2019

Attribution by Indictment

Chimène Keitner
UC Hastings College of the Law, keitnerc@uchastings.edu

doi:10.1017/aju.2019.34

SYMPOSIUM ON CYBER ATTRIBUTION

ATTRIBUTION BY INDICTMENT

*Chimène I. Keitner**

The challenges of attributing malicious cyber activity—that is, identifying its authors and provenance with a sufficient degree of certainty—are well documented. This essay focuses on a phenomenon that I call "attribution by indictment." Since 2014, the United States has issued more than a dozen indictments that implicate four foreign states in malicious cyber activity: China, Iran, Russia, and North Korea. Ten of these indictments were issued in 2018, suggesting that this practice is likely to continue and even intensify in the near term. Attribution by indictment uses domestic criminal law, enforced transnationally, to define and enforce certain norms of state behavior in cyberspace. This essay analyzes the U.S. practice of attribution by indictment as a response to malicious cyber activity.[1]

U.S. Practice Regarding Cyber-Related Indictments

On May 29, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the Chinese military for computer hacking and economic espionage against U.S. companies.[2] Attorney General Eric Holder announced "the first ever charges against a state actor for this type of hacking."[3] Acting Assistant Attorney General for National Security John Carlin emphasized that "[s]tate actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag."[4] The five named defendants were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA). Each was charged with thirty-one counts of violating U.S. criminal law. The fifty-six-page indictment appended five exhibits. Each appendix contained a photo of a named defendant and a list of his known aliases.[5] These photos were also printed conspicuously on "wanted" posters displayed by the Department of Justice.[6]

The public announcement of this attribution by means of criminal indictment had at least three audiences. First, there was an audience of Chinese authorities and potential hackers. The United States sought to show this audience

* *Alfred & Hanna Fromm Professor of International Law, UC Hastings Law.*

[1] On the U.S. strategy, see Adam Hickey's remarks at CyberNextDC (Oct. 4, 2018); John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SECURITY J. 391 (2016).

[2] U.S. 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).

[3] *Id.*

[4] *Id.*

[5] United States v. Wang Dong, No. 14–118 (W.D. Pa. May 1, 2014).

[6] Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014).

the extent of U.S. detection capabilities and U.S. willingness to impose criminal punishment. Two years earlier, two senior U.S. officials had met with their counterparts in Beijing to confront them with proof that the PLA was hacking U.S. companies, and President Obama raised the issue with President Xi.[7] The indictment escalated the issue within the bilateral relationship, and on the world stage.

Chinese officials met the U.S. allegations, and the indictment, with outrage and denial. Chinese Foreign Ministry Spokesperson Qin Gang denounced the PLA indictment as "based on deliberately fabricated facts" and "grossly violat[ing] the basic norms governing international relations."[8] He accused the United States of being the real law-breaker through its "long [involvement] in large-scale and organized cyber theft as well as wiretapping and surveillance activities against foreign political leaders, companies and individuals."[9] China's diplomatic responses included delivering a démarche to the U.S. Ambassador to China and halting participation in the U.S.–China Cyber Working Group.[10] Ultimately, however, the United States and China committed explicitly not to hack each other's private sector targets in 2015.[11] Reports indicate that the raw volume of Chinese IP and trade secret theft declined after 2014, but causation remains unclear.[12] Declarations of success in deterring misconduct appear to have been premature.[13]

Second, the indictment spoke to a U.S. domestic audience. According to the cofounder of the CrowdStrike cybersecurity firm, the indictment "sen[t] a signal to U.S. companies that ha[d] thought that the government could not do anything to hold state-sponsored hackers accountable."[14] Third, the indictment had an international audience comprised of other foreign states and individuals, including Russian authorities and potential hackers.[15]

The Department of Justice issued another indictment for theft of sensitive data in 2014 against Su Bin, the owner and manager of a Chinese aviation technology company. Su was arrested in Canada, and eventually pled guilty to the charges.[16] The original unsealed indictment characterized his coconspirators obliquely as "affiliated with multiple organizations and entities in the PRC."[17] Two years later, when the practice of attribution by indictment was more firmly established, Assistant Attorney General Carlin explicitly identified Su's coconspirators as "hackers from the People's Liberation Army Air Force," thereby connecting the theft directly to the Chinese state.[18]

[7] Ellen Nakashima, *Indictment of PLA Hackers Is Part of Broad U.S. Strategy to Curb Chinese Cyberspying*, WASH. POST (May 22, 2014); Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015).

[8] Ministry of Foreign Affairs of the People's Republic of China, China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel (May 20, 2014).

[9] *Id.*

[10] Shannon Tiezzi, *China's Response to the US Cyber Espionage Charges*, THE DIPLOMAT (May 21, 2014).

[11] The White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015).

[12] *See, e.g.*, Jack Goldsmith, *U.S. Attribution of China's Cyber-Theft Aids Xi's Centralization and Anti-Corruption Efforts*, LAWFARE (June 21, 2016).

[13] *See* Jack L. Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2018).

[14] Ellen Nakashima & William Wan, *U.S. Announces First Charges Against Foreign Country in Connection With Cyberspying*, WASH. POST (May 19, 2014).

[15] *See, e.g.*, Andy Greenberg, *Obama Curbed Chinese Hacking, but Russia Won't Be So Easy*, WIRED (Dec. 16, 2016).

[16] U.S. Dep't of Justice, Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information (Mar. 23, 2016).

[17] United States v. Su Bin, No. 14–1318M (C.D. Cal. June 27, 2014).

[18] U.S. Dep't of Justice, Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison (July 13, 2016).

The recent surge in indictments suggests that Chinese cyber espionage remains a major problem. Two indictments unsealed at the end of 2018 explicitly charge Chinese government actors with cyber-related crimes.[19] These indictments allege that China has engaged in malicious cyber activity for commercial purposes, but Jack Goldsmith and Robert Williams note that even indictments of purportedly private Chinese actors "implicate the blurry line between state and non-state actors and between 'national security' and 'commercial' purposes," a line that is "especially blurry … in the Chinese context."[20]

In contrast to the commercially-focused Chinese indictments, U.S. indictments of Russian hackers have explicitly alleged political rather than commercial motivations.[21] Four indictments issued in 2018 allege that the defendants interfered unlawfully in domestic political processes and participated in what the Department of Justice has characterized broadly as "information warfare."[22] Deputy Attorney General Rod Rosenstein emphasized in conjunction with these indictments that "[t]he Internet allows foreign adversaries to attack America in new and unexpected ways."[23] Like the Chinese indictments, the Russian indictments have both foreign and domestic audiences, and combine law enforcement with foreign policy goals.

Functions of Attribution

Thomas Rid and Ben Buchanan have argued that "*attribution is what states make of it.*"[24] The strategic problem for defenders is "how to deter future attacks while maintaining escalation dominance"[25]—that is, how to ensure that a robust defense does not unleash a cycle of mutually destructive offensive measures.

As a technical matter, the attribution process is generally triggered by "indicators of compromise."[26] When the United States ascertains to a sufficient degree of certainty that foreign state actors are responsible for a given intrusion, government officials must decide whether, how, and to whom to communicate that finding. The requisite threshold of certainty might vary depending on a particular agency's "mission outcome."[27] While attributive statements in the intelligence and policy contexts might be accompanied by qualifiers that indicate their respective

[19] U.S. Dep't of Justice, Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years (Oct. 30, 2018); 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).

[20] Jack Goldsmith & Robert Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE (Nov. 30, 2017).

[21] The outlier is the 2017 indictment charging Russian Federal Security Service (FSB) officers with economic espionage and other criminal offenses in connection with the massive hack of Yahoo's network and webmail accounts. 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).

[22] U.S. Dep't of Justice, Russian National Charged with Interfering in U.S. Political System (Oct. 19, 2018); U.S. Dep't of Justice, U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Oct. 4, 2018); U.S. Dep't of Justice, Deputy Attorney General Rod J. Rosenstein Delivers Remarks Announcing the Indictment of Twelve Russian Intelligence Officers for Conspiring to Interfere in the 2016 Presidential Election Through Computer Hacking and Related Offenses (July 13, 2018); U.S. Dep't of Justice, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System (Feb. 16, 2018).

[23] Deputy Attorney General Rod J. Rosenstein Delivers Remarks, *supra* note 23.

[24] Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRAT. STUD. 4, 7 (2015).

[25] David E. Sanger & Nicole Perlroth, *What Options Does the U.S. Have After Accusing Russia of Hacks?*, N.Y. TIMES (Oct. 8, 2016).

[26] Rid & Buchanan, *supra* note 25, at 9.

[27] 2016 Public-Private Analytic Exchange Program Team, *Cyber Attribution Using Unclassified Data* (Sept. 9, 2016) at 2.

degrees of certainty,[28] attributions in criminal indictments are phrased definitively. In order to pursue charges, prosecutors must believe that "the person's conduct constitutes a federal offense, and that the admissible evidence will probably be sufficient to obtain and sustain a conviction."[29] Although some have criticized the Department of Justice's focus on identifying "which particular villain pressed the ENTER key"[30] as excessive, granular determinations are necessary in order to hold individuals responsible under domestic criminal law. They can also substantiate the link between the conduct and a foreign state.

Rid and Buchanan characterize the PLA indictment as "exceptionally detailed," even though it "did not reveal a great amount of attributive evidence" from a technical perspective.[31] In their assessment, "releasing these details bolstered the government's case and its overall credibility on attribution."[32] Moreover, although private companies are active in the attribution business, "only states have the resources … to attribute the most sophisticated operations with a high level of certainty."[33] Governments' attributions are not, however, free from challenge. For example, in December 2014, the FBI indicated that it "now ha[d] enough information to conclude that the North Korean government" was responsible for the cyberattack targeting Sony Pictures Entertainment—an attribution that President Obama repeated in a press conference.[34] As Christopher Painter later recounted, "many voiced doubts" about this attribution, and "instead offered a variety of alternative, often conspiratorial, theories."[35] The 2018 charges against a named member of a North Korean government-sponsored hacking team for the attack on Sony Pictures, among others, finally put these doubts to rest.[36]

Attributions by indictment combine certain policy goals of attribution with law enforcement goals of prosecution. These include *coercion*: incapacitating wrongdoers by publicizing threat intelligence and, where possible, apprehending them; *deterrence*: making the violation of U.S. law sufficiently costly to prevent repetition by the defendant (specific deterrence) or other actors (general deterrence); and *expression*: defining standards of behavior and "naming and shaming" violators, as well as broadcasting U.S. detection capabilities.

The Coercive Function

The goal of incapacitation by apprehension may remain elusive, but the forensic work done as part of criminal investigations provides information that can form the basis for other government actions. For example, in conjunction with the public attributions contained in the indictments issued by the Department of Justice, the U.S. Computer Emergency Readiness Team within the Department of Homeland Security collects and posts additional technical details on the tactics, techniques, and procedures used by cyber threat actors including China and

[28] Central Intelligence Agency, Words of Estimative Probability (1964).

[29] U.S. Dep't of Justice, Justice Manual 9–27.220.

[30] Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks* 7 (Atlantic Council Issue Brief, Jan. 2012).

[31] Rid & Buchanan, *supra* note 25, at 27.

[32] *Id.* at 28.

[33] *Id.* at 31.

[34] FBI National Press Office, Update on Sony Investigation (Dec. 19, 2014); The White House, Remarks by the President in Year-End Press Conference (Dec. 19, 2014).

[35] Christopher Painter, *US Moves to Expose North Korea's Malicious Cyber Activity*, The Strategist (Sept. 10, 2018).

[36] U.S. Dep't of Justice, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018).

Russia.[37] These details can provide the factual predicate for taking other steps, such as imposing sanctions, while also providing actionable information to potential targets.

Although incarceration can incapacitate individual wrongdoers, tools such as economic sanctions are more likely to put pressure on regimes that support malicious cyber activity—but the United States must be willing to absorb the costs associated with sanctions, such as potential disruptions in trade and economic relationships. In addition, the Department of Defense has recently articulated a strategy of "defending forward," which could serve both an incapacitation function (blocking attacks) and a deterrence function (putting attackers on notice of potential consequences).[38] As Nina Kollars and Jacquelyn Schneider note, "'defend forward' suggests a preemptive instead of a reactive response to cyber attacks."[39] Consequently, depending on what "defending forward" means in practice, it could run a heightened risk of escalation.[40] It could also make it more difficult for the United States to promote international norms of restraint in cyberspace and to encourage respect for domestic laws prohibiting cyber intrusions.

The Deterrent Function

The White House's September 2018 *National Cyber Strategy* indicates a commitment to "deter[ring] malicious cyber actors by imposing costs on them and their sponsors by leveraging a range of tools, including but not limited to prosecutions and economic sanctions, as part of a broader deterrence strategy."[41] The effectiveness of deterrence in criminal law relies on aversion to the possibility of detection and punishment. Detailed cyber-related indictments demonstrate U.S. capabilities for detecting and identifying malicious cyber activity. Uncertainty about the extent of U.S. government knowledge regarding particular cyber activities, and about whether third countries will cooperate with U.S. law enforcement in information-sharing and extradition, could also have a deterrent effect on potential attackers. The question, on an individual level, is whether the threat of detection and punishment is sufficiently large compared to the financial and other incentives individuals might have to engage in criminal conduct.

The Expressive Function

Although U.S. indictments charge individuals and entities with violations of U.S. law, some of the accompanying statements invoke international norms. For example, when the United States indicted Park Jin Hyok for hacking on behalf of North Korea, Assistant Attorney General for National Security John Demers stated that "[t]he scale and scope of the cyber-crimes alleged by the Complaint is staggering and offensive to all who respect the rule of law and the cyber norms accepted by responsible nations."[42] When the United States announced the indictment of Chinese APT10 members in December 2018, the other "Five Eyes" countries issued contemporaneous statements confirming and condemning APT10's continued targeting of organizations worldwide.[43] The ability to

[37] U.S. Computer Emergency Readiness Team, Chinese Malicious Cyber Activity; U.S. Computer Emergency Readiness Team, GRIZZLY STEPPE–Russian Malicious Cyber Activity.

[38] SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018).

[39] Nina Kollars & Jacquelyn Schneider, *Defending Forward: The 2018 Cyber Strategy Is Here*, WAR ON THE ROCKS (Sept. 20, 2018).

[40] *See, e.g.*, Lyu Jinghua, *What Really Matters in 'Defending Forward'?*, LAWFARE (Nov. 26, 2018).

[41] THE WHITE HOUSE, NATIONAL CYBER STRATEGY 8 (2018).

[42] U.S. Dep't of Justice, *supra* note 36.

[43] UK National Cyber Security Centre, Advisory: APT10 Continuing to Target UK Organisations (Dec. 20, 2018); New Zealand National Cyber Security Centre, Cyber Campaign Attributed to China (Dec. 21, 2018); Canadian Centre for Cyber Security, Malicious

forge a global agreement on standards of state behavior in cyberspace has been hampered by many factors, including the innate desire of high-capability countries to maximize their freedom of maneuver, the lack of trust among key players, and the limited benefits China and Russia appear to associate with joining a "club" of cyber-good-citizens. Even though China continues vehemently to deny that it has engaged in the alleged misconduct (rather than arguing that such conduct is lawful), agreeing on binding and universally applicable "rules of the road" in cyberspace has proved elusive.[44]

Domestic law has not traditionally been viewed as an effective tool for controlling the behavior of foreign states. Given the relative imperviousness of the four defendant regimes to attempts at public shaming, the most important audience for U.S. attributions by indictment might be U.S. allies and the public. As other states cooperate with, and stand behind, U.S. attributions, they can solidify shared understandings about appropriate state behavior and the importance of sharing and disseminating threat intelligence. The galvanizing effect of law enforcement cooperation on the ability of like-minded countries to identify the origins of malicious cyber activity, and to articulate shared understandings of prohibited behavior, might end up being the most tangible benefit of the U.S. practice of attribution by indictment.

Cyber Activity Targeting Information Technology Managed Service Providers (Dec. 20, 2018); Australian Minister for Foreign Affairs & Australian Minister for Home Affairs, Joint Media Release, Attribution of Chinese Cyber-Enabled Commercial Intellectual Property Theft (Dec. 21, 2018).

[44] *See, e.g.*, Elaine Korzak, *UN GGE on Cybersecurity: The End of an Era?*, THE DIPLOMAT (July 31, 2017).