some cases, there is a shared motive to disclose information in order to better secure the cybersecurity ecosystem: by outing attackers, attributors hope to deter further attacks by cowing the countries and individual state operatives responsible for them and to enable network administrators to improve their defenses. But companies that out government attacks also have other incentives. The publicity that comes with accusing governments is good for business. Attributions demonstrate the companies' skill at discovering sophisticated intruders and often spur positive press coverage.[13]

Finally, the implications of attributions differ for governmental and nongovernmental attributors. Governments that accuse other governments face pressure to follow up on the naming-and-shaming of attribution with more robust responses, like indictments, sanctions, or responsive cyber actions.[14] This expectation may discourage governmental attributions in the first place. Nongovernmental attributors do not face comparable pressures for follow-up.

Nongovernmental attributions, particularly those by private companies, carry some risks for states and for the international system. The fact that they are marketing tools for companies means that the decision to accuse states

Threat Group, Using CVE-2017-11882 Exploit, FireEye (Dec. 7, 2017) (identifying hackers "work[ing] on behalf of the Iranian government" as responsible for cyberespionage against a Middle Eastern government); Darien Huss, *North Korea Bitten by Bitcoin Bug: Financially Motivated Campaigns Reveal New Dimension of the Lazarus Group*, ProofPoint (2017) (attributing to North Korea a hacking campaign focused on cryptocurrency).

[7] Dmitri Alperovitch, Bears in the Midst: Intrusion into the Democratic National Committee, CrowdStrike Blog (June 15, 2016).

[8] *See, e.g.*, 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) (accusing the United Arab Emirates of spying on a human rights advocate); Lookout & Electronic Frontier Found., Dark Caracal: Cyber-Espionage at a Global Scale (2018) (attributing to Lebanon's General Directorate of General Security espionage focused on mobile devices).

[9] U.S. Dep't of Homeland Security Press Office, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security (Oct. 7, 2016).

[10] *See, e.g.*, Mandiant, *supra* note 5, at 66–74 (providing links to appendices with technical details).

[11] *See, e.g.*, sources cited *supra* note 8.

[12] *See, e.g.*, *In Data Breach, Reluctance To Point The Finger at China*, NPR (July 2, 2015) (quoting Director of National Intelligence James Clapper stating, about the Office of Personnel Management (OPM) hack, "You have to kind of salute the Chinese for what they did … . You know, if we had the opportunity to do that, I don't think we'd hesitate for a minute.").

[13] *See, e.g.*, Jim Finkle, *Mandiant Goes Viral After China Hacking Report*, Reuters (Feb. 22, 2013).

[14] *See, e.g.*, David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. Times (Oct. 7, 2016).

https://doi.org/10.1017/aju.2019.33 Published online by Cambridge University Press

is not governed by any strategic national vision of diplomacy or interagency governmental process. Private attributions may occur at times or in ways that disrupt governments' diplomatic efforts.[15]

At the same time, private attributions may cause accountability confusion. Numerous companies have alerted the U.S. government prior to publishing attribution reports,[16] and in other circumstances, the U.S. government has reportedly given companies information that they use to attribute state-sponsored cyberattacks.[17] The diplomatic consequences of private attributions can be exacerbated by these interactions, which render unclear the extent to which nominally private attributions are coordinated with the U.S. government, in particular.[18]

Another risk for governments is that the detailed nongovernmental attribution reports will set evidentiary expectations that governments will be reluctant to meet. Call it a "cyber-CSI effect."[19] The "CSI effect" is the alleged phenomenon whereby the public's expectations about trial evidence are set by shows like *CSI*, leaving prosecutors in real-world trials to deal with jurors' unrealistic expectations about the nature of evidence they can produce.[20] Although the practice of private actors does not count as state practice for purposes of creating customary international law, it can help to shape expectations among the public, the cybersecurity community, and even states about the amount and type of evidence needed to make an attribution credible. Governments run a risk that if they do not deliberately craft norms or customary international law on the evidentiary standards for cyberattack attribution, the detailed nongovernmental attribution reports will set norms and ultimately push governments to disclose more evidence than they would like in order to satisfy skeptical observers.

Structuring Attribution

The importance of attributions, combined with the reluctance of governments to make attributions and the risk of politicization when they do, has spurred several recent proposals to centralize attribution in a new international entity. The Atlantic Council suggested a Multilateral Cyber Attribution and Adjudication Council that would provide "a consensus attribution of illegal cyber campaigns by states and a formal process for adjudicating associated interstate disputes."[21] Microsoft proposed a multistakeholder attribution body "consist[ing] of technical experts from across governments, the private sector, academia, and civil society" and modeled on the International Atomic Energy Agency.[22] RAND Corporation researchers went further, proposing a "Global Cyber Attribution Consortium" that would entirely exclude states.[23] Instead, the Consortium would be comprised of "technical experts from cybersecurity and information technology companies, as well as academia," and "cyberspace policy experts, legal scholars, and international policy experts from a diversity of academia and research organizations."[24]

[15] *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 529 (2017).

[16] *See* Chris Bing, *In the Opaque World of Government Hacking, Private Firms Grapple with Allegiances*, CYBERSCOOP (July 23, 2018) (reporting that Dell SecureWorks, FireEye, McAfee, Microsoft, TrendMicro, and ThreatConnect have notified the U.S. government).

[17] *See* SHANE HARRIS, @WAR 209 (2014) (reporting that the U.S. government gave Mandiant information used in the APT1 report); Shane Harris, *Security Firm: China Is Behind the OPM Hack*, DAILY BEAST (July 9, 2015) (reporting that Crowdstrike's allegation that China was responsible for the OPM hack was "based on technical information provided by the U.S. government").

[18] *See* Eichensehr, *supra* note 15, at 529 (discussing the risk of accountability confusion).

[19] Kristen Eichensehr, *Risky Business: When Governments Do Not Attribute State-Sponsored Cyberattacks*, NET POLITICS (Oct. 4, 2016).

[20] *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 349 (2012) (describing the "CSI effect").

[21] JASON HEALEY ET AL., CONFIDENCE-BUILDING MEASURES IN CYBERSPACE 10 (ATLANTIC COUNCIL, 2014).

[22] SCOTT CHARNEY ET AL., FROM ARTICULATION TO IMPLEMENTATION: ENABLING PROGRESS ON CYBERSECURITY NORMS 11 (2016).

[23] JOHN S. DAVIS II ET AL., STATELESS ATTRIBUTION: TOWARD INTERNATIONAL ACCOUNTABILITY IN CYBERSPACE 29 (2017).

[24] *Id.*; *see also* JUSTIN COLLINS ET AL., UNIV. OF WASH., CYBERATTACK ATTRIBUTION: A BLUEPRINT FOR PRIVATE SECTOR LEADERSHIP 26 (2017).

https://doi.org/10.1017/aju.2019.33 Published online by Cambridge University Press

These proposals for centralizing cyberattack attribution have much to recommend them, and, with the exception of the states-only Atlantic Council proposal, they wisely preserve an important, and in some cases dominant, role for nongovernmental experience, expertise, and resources for attributing state-sponsored cyberattacks. At the same time, all of the proposals face an uphill climb: they need buy-in from actors with sometimes divergent interests, and any new entity would take time to build its capabilities and credibility. In the meantime, state-sponsored cyberattacks will continue, along with the corresponding need for credible attribution.

The current system of attribution, messy and unsystematic as it is, has underappreciated virtues that could be bolstered to help foster stability in cyberspace and that suggest a continued role for a multiplicity of attributors even alongside a possible future attribution entity.[25]

The current system is decentralized, with a mix of public and private attributors and a range of attribution mechanisms. Take the attribution to Russia of the DNC and related hacks. The first attribution came from Crowdstrike, which the DNC had hired to investigate.[26] Other private companies and researchers quickly confirmed Crowdstrike's attribution to Russia.[27] Months later, the U.S. government confirmed the attribution in a public statement and later imposed economic sanctions.[28] In July 2018, Special Counsel Robert Mueller presented and a grand jury returned an indictment charging Russian intelligence officers with hacking the DNC, among other election-related targets.[29] And finally, as part of a coordinated effort to attribute a number of hacking campaigns to Russia, the United Kingdom, Australia, and New Zealand announced in October 2018 that they also attributed the DNC hack to Russia.[30]

Although rapid attribution by a single authoritative international entity might have been desirable, the DNC attribution illustrates some of the helpful features of the current decentralized attribution landscape.

First, decentralized attribution can foster transparency about states' actions in cyberspace. In the DNC case, the decentralized system allowed different attributors to act when they were ready, with Crowdstrike and other companies moving quickly and governments moving more slowly. The attribution pacing was not tailored to the most hesitant party involved; it proceeded in pieces as different attributors made their assessments and went public. Decentralization may therefore prompt faster attributions, yielding earlier transparency and thus earlier opportunities to establish defenses. Decentralization can also foster transparency in a broader range of cases. As noted above, nongovernmental attributions have outed different kinds of government activity, including espionage against human rights advocates, activity by a broader range of governments, and actions by governments that victim governments are reluctant to call out.[31] Having a multiplicity of attributors to supplement attributions by an international entity could preserve these benefits.

[25] In an upcoming article, I explore in detail how public cyberattack attributions can help to foster stability and avoid conflict in the international system and how best to structure such attributions.

[26] Alperovitch, *supra* note 7.

[27] Ellen Nakashima, *Cyber Researchers Confirm Russian Government Hack of Democratic National Committee*, WASH. POST (July 20, 2016) (discussing confirmation of the attribution by Fidelis Cybersecurity and Mandiant); Matt Tait, *On the Need for Official Attribution of Russia's DNC Hack*, LAWFARE (July 28, 2016).

[28] *See* Dep't of Homeland Security Press Office, *supra* note 9; The White House, Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016).

[29] Indictment, United States v. Netyksho et al., No. 18-cr-215, (D.D.C. July 13, 2018).

[30] UK National Cybersecurity Centre, Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed (Oct. 4, 2018); Prime Minister of Australia, Attribution of a Pattern of Malicious Cyber Activity to Russia (Oct. 4, 2018); New Zealand Gov't Communications Security Bureau, Malicious Cyber Activity Attributed to Russia (Oct. 4, 2018).

[31] *See supra* notes 11–12 and accompanying text.

https://doi.org/10.1017/aju.2019.33 Published online by Cambridge University Press

Second, a multiplicity of attributors can act as force multipliers. Investigating and attributing cyberattacks is time- and resource-intensive. Attributions by nongovernmental attributors now supplement publicly available resources and provide a way to do public attributions without compromising classified intelligence sources and methods.[32] Preserving a multiplicity of attributors could supplement whatever resources are made available to an attribution entity, which would likely remain somewhat resource constrained.

Finally, and perhaps most importantly, the multiplicity of attributors in a decentralized system can bolster the credibility of attributions in several ways. Different attributors may persuade different audiences. For example, skeptical cybersecurity researchers who might be disinclined to credit a parsimonious attribution by a victim government might nonetheless believe a detailed attribution report published by a well-respected company. Or governments around the world might credit the attribution judgment of a nonvictim government that confirms a victim's attribution. Decentralized attribution ensures that acceptance of an attribution rests on the credibility of no single institution. Also, having a multiplicity of attributors allows for cross-checking, which helps to ensure the accuracy of attributions. This could be accomplished by peer review of results reached within a proposed international attribution entity as well.[33] But decentralization is already fostering a sort of ad hoc peer review where companies have incentives to confirm or debunk others' attributions and thereby enhance (or undermine) the attributions' credibility.

Ideally, the proliferation of confirmatory attributions would come from diverse attributors, with broad geographic, political, and public/private status. The proposals for an international attribution entity recognize that diversity in the organization's membership would bolster its credibility;[34] the same would be true for diverse but decentralized attributions. The diversity of attributors has begun to increase, but only to a limited extent. In the last year, the United States, other members of the Five Eyes intelligence alliance (Australia, Canada, New Zealand, and the United Kingdom), and a couple of additional allies have undertaken several coordinated attributions, including attributing the WannaCry ransomware to North Korea[35] and cyberattacks on chemical weapons investigators and worldwide antidoping authorities to Russia.[36] Because confirmatory attributions often rely on shared intelligence, it is unsurprising that the coordinated attributions have been made by close allies. But sharing intelligence more widely, though certainly not without costs, also has a significant potential upside. Future attributions would gain credibility if the attributors included a broader range of countries and companies from around the world. Such a credibility gain might be worth the risks of broader sharing of intelligence related to cyberattack attribution.

Conclusion

The utility of attribution alone as a response to state-sponsored cyberattacks is highly debatable, but public attributions at least shed light on what states are doing in cyberspace. Private attributors have an important role to play in filling gaps when states do not attribute and in checking and supplementing states' attributions. Accurate and credible public attributions can help to build agreement about the factual realities of states' behavior in cyberspace, and agreement on facts may open the door to eventual agreement on law to govern states' actions.

[32] *See* Eichensehr, *supra* note 15, at 529. Private attributors have concerns, however, about preserving their own sources and methods. *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).

[33] *See* Charney et al., *supra* note 22, at 12.

[34] *See, e.g.*, *id.*; Davis II et al., *supra* note 23, at 27–29.

[35] *See, e.g.*, The White House, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017).

[36] *See, e.g.*, David E. Sanger et al., *Russia Targeted Investigators Trying to Expose Its Misdeeds, Western Allies Say*, N.Y. Times (Oct. 4, 2018).

https://doi.org/10.1017/aju.2019.33 Published online by Cambridge University Press