Access, Attribution, Accountability: Three Challenges in International Cyber Law Enforcement

As the novel coronavirus ravages the globe, repositories of information are being migrated online to meet the demands of a nascent remote workforce. Cyber criminals, operating with devastating efficiency, have not missed this opportunity to exploit a flood of new online activity: infiltrating the now-ubiquitous Zoom video conferencing service, hacking hospital networks, and baiting unwary victims into providing personal and financial information. These attacks are emblematic of the sweep and sophistication of modern cybercrime. This background paper discusses the barriers to holding malicious cyber actors to account through criminal law enforcement across national borders. It explores these challenges through three lenses: access, attribution, and accountability. Moreover, it considers the role that diverse stakeholders—prosecutors, business entities, academics, technologists, and policymakers—play in addressing these challenges.

Access

In 2018, the Department of Justice’s (DOJ) Cyber Digital Task force released a landmark report assessing the Department’s work and identifying areas to improve the efficacy of cyber investigation and prosecution. The problem of access to data—the digital fingerprints upon which prosecutors rely to prove the guilt of malicious cyber actors—looms large in the report. The report notes that unlike traditional physical evidence, which can be readily identified and seized by criminal investigators, in the cyber context, “relevant data [for prosecution] is often hard to reach, hidden on computers half a world away, lurking on dark markets, or protected by anonymized host servers or encryption.” The traditional mechanism for obtaining criminal evidence abroad, Mutual Legal Assistance Treaties (MLAT), have proven slow and cumbersome in the cyber context. A 2018 RAND study regarding law enforcement access to digital evidence in remote data centers found that the “MLAT process is inadequate to meet the growing need for law enforcement access to extraterritorial digital evidence.” Increasingly conscious of the “MLAT problem,” U.S. lawmakers passed the Clarifying Lawful Overseas Uses of Data Act (CLOUD Act) in March 2018, enhancing the ability of technology companies to comply with court-ordered demands for the production of data stored extraterritorially. The CLOUD Act is, however, no panacea for U.S. investigators, as it is only operative where the overseas data in question is controlled by an entity subject to U.S. jurisdiction. When one considers the broad spectrum of cyber actors, from States and their proxies to lone wolves and politically motivated hacktivists, the narrow reach of the CLOUD Act is laid bare.

Robust, end-to-end (more colloquially, “warrant-proof”) encryption is another barrier to law enforcement personnel accessing cyber data. Domestically, this problem has manifested in the well-publicized wrangling between the DOJ and Apple regarding the Department’s repeatedly thwarted requests for Apple’s assistance in unlocking iPhones believed to contain criminal evidence. The DOJ-Apple dispute is of a piece with a broader debate about whether a law enforcement “backdoor” should be available to access encrypted user data without user consent. Indeed, technology companies that have doubled down on unassailable end-to-end encryption in defiance of strident harangues by Attorney General William Barr have become a cause célèbre among privacy advocates and legal academics. In the coming years, lawmakers will be charged with reconciling these deeply entrenched, conflicting commitments to “law enforcement tools
and authorities, information security, and individual privacy.” As one commentator has wisely noted, this fraught undertaking must give primacy to “genuinely neutral technical analysis” over the rhetorical flourishes and “loaded language” that dominate the current discourse. To that end, academicians from the legal, political science, international relations, and technology disciplines will be essential voices in charting a principled course between security imperatives and privacy expectations.

While data encryption has clear implications for criminal investigators seeking to reach criminal evidence on a given digital platform, an equally formidable access barrier occurs when law enforcement fails to learn of malign cyber activity in the first place. As noted by the White House Council of Economic Advisors, “most data breaches are not reported,” posing a “major challenge for the U.S. government in its battle against cybercrime.” This information-sharing deficit has particular salience in the finance and business sectors, where there are compelling reasons not to report cyber intrusions, including regulatory, reputational, and financial costs. Identifying this “data gap” as the “main challenge in managing cybersecurity,” a recent article in the Harvard Business Review has advocated for the establishment of a global standard for reporting cyberattacks, including from businesses. Such a standard, the authors hasten to add, would require greater participation incentives than those existing at present, including assured organizational anonymity and enhanced operational support to bolster security monitoring and reporting capacity. Nascent efforts to bridge that public-corporate divide are in the offing, including the 2018 “Paris Call for Trust and Stability in Cyberspace,” but more work is needed to translate principles into action. Just as academicians will be essential to navigating thorny balances between privacy and security, commercial actors will be instrumental in crafting an information-sharing regime that can facilitate law enforcement and security ends without exacting unacceptable fiscal outcomes—a business case for cyber information sharing, if you will. But information-sharing gaps transcend commercial actors. Indeed, information-sharing barriers persist even among law enforcement. The problem is particularly pronounced where international law enforcement agencies conduct joint cyber investigations, but remain “wary of sharing information with one another.” Unless and until individuals, businesses, and international law enforcement personnel more readily share information regarding cyber threats and intrusions, a persistent “data gap” will continue to blunt the efficacy of criminal law enforcement across national borders. Further, the data gap will exacerbate the challenges of attribution, which we now take up.

Attribution

In the context of cybercrime, examining criminal law enforcement across national borders demands an appreciation for the sheer difficulty of the enterprise, and in particular the problem of attribution. Attribution, the “process of assigning responsibility for carrying out a cyberattack,” was recently described by UCLA Law Professor Kristen Eichensehr as a “crucial predicate” to criminal indictment. As noted by Professor Eichensehr, attribution is not a unitary concept, but rather comprises elements of technical, legal, and political analysis. Eichensehr finds common analytical ground with the Hoover Institution’s Herbert Lin, who has observed that the “multidimensional” nature of attribution requires a combination of technical forensics, intelligence, and geopolitics. Commanding any one of these disciplines requires years or decades of study, training, and experience. But distilling these diverse evidentiary strands into a
defensible attribution conclusion presents a challenge that is perhaps greater than the sum of its parts. As the Office of the Director of National Intelligence’s (ODNI) 2018 Guide to Cyber Attribution candidly observes, the “painsstaking work of attribution requires several weeks or months of analyzing intelligence and forensics.” Further, even when attribution is possible, intelligence agencies and even law enforcement officers may be loath to reveal the sources and methods integral to their attribution decision. Thus, the need to protect and preserve assets and information channels essential to future attributions may have a dampening effect on criminal prosecution of cybercrime.

The technical challenges of attribution are rendered more difficult by increasingly sophisticated tradecraft employed by China, Russia, North Korea, Iran, and their proxies in the cyber domain. As malign cyber actors exact evermore complex digital and even kinetic harms, they have also invested in tools to better cover their tracks. While the ODNI report asserts that the establishment of attribution is “difficult but not impossible,” it is important to remember that attribution deals in degrees of certainty, not absolutes—what Professor Jack Goldsmith has called “good-enough attribution.” This is familiar terrain for intelligence officials, where “assessments” operate along a spectrum of confidence, probability, and risk. But for criminal investigators accustomed to obtaining evidence to sustain guilt beyond a reasonable doubt, achieving “degrees of certainty” is cold comfort.

The full spectrum of technical, legal, and political components of attribution have been on display in recent years. The 2015 Sony Pictures case is an instructive example. The U.S. government formally accused North Korea of hacking Sony Pictures Entertainment, destroying Sony network systems, and stealing data. In short order, a wave of critics cast doubt upon the veracity of the FBI’s conclusions. That criticism was fueled by technical and legal considerations. As to the former, skeptics pointed to forensic indicators that the hackers were likely aided by Sony insiders. Regarding the latter, controversy regarding the U.S. accusation is in part attributable to the indeterminate standard of proof “states must meet when accusing other states of internationally wrongful acts.” Finally, a political calculus animated White House debates about directly confronting North Korea, weighing vindication of U.S. security interests against the maintenance of bilateral ties with Asian partners, such as Japan, that opposed public accusation. The Sony Pictures case—marked by impugned technical analysis, an indeterminate legal standard of proof, and competing political considerations—thus vividly illustrates the magnitude and complexity of the attribution challenge. But a discernable trend toward greater “coordinated attribution”—involving multilateral cooperation and coordinated attribution statements—augurs well for mitigating such challenges. For example, the May 2017 WannaCry ransomware attack and June 2017 NotPetya cyberattack were both met with a host of coordinated attribution statements from, among others, the United States, United Kingdom, Australia, New Zealand, and Canada.

Accountability

Despite these challenges, the U.S. government has invested heavily in enhanced attribution capabilities through a “whole of government” approach spanning its law enforcement, intelligence, and defense sectors. These investments have paid dividends. The U.S. government has shown enhanced capability and willingness to publicly attribute malicious cyber activities to
foreign governments, as well as agents acting on their behalf. But in an environment where precision attribution is increasingly available, the question remains what method of public accountability—if any—is appropriate. As with attribution, these accountability decisions require cross-cutting analysis. Selecting from the four prevailing public accountability mechanisms (criminal indictment, sanctions, technical alerts, and official statements) in response to cybercrime across national borders requires weighing technical factors, legal parameters, and foreign policy implications.

In recent years, a primary U.S. government avenue of public accountability for foreign state-linked hackers is criminal indictment. Perhaps unsurprisingly, few of these indictments lead to an actual prosecution. Nor is that the point. Rather, the indictment strategy is often predicated on a deterrence theory. Professor Goldsmith—a critic of the indictment strategy—acknowledges at least some deterrent effect is achieved through an indictment’s demonstration that the “U.S. government can burrow deeply into foreign intelligence services . . . and pick out their individuals and activities with extraordinary precision.” But the modest deterrence benefits of indictment may be outweighed by significant costs. For example, Professor Goldsmith observes that a U.S. demonstration of precision attribution capacity necessarily compromises the future use of those capabilities. Further, the scant number of successful foreign state cyber prosecutions renders indictment a paper tiger, which may act to embolden additional state-sponsored cyber intrusions.

The indictment of foreign state actors for cybercrimes is also at odds with the “general U.S. policy of not indicting foreign officials whose acts may carry some imprimatur of state action.” Recent, high profile U.S. indictments of individuals for foreign state-linked cybercrimes include four members of China’s People’s Liberation Army accused of hacking into Georgia-based Equifax, nine Iranians acting as agents of the Islamic Revolutionary Guard Corps accused of hacking hundreds of U.S. universities, and twelve Russian intelligence officers accused of hacking the Democratic National Committee. This pattern of aggressive indictment for state-sponsored hacking has set an unsettling precedent for current and former cyber operators in the U.S. military and intelligence services. Former U.S. military cyber warfare officer Robert Lee, writing in Wired, finds this pattern “troubling,” and argues that indictments should be focused on malicious government action, rather than on their cyber agents. Further, he notes that an aggressive U.S. government indictment program raises the spectre of U.S. military and intelligence officials being criminally charged abroad for their cyber actions on behalf of the U.S. government. Finally, he suggests that indictments focused on individuals (including their picture, name, age, and military or commercial affiliation) allow nations directing cybercrime to shift the narrative toward the individuals working at their behest.

Given the substantial criticism of criminal indictment as a method of cybercrime accountability, a number of commentators have urged that the U.S. government shift to more nation-focused approaches including public statements (“naming and shaming”) and economic sanctions. Naming and shaming, for example, obviates the need for publicizing U.S. cyber surveillance and investigatory capabilities that is implicit in necessarily granular indictments, preserving such tools for future use. At the same time, an increasingly robust sanctions regime now provides for cyber sanctions in response to malicious cyber activities and election interference. While the drawbacks of criminal indictment have been widely catalogued, public statements or sanctions
alone are a necessary but not sufficient component of cyber accountability decisions. For example, in dealing with China—whose rampant cyber intrusions and intellectual property theft against U.S. agencies and companies are well documented—it may be difficult to parse cyber-focused sanctions from those imposed as part of the ongoing trade war, reducing their symbolic and substantive bite. Furthermore, the weight of other economic and foreign policy implications can quickly preclude the imposition of cyber sanctions. Indeed, this was precisely the case in 2018, when Treasury Secretary Mnuchin blocked sanctions against China, proposed in response to intellectual property theft, in the interest of pending trade negotiations. Moreover, cyber-sanctions can be sidelined for other economic considerations, including fear of retaliatory measures taken against U.S. companies operating in China. Such calculations illustrate, as with attribution, that accountability decisions are made amidst a complex backdrop of technical, foreign policy, economic, and legal considerations.

* * *

As the 2020 Yale Cyber Leadership Forum takes up the topic of Criminal Law Enforcement Across National Borders, we can all look forward to the insights of leaders in government and business that must directly confront emerging cybercrimes, and those nations and individuals that carry them out, in a very direct way. Leaders in government and business must work together to meet the challenges of access, attribution, and accountability if we are to succeed in improving criminal law enforcement in a cyber domain that transcends national borders.

**Background Readings: Criminal Law Enforcement Across National Borders**


* Joel Coito currently serves as a Judge Advocate in the U.S. Coast Guard. The views expressed in this posting are those of the author and do not reflect the official policy or position of the U.S. Coast Guard, the Department of Homeland Security, or the U.S. government.