Cite as Hinck & Maurer, 10 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2020)

Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity

Garrett Hinck & Tim Maurer*

INTRODUCTION

The question of how states attribute responsibility for malicious cyber activity to other state actors has provoked much attention from both policymakers and scholars.[1] Yet one approach to this problem has not been analyzed in depth: the use of criminal charges to allege or suggest state responsibility for cyber incidents. The United States has increasingly used this instrument since 2014. Its Department of Justice in fact adopted an explicit goal of bringing charges against foreign actors responsible for cyber activity.[2] Federal prosecutors have unsealed a series of indictments and criminal charges against Chinese intelligence officers involved in the theft of intellectual property and Iranian and North Korean individuals who carried out destructive cyber attacks on behalf of their governments. This also includes charges against Russian intelligence officers alleged to have interfered in the 2016 U.S. election.

This increasing number of criminal charges raises several important questions: What are the goals of these criminal charges, especially those against foreign intelligence officers unlikely ever to be arrested by U.S. law enforcement? Are criminal charges merely a more formal approach to alleging state responsibility than leaking statements from "senior administration officials" to the media about cyber threats from other states? And how should this strategy of bringing criminal charges be evaluated in the context of broader U.S. policy efforts to combat malicious cyber activity? How does it interact with the Justice Department's stance of independence from political considerations?

The U.S. first publicly brought criminal charges that explicitly alleged that a foreign state played a role in malicious cyber activity in 2014, with charges against five officers in the Chinese People's Liberation Army (PLA) for stealing intellectual property (IP) from a number of U.S. companies, including Westinghouse, U.S. Steel, and Alcoa. Since then, the Justice Department has brought or unsealed twenty-three additional sets of charges, some of which specifically alleged foreign state responsibility for online influence operations, a category often discussed in tandem

* Garrett Hinck is a researcher at the Carnegie Endowment for International Peace working on nuclear and cybersecurity policy. Tim Maurer is Co-director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace. In 2018, Cambridge University Press published his *Cyber Mercenaries: The State, Hackers, and Power*, a comprehensive analysis examining proxy relationships between states and hackers.

The authors wish to thank Jon Bateman, Michael Daniel, Martha Finnemore, Jonah Hill, Duncan Hollis, Matthew Noyes, officials at the U.S. Department of Justice's National Security Division, and the experts at the workshop organized by Third Way's Cyber Enforcement Initiative for providing invaluable comments and feedback on this article.

[1] Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 974 (2011).

[2] *See* Adam Hickey, senior Dep't of Justice official, Remarks at CyberNext DC (Oct. 4, 2018), https://perma.cc/5FQX-MT5G.

with malicious cyber activity. These criminal charges have been brought against individuals from China, Russia, North Korea, Iran, and Syria. The 2018 National Cyber Strategy named all but the last of these countries as adversaries against the United States in cyberspace.

This article addresses the policy implications of criminal charges against foreign hackers with conceptual and empirical analysis. It consists of five sections. The first section provides background and discusses previous attempts to fit criminal charges into policy analysis. Next, the second section proposes a conceptual framework for criminal charges as a response to nation-state hacking. It describes how criminal charges differ from other responses and the varied aims that the U.S. can pursue with indictments. The third section then discusses the choices that policymakers must make in deciding whether and how to use criminal charges. In the fourth section, the article applies the conceptual framework to case studies for each of the states (China, Russia, Iran, Syria, and North Korea) that U.S. indictments have named as backing malicious cyber activity thus far. The fifth section discusses trends in the record of criminal charges as a whole. Lastly, this article evaluates the current and future role of criminal charges as a component of U.S. cyber policy. In particular, it proposes that charges can have value as a means of "persistent enforcement" by disrupting foreign hackers.[3]

I. BACKGROUND

Nation-state cyber intrusions have led to some of the largest and most consequential thefts and attacks on the United States in recent years. The hack of the Office of Personnel Management in 2015 alone put the personal records of 21.5 million federal workers with security clearances in the hands of a foreign government.[4] The twin ransomware worms, WannaCry and NotPetya, caused billions in damage to U.S. companies.[5] Industry leaders and U.S. intelligence officials have decried the mass theft of intellectual property from U.S. corporations – with former NSA Director Keith Alexander calling it "the greatest transfer of wealth in human history."[6]

However, state involvement in malicious cyber activity is not binary. A state's hackers may or may not be officers in their intelligence services or militaries or they may be independent hackers or even part of criminal groups. Much of the activity that is described as "state-sponsored" is in fact carried out by such proxies whose relationship to the state falls in a spectrum from outright delegation of specific missions to non-governmental actors to more ambiguous orchestration and

[3] This term is loosely associated with the 2018 Command Vision for U.S. Cyber Command focusing on "persistent engagement." *Achieve and Maintain Cyberspace Superiority*, U.S. CYBER COMMAND (Apr. 2018), https://perma.cc/WH43-KGJF.

[4] Ellen Nakashima, *Hacks of OPM database compromised 22.1 million people, federal authorities say*, WASH. POST (July 9, 2015, 8:33 PM), https://perma.cc/7T77-MSYV.

[5] Jonathan Berr, *WannaCry ransomware attack losses could reach $4 billion*, CBS NEWS (May 16, 2017, 5:00 AM), https://perma.cc/6BS4-Q5TC; Kim Nash, Sara Castellanos & Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*, WALL ST. J. (June 27, 2018, 12:03 PM), https://perma.cc/Z3VM-8H7U.

[6] Josh Rogin, *NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history*, FOREIGN POLICY (July 9, 2012, 6:54 PM), https://perma.cc/WT9W-T8QE.

sanctioning of criminal and other hacker groups.[7] Moreover, since proxy actors' motivations are multifaceted themselves in that they may be working for their states out of a sense of patriotic motivation, for financial opportunities, or to avoid prison or other penalties, assessing which activities qualify as state-linked is a complicated task.

It is in response to the threat of state-sponsored cyber activities that the U.S. government has rolled out a series of new policies – including the 2018 National Cyber Strategy's Cyber Deterrence Initiative and the much-discussed changes to the guidelines for the use of offensive cyber weapons.[8] Criminal charges have formed a critical component of the response from the FBI and Department of Justice – which investigate nation-state cyber incidents that affect domestic companies and individuals.

Yet, the unsealed criminal charges that allege state responsibility for foreign hacking are unusual when compared to the Justice Department's common practices. As mentioned, in a number of cases, the Justice Department has publicly charged individuals it does not have custody over and who are unlikely to ever see the inside of a U.S. courtroom. Only 6% of charged individuals listed in our data set have been arrested to date. Even more unusually, a number of these individuals have been officers in other states' militaries or intelligence services. And last, and perhaps most vitally – criminal charges' effect on state adversary behavior remains unclear. Russia has deflected a number of charges against its spy services and appears to be more than happy to target Western politicians and infrastructure. And China has continued its wide-reaching thefts of U.S. intellectual property – even as the 2015 U.S.-China deal to stop such activity broke down in late 2018 and the U.S. unsealed yet more charges alleging Chinese economic espionage.

Since 2014, the Department of Justice has unsealed, at least, 24 cases and 195 counts against 93 foreign nationals that either explicitly allege or where we have reason to believe foreign state responsibility for malicious cyber activity or foreign influence operations. Sixteen of the 24 have come in the Trump administration. Seven were against Chinese hackers, seven were against Iranians, six were against Russians, three were against Syrians, and one was against a North Korean hacker. Of these, seven have come since August 2018, when the Trump administration released its Cyber Strategy. Figure 1 shows how the frequency has picked up in the last year:

[7] TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 20 (2018).

[8] WHITE HOUSE, 2018 NATIONAL CYBER STRATEGY 21 (Sept. 2018), https://perma.cc/F445-8XP6; *see also* RECOMMENDATIONS TO THE PRESIDENT ON DETERRING ADVERSARIES AND BETTER PROTECTING THE AMERICAN PEOPLE FROM CYBER THREATS, OFFICE OF THE COORDINATOR FOR CYBER ISSUES, U.S. DEP'T OF STATE (May 31, 2018). For offensive cyber policy changes, see Dustin Volz, *Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive*, WALL ST. J. (Aug. 15, 2018, 11:36 PM), https://perma.cc/EX7N-LPFA; *see also* Erica Borghard, *What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?*, COUNCIL ON FOREIGN RELATIONS (Sept. 10, 2018), https://perma.cc/Q2KW-PR2Q.

Figure 1. Timeline of Criminal Charges Against Foreign Hackers (by filing date)

2019	May (Unsealed May 2019)	Fujie Wang and John Doe (China) - Anthem Hack
	Feb (Unsealed Feb 2019)	Witt et al. (Iran) - Espionage against U.S. intelligence orgs
2018	Dec (Unsealed Dec 2018)	Zhu and Zhang (China) - MSS Cloudhopper IP Theft (APT 10)
	Nov (Unsealed Nov 2018)	Savandi and Mansouri (Iran) - SamSam Ransomware
	Oct (Unsealed Oct 2018)	Zhang et al. (China) - JSSD Hacking of Aerospace Cos.
	Oct (Unsealed Oct 2018)	Morenets et al. (Russia) - GRU Anti-Doping Orgs, OPCW Hacks
	Sep (Unsealed Oct 2018)	Elena Khusyaynova (Russia) - Project Lakhta Influence Operation
	Jul	Netyshko et al. (Russia) - DNC, DCCC Hacks and 2016 Election
	Jun (Unsealed Sep 2018)	Park Jin Hyok (North Korea) - Sony, WannaCry, Bangladesh bank
	May	Umar Agha and Firas Dardar (2nd set of charges) - Syrian Electronic Army
	Feb (Unsealed Mar 2018)	Mabna Institute (Iran) - IRGC-linked IP theft campaign
	Feb	Internet Research Agency (Russia) - Election influence operations
2017	Nov (Unsealed Nov 2017)	Behzad Mesri (Iran) - Hack of HBO
	Sep (Unsealed Nov 2017)	Wu Yingzhou et al. (China) - Boyusec IP theft
	Aug (Unsealed Aug 2017)	Arrest of Yu Pingan (China) - OPM hack-linked malware
	Feb (Unsealed Mar 2017)	Dokuchaev et al. (Russia) - Yahoo Hack
2016	Apr (Unsealed Jul 2017)	Ajily and Rezakhah (Iran) - Arrow Tech IP Theft
	Jan (Unsealed Mar 2016)	ITsec and Mersad Co. (Iran) - Financial Sector DDoS, Bowman Dam
2015	Sep (Unsealed Mar 2016)	Peter Romar and Firas Dardar (Syria) - Syrian Electronic Army
2014	Jun	Arrest of Su Bin (China) - Boeing hack (C-17 IP Theft)
	Jun (Unsealed Mar 2016)	Umar Agha and Firdas Dardar (Syria) - Syrian Electronic Army
	May (Unsealed Jun 2014)	Evgeniy Bogachev (Russia) - GameOver Zeus Botnet
	May (Unsealed May 2014)	PLA Unit 61398 (China) - Economic Espionage (aka APT 1)
2013	Nov (Unsealed Dec 2015)	Arrest of Nima Golestaneh - Arrow Tech IP Theft

Then-Assistant Attorney General for National Security at the Department of Justice, John Carlin, a key official responsible for the initial push on indictments of state-linked hackers, wrote about the integration of law enforcement into a "whole of government approach" to combating cyber threats in 2016.[9] With the significantly larger number of criminal charges now publicly available, the time is ripe for a policy-focused analysis of the use of charges to complement other emerging literature on the topic, focusing on indictments in the context of deterrence of offensive cyber operations, as well as on the formation of norms of international behavior in cyberspace.[10]

II. CONCEPTUAL FRAMEWORK

[9] JOHN P. CARLIN & GARRETT M. GRAFF, DAWN OF THE CODE WAR 47-48, 201-05 (2018); John Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SECURITY J. 391 (2016).

[10] Martha Finnemore & Duncan Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, EUR. J. INT'L L. (forthcoming 2019); Nathan Ryan, *Five Kinds of Cyber Deterrence*, 31 PHIL. & TECH. 331 (2017).

This section details a framework for understanding criminal charges and their utility to policymakers. It first establishes what makes criminal charges a unique tool, then elaborates the purposes that criminal charges can serve, and finally discusses considerations for integrating charges with broader cyber policy goals.

A. Distinguishing characteristics of criminal charges

Criminal charges differ from many other ways of responding to cyber incidents – such as formal diplomatic demarches, public statements from senior officials, or punitive actions like sanctions or even offensive cyber operations. They combine a public communications function with a punitive function – and they do so under a particular set of constraints – all of which make criminal charges a unique instrument from a policy perspective. In brief, criminal charges stand apart because (1) they require the presentation of evidence to either a grand jury or a judge with an attestation that the U.S. government can prove its allegations in a public trial; (2) they target specific individuals, not states writ large; (3) they are intended to enable arrests as opposed to just being public statements.

First, criminal charges require a high standard of publicly-releasable evidence. To bring criminal charges, federal prosecutors must convince a majority of a grand jury or a federal judge that there is probable cause to believe the defendant is guilty. The prosecutors must then be prepared to prove at a later stage, before a jury, that the defendant is guilty "beyond a reasonable doubt."[11] This is a higher burden of proof – and proof that must lay out its evidence in public and be challenged in a criminal trial before an independent judge and jury - compared to the standards of information on which policymakers usually make decisions in the national security space.[12] Prosecutors must thus consider whether they actually have the requisite evidence of criminal violations that meets a high standard of proof. This is complicated for cyber incidents where information collected through intelligence means is often inadmissible in a courtroom or would disclose sensitive intelligence sources and methods. In contrast to other ways that the U.S. can point its fingers at adversaries such as a public statement, criminal charges require it to lay out its evidence, show where the evidence was obtained at a high level of detail, and assert that it can hold up in a criminal trial before an independent judge and jury. This limits criminal charges' utility as a policy tool since such evidence may simply not be available in certain cases or not available at the most useful moment to bring charges.

Second, criminal charges are individual-centric. This raises both challenges and opportunities for policymakers, since the primary question of interest from a foreign policy perspective is not which person carried out the attack but which state is responsible. For instance, when the FBI attributed the attack on Sony Pictures in 2014, it noted the North Korean government was

[11] *Federal Indictments: Answers to Frequently Asked Questions*, BURNHAM & GOROKHOV (2009), https://perma.cc/8TA2-PB3M.

[12] *See generally* Frederic Lemieux, *Six Myths About National Security Intelligence*, THE CONVERSATION (Jan. 31, 2017), https://perma.cc/GMQ9-QL3N (broad overview); *see also* James Clapper, *Intelligence Community Directive 203: Analytic Standards*, ODNI (Jan. 2, 2015), https://perma.cc/CH3R-32Z6 (more detailed discussion).

responsible for the attack – but did not name any individuals.[13] Naming individuals is challenging – especially individuals operating within closed societies like North Korea or within intelligence agencies – so just collecting enough evidence to name specific individuals can be a challenge. But in many instances, even pinpointing a specific individual does not clearly establish state responsibility, as discussed above. When prosecutors unseal criminal charges against hackers acting as a proxy, they could have the choice of whether to allege state sponsorship – and thus modulate or heighten the impact of the criminal charge's accusations. And even when the named hackers are integrated into a state's military or intelligence apparatus, policymakers must make choices about the individuals named. How high up the chain of command should they go, that is, to what extent can they prove a criminal conspiracy among higher officers? What effects will disclosing the identities of these officers have?

Third, criminal charges are a necessary predicate for law enforcement actions. This is obvious – federal authorities generally need a grand jury indictment to make an arrest. In this way, unsealed criminal charges both communicate about a cyber incident and form a basis for action in response, specifically against the charged individuals. This is a significant difference from other responses like public statements.

B. Purposes

There are a number of ways that criminal charges have utility for policymakers. And this utility changes from short-term response to specific incidents to, in the longer-term, contributing to enforcing international norms of behavior in cyberspace. It is useful to consider the varying purposes in a spectrum of time since the originating incident because unsealing criminal charges can serve both immediate purposes and have effects that play out over a longer period. In most cases, criminal charges serve multiple ends, and they do this with varying effectiveness. Sometimes, the different purposes complement each other, and other times they are at odds. For example, when an indictment is kept under seal in the hope of making an arrest, it does not have the public communicative functions described below. The next section discusses how criminal charges contribute to broader policy efforts by publicizing attribution, satisfying domestic audiences that can include victims, punishing the responsible individuals, disrupting ongoing or future malicious activity, naming and shaming adversary states, cooperating with allies, and contributing to the formation of international norms of behavior.

In the short term, immediate response to a cyber incident, the primary purpose of unsealing criminal charges relates to *attribution.*[14] It is worth noting that before the series of criminal charges

[13] FED. BUREAU OF INVESTIGATION, UPDATE ON SONY INVESTIGATION (Dec. 19, 2014), https://perma.cc/5D4H-EHS6.

[14] Note that attribution from a governmental perspective has two components that come in sequence. First, internally the relevant agencies combine different sources of intelligence to reach a conclusion with a reasonable degree of confidence about which actor is responsible for the activity. Second, public attribution is the decision to make the internal attribution known to the world. This is a policy decision. When we discuss attribution we refer to the second component, public attribution. For more, see the distinction between the technical and strategic levels of attribution in Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks* 38 J. STRATEGIC STUD. 4, 9 (2015).

began in 2014, there was a prominent debate in academic and technical communities about the feasibility of attributing state-backed cyber activities, with literature around 2014 arguing that better attribution was possible but not yet demonstrated.[15] In late 2014, when the FBI publicly attributed the Sony hack to North Korea, this prior sense of uncertainty provoked some controversy about the validity of that attribution.[16]

First, criminal charges can directly attribute activity to a target state. This was the case with the hack of Yahoo! where the indictment revealed that Russian intelligence officers had broken into the email provider.[17] In these cases, criminal charges do not provide an initial attribution but can provide clarity to the technical community when disputed attributions exist.

Second, attributions – and particularly attributions in the form of criminal charges - can respond to pressure from the private sector to "do something" in response. Often, companies find that disclosing that the perpetrator behind a massive breach or attack on their services is a nation state can help to avoid hard questions about their security and instead focus attention on how the U.S. government can protect them. In the case of the 2011-2013 distributed denial of service (DDoS) attacks against major U.S. financial institutions, the March 2016 indictment against a cadre of Iranian hackers was largely in response to demands from big banks for the U.S. to take some kind of public action in response.

Third, in cases where the U.S. government has already made a formal attribution, criminal charges can buttress these claims with detailed technical evidence. The technical community of cybersecurity experts working at private companies in the United States and abroad has often questioned attributions of nation-state activity that do not provide explanations or further evidence detailing how the U.S. arrived at its conclusions. This is not confined to technical experts. Political figures also dispute official attributions – as President Trump did when the U.S. intelligence community attributed the 2016 election interference operations to Russia's GRU and FSB.[18] Special Counsel Robert Mueller's two 2018 indictments of Russians for social media hijacking and election hacking helped support the intelligence community's conclusions in the public's eyes.

Fourth, criminal charges do more than just provide a statement of attribution because they provide a legal basis to *punish* – when indictments actually lead to arrests. Criminal charges indicate that the U.S. government aims to hold those responsible for a cyber attack responsible and to provide *retribution* for the victims of that attack. Punishment through the criminal justice system is one means to achieve that ends. However, public indictments of state-backed actors, especially of individuals in security services, are often unlikely to actually bring those named to justice, even though the Justice Department has arrested a small number of foreign hackers. But in the context of state-sponsored hacking, criminal charges do not just hold the charged individuals responsible.

---

[15] Jon R. Lindsay, *Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattacks*, 1 J. CYBERSECURITY 53, 63 (2015); Rid & Buchanan, *supra* note 14, at 7.

[16] FED. BUREAU OF INVESTIGATION, *supra* note 13; David Auerbach, *Don't Trust the FBI Yet*, SLATE (Jan. 7, 2015, 2:31 PM), https://perma.cc/XN2B-RMGC.

[17] Vindu Goel & Eric Lichtblau, *Russian Agents Were Behind Yahoo Hack, U.S. Says*, N.Y. TIMES (Mar. 15, 2017), https://perma.cc/PSS9-L7G3.

[18] Kristina Peterson, *Republicans Reproach Trump on Russian Meddling*, WALL ST. J. (July 16, 2018, 4:59 PM), https://perma.cc/Y4YK-36L7.

They hold the state that directed, controlled, or provided instructions to its agents to carry out the attack responsible as well; this is a unique purpose for criminal charges in this space.

In the medium-term, the purposes of criminal charges relate to *disruption* and *diplomacy.* First, criminal charges can have direct purposes related to *disrupting* malicious activity. Criminal charges let law enforcement authorities seize persons or property, including online infrastructure, like web domains or online accounts, involved in the operations, as discussed above. However, public criminal charges of state-linked hackers often do not lead to arrests because the hackers are safe in the target state or in countries with no extradition treaty with the United States. In these cases, the public disclosure of the alleged hackers' tools and techniques is helpful to the technical community in both attributing and defending against activity from the same threat actor. Criminal charges may help motivate the adoption of security measures based upon shared technical information – for instance, an alert from the U.S-CERT would be more ideal to share indicators of compromise (IOC) – which may not be relevant to the specific criminal charges but would be key information to defend against further activity by the same actor.[19]

In addition, criminal charges could potentially have a disruptive effect on the target state's relationship with its proxies.[20] Since the hackers that work for U.S. adversaries like Russia and Iran are often not official governments employees but instead operate out of front companies with varying degrees of state oversight, calling out individuals puts them in an uncomfortable spotlight. Criminal charges impose costs on individuals; even if they are not arrested, they cannot travel or do business in the United States or countries which may cooperate with U.S. law enforcement, such as those countries with and extradition treaty with the U.S. Public charges may expose individuals as being in the employ of intelligence or security services, which may have a reputational cost.[21] And those security services may not want to employ those hackers in the future. In the medium-term, this could have an effect of either distancing those proxies from the target state or dissuading other hackers from signing up to work as proxies.

Under slightly different circumstances, criminal charges can have a converse purpose: they can aim to incentivize states to reassert control over their proxies, whose activities may not have endorsement from top policymakers. For instance, the criminal charges of criminal hacker groups operating out of Syria and Iran which are clearly tacitly tolerated by their respective governments, could be a way of showing that the U.S. has taken interest in the groups and would like to pressure the regimes to stop their activities.

[19] For example, recently released U.S. CERT technical alerts which provide IOCs include U.S. CERT, AA19-024A, DNS INFRASTRUCTURE HIJACKING CAMPAIGN (2019); U.S. CERT, TA18-275A, HIDDEN COBRA – FASTCASH CAMPAIGN (2019).

[20] For more information about other policy responses to disrupt state-proxy relationships, see Maurer, *supra* note 7, at 139.

[21] For example, one of the most prominent disclosures resulting from the indictment of several Russian intelligence officers for hacking numerous anti-doping groups and chemical weapons watchdogs was that the reveal of their names (also published by the Dutch and UK governments) allowed an investigative group to identify a list of 305 GRU operatives from a vehicle registration list. *305 Car Registrations May Point to Massive GRU Security Breach*, BELLINGCAT (Oct. 4, 2018), https://perma.cc/4M99-CESG.

Discussions of efforts to enhance cyber *deterrence* have in some cases touched on criminal charges.[22] To the extent that criminal charges establish the ability and willingness of the United States to attribute responsibility for major malicious cyber activity to its adversaries, criminal charges do have a bearing on this discussion. But by itself attribution is not a deterrence strategy and the question of whether the U.S. is deterring its adversaries is an entirely separate evaluation that would have to consider a number of other factors such as what specific activities the U.S. aims to deter, the states' relationship with the U.S., among others. Based on the existing record, bringing criminal charges against foreign hackers and online influence operators does not appear to impose enough costs on adversaries to convince them to cease from further malicious activity.

However, it may be possible that by adding more operational friction to adversary hackers – for instance by forcing them to factor the cost of attribution or arrests of their hackers or proxies into their calculations, state-backed hackers might follow much stricter operational security procedures to avoid detection. In this way criminal charges can add costs to constrain the adversary's broader actions. Another form of cost imposition is through "naming and shaming" – which commentators have often pointed out is unlikely to deter the target state by itself.[23] In a theoretical view, naming and shaming works within the wider social system of international states by labeling certain behavior as deviant, mobilizing public opinion and other states to condemn the behavior, and making it more and more costly for the target state to continue its deviations from accepted norms.[24] As mentioned, discussion of criminal charges has focused on whether this theory is applicable in practice. These discussions often miss other potential diplomatic goals like pressuring the target state to take a related, affirmative action, such as agreeing not to use certain types of attacks or put certain targets off limit. The 2014 PLA hackers indictment ultimately seemed to play a role in a broader U.S. campaign to put pressure on China to agree not to conduct cyber-enabled economic espionage, which culminated in the September 2015 U.S.-China agreement.[25]

Additionally, in terms of diplomacy, criminal charges can be a component of reassurance or partnership with allies and other governments to respond to an incident that has global effects. Criminal charges are increasingly a tool the U.S. deploys as part of joint actions with like-minded governments to attribute and respond to state-backed hacking. As an example, in October 2018, when the governments of the UK, the Netherlands, Canada, as well as the United States jointly attributed a hacking campaign against the Organisation for the Prohibition of Chemical Weapons (OPCW), the World Anti-Doping Agency (WADA), and sports anti-doping agencies around the world to Russia's military intelligence agency, the GRU, the Justice Department unsealed an

[22] Ryan, *supra* note 10 at 335; *see* Jack Goldsmith & Robert Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE BLOG (Dec. 28, 2018, 9:00 AM), https://perma.cc/2ZQA-ZLWC.

[23] Chris Bing, *Former NSA hackers: Yahoo indictments won't slow down Russian cyberattacks*, CYBERSCOOP (Mar. 17, 2017), https://perma.cc/M7G7-ANKP.

[24] Mathrew Krain, *J'Accuse! Does Naming and Shaming Perpetrators Reduce the Severity of Genocides or Politicides?*, 56 INT'L. STUD. Q. 574, 576 (2012).

[25] Adam Segal, *The U.S.-China Cyber Espionage Deal One Year Later*, NET POLITICS, COUNCIL ON FOREIGN RELATIONS (Sept. 28, 2016), https://perma.cc/CX66-ZUQV.

indictment against seven named GRU officers for the same activities.[26] However, no U.S. allies have publicly brought their own criminal charges that specifically allege state responsibility for malicious cyber activity, which raises the question whether it is a matter of resources, domestic law, or policy willingness inhibiting other states from pursuing criminal charges.[27]

Finally, in the long-term, criminal charges contribute to the United States' effort to build and enforce norms and rules of the road for cyberspace. Unsealing criminal charges helps to clarify which types of activities the U.S. considers as violating norms, especially if Justice Department officials emphasize this in their public comments. Criminal charges are helpful because they are about a concrete set of actions, rather than the vaguer concepts referred to in norms agreements like "the proliferation of malicious ICT," which can be hard to define in practice.[28] When they are a part of a broader set of initiatives to build and enhance international norms, criminal charges can play a role in reinforcing acceptable standards of state behavior. Moreover, as Finnemore and Hollis argue, criminal charges (and accusations more broadly) could play a significant role in shaping customary international law through the emerging *opinio juris* of legitimate state behavior in this domain.[29] In this regard, criminal charges may be contributing to a broader trend in international law toward greater individualization of enforcement measures.[30] While it is impossible to assess this development in terms of a single case, it is important to consider how the foreign hacking charges will influence future international norms of behavior in cyberspace.

III. CRIMINAL CHARGES AS POLICY: CONSIDERATIONS

Whether criminal charges should be used as a policy tool is a contested issue, even within the U.S. government. Using their autonomy, officials in the Justice Department have advanced their strategy of foreign hacking charges despite concerns from other agencies and departments that traditionally manage U.S. foreign policy. Therefore, one reason that some criminal charges appear

[26] Press Release, 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://perma.cc/5TKH-EXPE.

[27] Although we could find no evidence of such charges, there may be analogues in the UK's charging of the two named GRU officers for the Skripal attacks. However, these charges did not involve cyber activity. Vikram Dodd, *Salisbury poisonings: police name two Russian suspects*, GUARDIAN (Sept. 5, 2018, 7:54 AM), https://perma.cc/59L8-VVZT. Another subject for future research – beyond the scope of this paper – would be to examine if other countries' criminal justice systems could be used in similar ways to U.S. criminal charges or if differences in process (such as approval process for indictments) prevent other countries from taking similar measures. One case to examine is when the Dutch defense intelligence service took custody of four of the GRU hackers who were indicted on October 4, 2019. The MIVD intercepted them in the course of an operation in April 2018 and then expelled them. The Dutch prime minister defending the decision not to hold the officers, saying it was not a criminal inquiry. *Russia cyber-plots: Dutch defend decision not to arrest suspects*, BBC (Oct. 6, 2018), https://perma.cc/8XCQ-DEVH.

[28] Garrett Hinck, *Private-Sector Initiatives for Cyber Norms: A Summary*, LAWFARE BLOG (June 25, 2018, 7:00 AM), https://perma.cc/G4Q7-LEMC.

[29] Finnemore & Hollis, *supra* note 10, at 11.

[30] *See generally* Larissa van der Herik, *The Individualization of Enforcement in International Law: Exploring the Interplay between United Nations Targeted Sanctions and International Criminal Proceedings*, *in* THE PURSUIT OF A BRAVE NEW WORLD IN INTERNATIONAL LAW 234 (Tiyanjana Maluwa et al. eds., 2017).

to clash with foreign policy efforts from other parts of the government could be that those agencies and the Justice Department disagree on the relative priority of competing interests.

Prosecutors must consider all the below factors in their decision process, which has several different relevant questions that determine the impact of their decision. First, they must decide whether to bring charges at all. If they do so, they then must consider whether to explicitly allege foreign state responsibility – a fraught question for all the reasons discussed in this article. Next, should prosecutors keep the indictment under seal in order to potentially arrest those charged or make the charges public? How should they time the public release of the charges to maximize their impacts? Furthermore, prosecutors also have the option of using other policy tools like an INTERPOL Red Notice, civil enforcement, or working with policymakers to bring sanctions, diplomatic action or other tools to bear.

The other options in the policy toolbox often provide alternatives or complements for an indictment. One model for thinking about this toolbox is the DIME(LE) framework, which comprises the various elements of statecraft: diplomacy, information, military, economy, and law enforcement.[31] As applied to state-sponsored hacking, the other available tools in the DIME(LE) model include policies like focused diplomatic engagement – which in part led to the 2015 U.S.-China cyber espionage agreement – and economic tools such as sanctions. Justice Department officials have often raised the point that law enforcement action can be accompanied with other policy options for countering illicit activities.[32]

However, applying the DIME(LE) framework to criminal charges points to some issues. The Justice Department fiercely guards its prosecutorial independence, which could raise problems, for example, for the State Department's efforts to calm a relationship when criminal charges could ignite acrimony.[33] In practice, this has meant that the Justice Department independently decides whether or not to bring criminal charges. With that said, the timing of unsealing those charges may be subject to interagency discussions among a very small group of officials from the White House and the Departments of State, Treasury, and Commerce to provide awareness and enable relevant preparations, e.g. implications for diplomatic relationships. In other instances, criminal charges fit with the broader goals – for instance, to put pressure on a state to stop its hacking – and it is crucial that the timing of a criminal charge help and not hinder other efforts to use available policy tools. Considering the whole concept of using all levers of government power, some social science literature argues that using multiple tools of social influence will reinforce each other in some

[31] Maurer *supra* note 7, at 139.

[32] Adam Hickey, another Justice official, discussed how indictments and the other parts of the DIME(LE) model complemented each other in a speech in October 2018: "And even in the cases above [where we have yet to apprehend a defendant], the charges were never the end of the story: whether it is trade remedies, sanctions, contributions to network defense, or diplomatic efforts to rally likeminded nations to confront an adversary together, all of those charges served a greater purpose." Hickey, *supra* note 2.

[33] *See* Griffin Bell, U.S. Attn'y Gen., Address Before Department of Justice Lawyers, U.S. Dep't of Justice (September 6, 1978), https://perma.cc/2LRA-69AE ("[T]he Department [of Justice] must be recognized by all citizens as a neutral zone, in which neither favor nor pressure nor politics is permitted to influence the administration of the law."); *see also Communications with the White House Regarding Open Investigations, Adjudications, or Civil and Criminal Enforcement Actions,* U.S. DEP'T OF HOMELAND SECURITY (Mar. 1, 2003).

instances. In other instances, multiple tools of influence may change conditions or socialize their targets in such a way as to have a completely counterproductive effect.[34]

Additionally, criminal charges are not 'one-size-fits-all.' Criminal charges will have vastly different effects based on the target audience. For example, the Chinese government will react in a way that differs from how Iranian proxy groups for the IRGC will respond. In addition, different kinds of malicious behavior, such as election interference, intellectual property theft, extortion, or intrusions on critical infrastructure, may require different responses, and criminal charges may be an appropriate policy tool for only some. Of course, the U.S. criminal code limits in some respects the charges that the Justice Department can bring because the Justice Department can only charge hackers with violations of laws currently in force. Further, in their deliberations, prosecutors must consider other factors, such as the number of individuals the Justice Department could charge, their status as either government officials, military officers, or non-state proxies, and finally, whether they are located in countries where authorities could arrest and extradite them. Whether the Justice Department can readily arrest the person is crucial. It determines if the unsealed indictment will be primarily a speaking indictment, relying more on the disclosure of information and the normative power of U.S. criminal charges, rather than an indictment that limits the travel and potentially seizes the assets of the defendant. In contrast, arresting a hacker imposes a much greater cost on the target state and has a much larger impact. The challenge is that the hackers often operate behind national borders that protect them from arrest.

In using criminal charges to accomplish the purposes outlined above, in concert with other available policy tools, policymakers face further considerations on the potential risks and negative consequences of using criminal charges to respond to state-sponsored hacking.

A. Risk of disclosing sources and methods

While criminal charges often present detailed evidence gathered on hackers, going as far to present their photos, internet searches, and chat messages to superiors, disclosing such information can provide information about U.S. intelligence collection capabilities to adversaries. Prosecutors must strike a balance on what to disclose and how quickly they do so without compromising ongoing intelligence sources and methods. Conversely, it is sometimes advantageous to reveal U.S. government attribution capabilities because it removes doubt about attributions by showing exactly how the U.S. government obtained that information.

B. Risk of adversary response in kind or escalation

Bringing charges against individual officers in foreign adversaries' militaries and intelligence agencies raises the potential for those countries to charge members of the U.S. government with

[34] For instance, the famous Israeli Day Care experiment showed that imposing a cost to discourage behavior instead socialized individuals that it was a "price" rather than a "penalty" and increased the behavior. Uri Gneezy & Aldo Rustichini, *A Fine Is a Price*, 29 J. LEGAL STUD. 1, 1-17 (2000).

similar offenses.[35] Operators for U.S. Cyber Command could face criminal prosecutions in places like China, although it is less likely that they would have to fear extradition from third-party countries. Given that U.S. adversaries routinely violate human rights and their civil liberties protections range from few to none, U.S. hackers have voiced worries that facing criminal sentences in Beijing would be worse than facing charges in Pittsburgh.[36] However, although U.S. adversaries have not brought criminal charges against U.S. officials, Russia has sanctioned Justice Department officials for their role in the extradition of a hacker, Roman Seleznev, in 2013 from the Maldives.[37] Similar retaliation could be expected in the future and could apply even in cases, like Seleznev's, where there was no explicit allegation of state sponsorship.

C. Potential for declining impacts on adversary behavior

As the number of criminal charges increases, particularly against revisionist states like Russia that brush off international opprobrium, criminal charges may prove less viable for certain purposes, especially those related to exerting pressure on adversary governments. If criminal charges do not lead to definite changes in behavior or clear costs on individual hackers, their perceived signaling strength to external audiences could erode.[38]

D. Time required to assemble criminal charges.

Malicious activity, particularly that which has an immediate public impact like the 2011-2013 DDoS attacks or the 2016 hack of the DNC, creates pressure on the U.S. government to respond quickly. Criminal charges are often a poor solution to this problem because it takes time to investigate, compile rigorous evidence, and then convince a grand jury to approve the criminal charge. One indictment unsealed in 2018 referenced malicious activity from 2011 through 2015. It took Justice Department prosecutors until summer 2018 to unseal charges against GRU officers for hacking the DNC in 2016.

E. Failure to indict could imply tacit toleration of malicious activity

[35] Dave Aitel, *The Folly of 'Naming and Shaming' Iran*, LAWFARE BLOG (Apr. 19, 2016, 2:00 PM), https://perma.cc/T4XL-9HYZ.

[36] Lorenzo Franceschi-Bicchierai, *Ex-NSA Hackers Worry China and Russia Will Try to Arrest Them*, MOTHERBOARD (Dec. 1, 2017, 10:00 AM), https://perma.cc/9RDK-CAWT.

[37] *Russia Blacklists US Justice Officials Related to Seleznev's Detention*, SPUTNIK, (Jan. 29, 2015, 8:01 PM), https://perma.cc/SZ9T-PLB3.

[38] One way this might happen is that if the U.S. is unable to muster an effective response to a cyber attack, an indictment could be seen by domestic audiences and U.S. allies as an ineffective attempt to "do something." A public acknowledgement of the breach without an effective response may invite further attacks from other states. For a more detailed discussion of why this could be harmful, see Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities How a Digital World Disadvantages the United States in Its International Relations*, *in* AEGIS SERIES PAPER NO. 1806 13-14 (Hoover Institution, 2018).

Justice Department officials have commented that if they did not indict state-sponsored hackers, they would be sending a message to hackers that they could act with impunity.[39] As criminal charges have become a routine feature of U.S. responses to state-sponsored cyber activity, the risk becomes that in cases where the U.S. does not unseal an indictment, it signals that it tacitly accepts that activity as permissible.[40] In addition, as discussed above, there are often barriers to criminal charges like inaccessible information, the burden of convincing a grand jury, and timeliness considerations. In some cases, it simply is not possible to bring an indictment because of a lack of admissible evidence pointing to specific individuals.

F. Attributing malicious activity could magnify the impact of disinformation operations

While analysts generally perceive attribution as a positive step, there are some situations where it could be disadvantageous. For instance, Jack Goldsmith has argued that attributing the 2016 election disinformation operations to the Russian government may actually have enhanced the perceived impact of those operations.[41] In cases of incidents with significant political valence, policymakers should take into context how detailed criminal charges could affect the political climate, especially for information operations.

IV. CASE STUDIES

This section analyzes the currently available criminal charges with country-by-country micro case studies. The country of origin is often the most significant factor in determining hackers' tools, techniques, relationship to the state, and geopolitical motivations. As shown in Table 1, which provides an overview of criminal charges unsealed to date, the U.S. has unsealed charges against hackers working for five different states - China, Russia, Iran, Syria, and North Korea. Therefore, this section gives a brief overview of the alleged offenses in each set of charges on a country-by-country basis to put them in context.

A. China

The first unsealed US indictment that specifically alleged state responsibility for malicious cyber activity – the May 2014 indictment of five PLA officers for conducting a wide-ranging campaign of economic espionage against U.S. companies – came against China-linked hackers. Six more have followed, making China one of the states most often targeted by the Justice

[39] *See* John Demers, Assistant Attorney General for National Security, U.S. Dep't of Justice, Remarks on the Unsealing of an Indictment Against Russian GRU Officers for Various Malicious Cyber Activities (Oct. 4, 2018).

[40] A similar phenomenon occurs in international law, where failure to object to an action may contribute to a later conclusion that the action is lawful. *See* INT'L LAW COMM'N, DRAFT CONCLUSIONS ON IDENTIFICATION OF CUSTOMARY INTERNATIONAL LAW, U.N. Doc. A/CN.4/L.908 (2018) (Conclusion 10(3): "Failure to react over time to a practice may serve as evidence of acceptance as law (opinio juris), provided that States were in a position to react and the circumstances called for some reaction.").

[41] Jack Goldsmith, *The Downsides of Mueller's Russia Indictment*, LAWFARE BLOG (Feb. 19, 2018, 10:26 AM), https://perma.cc/H6B6-WDGN.

Department's criminal charges. All have involved allegations of economic espionage, including thefts of trade secrets. The May 2014 indictment supported a broader strategy by the US government that included further threats highlighting that Chinese cyber-enabled theft of trade secrets had become a top priority in the U.S.-China bilateral relationship.[42] In addition, in June 2014, Canadian authorities arrested a Chinese national, Su Bin, on a U.S.

[42] Ellen Nakashima, *U.S. developing sanctions against China over cyberthefts*, WASH. POST (Aug. 30, 2015), https://perma.cc/R4FL-5X6F.

Table 1.

Criminal Charges by Target State, Alleged Perpetrators and Type of Malicious Activity

Alleged perpetrators	Dates of Activity	Date Filed	Date Unsealed	Target State	Indictees	Malicious Activity Alleged	Victims
Nima Golestaneh	Oct 2012	Nov 2013	Dec 2015	Iran	1	IP Theft	Arrow Tech
PLA Unit 61398	2006 - 2014	May 2014	May 2014	China	5	IP Theft	Westinghouse, U.S. Steel, Alcoa
Evgeniy Bogachev	2011 - 2014	May 2014	Jun 2014	Russia	1	Extortion, Theft	Diffuse businesses, users
Agha and Dardar	Dec 2014	Jun 2014	Mar 2016	Syria	2	Website Defacement	News Orgs, White House
Su Bin	Oct 2008 - Dec 2014	Jun 2014		China	1	IP Theft	Boeing
Romar and Dardar	Dec 2014	Dec 2015	Dec 2015	Iran	2	Extortion, Money laundering	News Orgs, others
Mersad Co., IT Sec	2011 - 2013	Jan 2016	Mar 2016	Iran	7	DDoS, Hacking Dam	U.S. banks, Bowman Dam
Ajily and Rezakhah	2007 - Oct 2012	Apr 2016	Jul 2017	Iran	2	IP Theft	Arrow Tech
FSB	Dec 2014 - Dec 2016	Feb 2017	Mar 2017	Russia	4	Espionage	Yahoo
Yu Pingan	Apr 2011 - Jan 2014	Aug 2017	Aug 2017	China	1	Espionage	3 unnamed U.S. companies
Boyusec	2011 - May 2017	Sep 2017	Nov 2017	China	3	IP Theft	Moody's, Siemens, Trimble
Behzad Mesri	May - Aug 2017	Nov 2017	Nov 2017	Iran	1	Extortion	HBO
Internet Research Agency	Jul 2016 - Sep 2017	Feb 2018		Russia	13	Election Interference	U.S. electoral system
Mabna Institute	2013 - Dec 2017	Feb 2018	Mar 2018	Iran	9	IP Theft	U.S. universities, govt.
Agha and Dardar	Dec 2014	May 2018		Syria	2	Website Defacement	News Orgs, White House
Park Jin Hyok	Sep 2014 - Aug 2017	Jun 2018	Sep 2018	North Korea	1	Destruction, Extortion	Sony, UK NHS
GRU	Mar - Nov 2016	Jul 2018		Russia	12	Election Interference	DNC, DCCC
Elena Khusyaynova	2014 - Oct 2018	Sep 2018	Oct 2018	Russia	1	Election Interference	U.S. electoral system
GRU	Dec 2014 - May 2018	Oct 2018	Oct 2018	Russia	7	Hacking for Disinformation	OPCW, WADA, etc
China JSSD	Jan 2010 - May 2015	Oct 2018	Oct 2018	China	10	IP Theft	U.S.-French aerospace firm
Savandi and Mansouri	Dec 2015 - Sep 2018	Nov 2018	Nov 2018	Iran	2	Extortion	Port San Diego, Atlanta, others
China MSS	2006 - 2018	Dec 2018	Dec 2018	China	2	IP Theft, Espionage	Managed Service Providers
Iranians, Monica Witt	2013 - May 2015	Feb 2019	Feb 2019	Iran	5	Espionage	U.S. intelligence agencies
Fujie Wang and John Doe	Oct - Nov 2014	May 2019	May 2019	China	2	Data theft	Anthem Inc.

* Second set of charges filed for the same offenses.

extradition request. Bin worked at a small aerospace firm and had provided inside information to military hackers in China that allowed them to exfiltrate specific files of valuable data about the development of the C-17 military cargo plane and the F-35 joint strike fighter.[43] Although this arrest did not receive the publicity of the PLA indictment, later reporting indicated that Chinese officials took this as an even more significant move.[44] Subsequently, President Obama and President Xi reached the landmark 2015 U.S.-China cyber economic espionage agreement and cybersecurity companies reported a significant drop in Chinese cyber thefts from U.S. companies.[45]

Since 2015, the charges have followed a track that has aimed at steadily increasing pressure. The next indictment came after a gap of more than three years, in August 2017, when prosecutors in Los Angeles arrested a Chinese national, Yu Pingan, for hacking three different companies by using a malware variant linked to the OPM hack. The charges against Pingan did not mention the OPM hack, just the malware variant, noting that it was a rare type.[46] That November, federal prosecutors in Pittsburgh unsealed an indictment of three employees at the Chinese company Boyusec. The indictment charged the Boyusec employees with stealing trade secrets from Siemens, Moody's Analytics, and Trimble but importantly, did not make an explicit allegation of state sponsorship (although press reporting and security researchers identified links between Boyusec and China's Ministry of State Security (MSS)).[47] This created deniability for the Chinese government, and indeed, a month after the Justice Department unsealed the charges, Boyusec disbanded. In late 2017 and early 2018, U.S.-based researchers started to report that Chinese hacking for trade secrets had increased in volume. Some researchers argued that the cause of the resurgence was a shift in emphasis from the PLA to the MSS.[48]

In early 2018, a major report by the U.S. Trade Representative accused China of ramping up economic espionage, using this as a justification for the imposition of the first round of tariffs in the U.S.-China trade war.[49] As reciprocal rounds of tariffs mounted in value to the hundreds of billions of dollars, in the fall the U.S. unsealed a series of criminal charges focusing on MSS-

[43] Garrett Graff, *How the US Forced China to Quit Stealing – Using a Chinese Spy*, WIRED (Oct. 11, 2018, 6:00 AM), https://perma.cc/R9AP-DTB6.

[44] JOHN CARLIN & GARRETT GRAFF, DAWN OF THE CODE WAR 297 (2018) ("The Su Bin case, all but unnoticed by the public, had a large impact on Chinese thinking … In the space of barely a month, the United States had taken overt steps against two major Chinese economic espionage operations.").

[45] *U.S.-China Cyber Agreement*, CRS INSIGHT (Oct. 16, 2015), https://perma.cc/ZRL9-TZLC; FIREEYE, *Redline Drawn: China Recalculates its Use of Cyber Espionage* (June 2016), https://perma.cc/8SXN-CM3D.

[46] Devlin Barrett, *Chinese national arrested for allegedly using malware linked to OPM hack*, WASH. POST (Aug. 24, 2017), https://perma.cc/7HPQ-75H5.

[47] Elias Groll, *Feds Quietly Reveal Chinese State-Backed Hacking Operation*, FOREIGN POLICY (Nov. 30, 2017, 10:57 AM), https://perma.cc/97LR-ZQFX; Insikt Group, *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT 3*, RECORDED FUTURE (May 17, 2017), https://perma.cc/J3TU-NN8U.

[48] Lorand Laskai & Adam Segal, *A New Old Threat: Countering the Return of Chinese Industrial Espionage*, COUNCIL ON FOREIGN RELATIONS (Dec. 6, 2018), https://perma.cc/2FBQ-N4YD.

[49] Office of the U.S. Trade Representative, Section 301 Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation (Mar. 27, 2018), https://perma.cc/2DHS-RL4V; David Lawder, *USTR says China failed to alter 'unfair, unreasonable' trade practices*, REUTERS (Nov. 20, 2018, 6:19 PM), https://perma.cc/DM25-Y87D.

linked hackers. However, the first set of charges in this series actually did not involve hacking. Belgian authorities extradited a senior MSS officer, Yanjun Xu, to the U.S. on charges related to stealing trade secrets from multiple U.S. aviation and aerospace firms.[50] Two weeks later, The Justice Department unsealed an indictment against two officers in the Jiangsu Province Ministry of State Security (a regional branch of the MSS) and five hackers they recruited to break into a U.S.-French joint aerospace venture to steal engine-related technology designs.[51] The Justice Department timed these charges with another indictment two days later against a Chinese company for conspiring to steal semiconductor technology, although this case did not involve cyber-enabled theft.[52] At this announcement, Attorney General Jeff Sessions announced a "China Initiative" to combat Chinese-sponsored trade secrets thefts.[53]

At this point, the U.S. had not formally accused China of violating the 2015 agreement. This was because the actual agreement was narrow – the two nations said they would not employ cyber-enabled espionage to benefit private sector firms. Criminal charges brought to this date either charged non-cyber espionage or named activity that stopped before September 2015. This changed with the Justice Department's December indictment of two MSS officers in connection with a wide-ranging scheme over 12 years to hack managed services providers, which served as IT infrastructure for hundreds of companies.[54] This campaign, dubbed "Cloudhopper" by the cybersecurity teams at PwC and BAE Systems, was one the most significant and damaging sprees of economic espionage. With the indictment, the U.S. had concrete evidence, which Secretary of State Mike Pompeo and Secretary of Homeland Security Kirstjen Nielsen used as the basis of a joint statement alleging that China violated the accord.[55] Moreover, twelve close U.S. allies joined in issuing statements condemning China's behavior.[56] The G-20 had committed to the economic espionage norm, and this collective denouncement took the indictment as evidence to criticize China for breaching its commitments.

The China charges follow a very clear trajectory and focus on one principal activity: economic espionage. The Justice Department has not brought charges explicitly related to other types of

[50] Ellen Nakashima, *In a first, a Chinese spy is extradited to the U.S. after stealing secrets, Justice Dept. says*, WASH. POST (Oct. 10, 2018, 2:31 PM), https://www.washingtonpost.com/world/national-security/chinese-spy-charged-with-stealing-us-military-secrets-and-extradited-for-prosecution/2018/10/10/b2a7325c-cc97-11e8-920f-dd52e1ae4570_story.html.

[51] Colin Lecher, *Chinese spies hacked aerospace companies for years, Justice Department says*, THE VERGE (Oct. 30, 2018, 5:32 PM), https://perma.cc/9SBV-P9AF.

[52] Press Release, U.S. Dep't of Justice, *PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage* (Nov. 1, 2018), https://perma.cc/VDD7-7TV7.

[53] Preston Lim & Rachel Brown, *SinoTech: Department of Justice Launches Initiative to Address Chinese Economic Espionage*, LAWFARE BLOG (Nov. 14, 2018, 12:47 PM), https://perma.cc/VXZ9-KTGS.

[54] Brian Barrett, *How China's Elite Hackers Stole the World's Most Valuable Secrets*, WIRED (Dec. 20, 2018, 3:32 PM), https://perma.cc/JH3F-5S7K.

[55] Joint Statement by Secretary of State Michael R. Pompeo & Secretary of Homeland Security Kirstjen Nielsen, *Chinese Actors Compromise Global Managed Service Providers* (Dec. 20, 2018), https://perma.cc/PQ9S-NGSJ.

[56] The states that joined were: the UK, Canada, Australia, New Zealand, Denmark, Sweden, and Finland, Japan, Norway, the Netherlands, Germany, and Poland. Ellen Nakashima & David J. Lynch, *U.S. charges Chinese hackers in alleged theft of vast trove of confidential data in 12 countries,* WASH. POST (Dec. 21, 2018, 10:44 AM), https://perma.cc/U8AA-AX9Q.

malicious activity, even though there is evidence that China has sponsored it, such as the OPM breach. As the United States has aimed to curb China's activities along these lines, charges in 2014 helped provide the impetus for the 2015 U.S.-China agreement not to use cyber means for economic espionage. These criminal charges also had a more global effect: contributing to the anti-economic espionage norm at the G-20. However, the threat of future criminal charges clearly proved insufficient to enforce the norm against China. The series of criminal charges in late 2018 is perhaps the most strongly interlinked, mutually supportive set of criminal charges against any target state, but it is too soon to fully evaluate the long-term consequences. One early assessment is that the U.S. looks to use its criminal charges to mobilize allies and like-minded states internationally against norms violators more than to punish, deter, or engage the direct target states.

B. Russia

As of January 2019, the Justice Department has brought five separate cases of criminal charges against Russians for cyber-related crimes. The first charges came only a month after the PLA indictment, and at the time, did not clearly seem to implicate state sponsorship. This was because the indictment was against Evgeny Bogachev, the administrator of the GameOverZeus botnet, and the Justice Department unsealed the charges concurrently with a major international operation to take down the botnet. Only later reporting and sanctions on Bogachev announced in 2016 revealed that Bogachev was using the botnet to siphon information about Russian intelligence targets as well as to steal bank information.[57] The FBI had discovered this before taking down the botnet, and so the planned takedown, which originally just aimed to stop a major criminal operation, also served to disrupt a Russian intelligence gathering effort.[58]

Prosecutors have named and charged officers in Russia's security services, the GRU and FSB, in three out of the five sets of charges, starting with the March 2017 indictment of two FSB officers and two cyber criminals for their roles in the hack of Yahoo!.[59] This indictment was also significant because it revealed that Russia had employed cyber criminals to assist in carrying out the actual hacking of Yahoo!. It further led to the arrest of one of these criminals, Karim Baratov, in Canada and his subsequent extradition, which was an example of the effectiveness of criminal charges at locking up proxies.[60] In 2018, Special Counsel Robert Mueller's investigation of Russia's interference in the 2016 election led to three separate criminal indictments – one in July against seven GRU officers for their role in hacking the DNC and Clinton campaign's emails and releasing them.[61] This indictment paralleled other cyber indictments by focusing on unauthorized access to a computer, i.e. hacking. But the other two sets of charges, the first in February against the Internet

[57] Michael Schwirtz & Joseph Goldstein, *Russian Espionage Piggybacks on a Cyber Criminal's Hacking*, N.Y. TIMES (Mar. 12, 2017), https://perma.cc/NJL6-2A63.

[58] Carlin & Graff, *supra* note 44, at 296-97.

[59] Goel & Lichtblau *supra* note 17.

[60] Press Release, U.S. Dep't of Justice, *International Hacker-For-Hire Who Conspired With and Aided Russian FSB Officers Sentenced to 60 Months in Prison* (May 29, 2018), https://perma.cc/XTB3-6UJG.

[61] Mark Mazetti & Katie Benner, *12 Russian Agents Indicted in Mueller Investigation*, N.Y. TIMES (July 13, 2018), https://perma.cc/W7NE-CPPF.

Research Agency (IRA) and thirteen of its employees, and the second in October against Elena Khusyaynova, the chief accountant for the broader influence program of which the IRA was a part, focused on social media disinformation activities. To bring the charges, prosecutors relied on an innovative approach alleging a conspiracy to violate campaign finance laws.[62] The IRA cases have also provoked one of the only contested litigation resulting from cyber indictments: a court battle between the company Concord Management and Consulting (which owned the IRA) and the Mueller investigation.[63]

These three sets of charges resulted from the special counsel's office and demonstrated the Justice Department's prosecutorial independence, even contradicting President Trump's repeated dismissals of Russia's election interference efforts. In addition, these cases also had significant importance for Congress and the public because of the Russia investigation's political salience.

The fifth indictment came in October 2018, when the Justice Department unsealed charges against four more GRU officers (and three of the same from Mueller's charges) for hacking into the WADA, the OPCW, the international soccer association FIFA, and many other targets.[64] With this indictment, the U.S. joined with its allies in condemning Russia's activities. The UK and the Netherlands issued a strong joint statement, focusing particularly on how the hacking was aimed at discrediting the investigation into the poisoning of Sergei Skripal in Salisbury in early 2018.[65] One practical effect of these charges was, as iterated, that these operatives could not travel in the future to U.S.-allied countries – which several Russian GRU officers in fact did, going to the Netherlands to attempt to surveil the OPCW. Interestingly, the Netherlands apprehended the officers but did not extradite them to the U.S., likely because at that time (April 2018), the Justice Department did not have sealed charges against them ready. Instead, they expelled them since the officers were carrying diplomatic passports, and Dutch authorities explained that their counter effort was a military, not police operation.[66]

The October 2018 indictment also pointed to an interesting behavior: the Russian government took the OPCW's efforts to investigate the Skripal attack and WADA's investigations of its doping program seriously enough to try to hack those organizations and try to discredit them. Naming and shaming pressured Russia to do something, except that something was more aggressive hacking to discredit shaming efforts, supporting the already-sizeable body of evidence that Russia was responsible for the Skripal attack.

The policy value of the Russia charges may be in their effects against individuals and in disrupting Russia's relationships with its proxies – for instance, in how the Yahoo! hack led to

---

[62] Emma Kohse & Benjamin Wittes, *About That Russia Indictment: Robert Mueller's Legal Theory and Where It Takes Him Next*, LAWFARE BLOG (Mar. 7, 2018, 7:00 AM), https://perma.cc/9BDM-2X34.

[63] Spencer Hsu & Josh Dawsey, *U.S. judge refuses to toss out Mueller probe case against Russian firm owned by 'Putin's chef'*, WASH. POST (Nov. 15, 2018, 4:52 PM), https://perma.cc/G5DH-BHB7.

[64] Bill Chappell & Carrie Johnson, *U.S. Charges 7 Russian Intelligence Officers With Hacking 40 Sports and Doping Groups*, NPR (Oct. 4, 2018, 7:59 AM), https://perma.cc/L5VG-QFCK.

[65] *How the Dutch foiled Russian 'cyber-attack' on OPCW*, BBC (Oct. 4, 2018), https://perma.cc/92UE-E3MU; *Joint Statement from Prime Minister May and Prime Minister Rutte*, UK GOVERNMENT, (Oct. 4, 2018).

[66] Anthony Deutsch & Stephanie van der Berg, *Dutch government says it disrupted Russian attempt to hack chemical weapons watchdog*, REUTERS (Oct. 4, 2018, 6:31 AM), https://perma.cc/HSN8-L6E8.

Baratov's arrest and how the Bogachev indictment contributed to the GameOver Zeus takedown. In the last eighteen months, the Department of Justice has stepped up its efforts to indict and obtain extraditions of Russian hackers, some of whom may know about Russian government cyber activities.[67] As a rogue state, Russia is unlikely to take naming and shaming efforts seriously. Rather, the value of the indictments lies in their ability to demonstrate the U.S.' desire to uphold international norms to the audience of other states and potentially to enlist international collaboration, as in the OPCW indictment. Further, in the long-term, the three cases related to Russia's operations during the 2016 election may contribute to building a stronger norm against cyber-enabled election interference.

C. Iran

Although discussions of Iran's cyber threat have focused on the DDoS attacks detailed in a March 2016 indictment[68], the first criminal charges against an Iran-linked hacker came in 2013, against a single individual who was arrested in Turkey and then extradited to the U.S. in December 2015 to face charges related to hacking an engineering company in Vermont to steal valuable IP. This man, Nima Golestaneh, pled guilty, but court documents did not reveal much until 2017, when the Justice Department unsealed a follow-on indictment against two other Iranians where it alleged that they engaged in a scheme to steal IP related to missile guidance systems and then to provide that to the Iranian military, in violation of U.S. export controls.[69] However, at this time, Golestaneh was out of U.S. custody. President Obama gave him a conditional pardon as part of negotiations for the U.S.-Iran nuclear deal.[70]

In March 2016, the Justice Department unsealed charges against Iranians working for two companies affiliated with the Islamic Revolutionary Guard Corps (IRGC), accusing the Iranians of carrying out a massive DDoS campaign targeting financial institutions dating back to 2011. Analysts at the time said the attacks were in response to U.S. sanctions on Iran's nuclear program and to the Stuxnet virus's attack on Iran's uranium enrichment facilities.[71] At the time of the attacks, U.S. officials attributed them to Iran and the press reported on this attribution, but the U.S. did not make a public allegation. In late 2017, prosecutors in New York unsealed charges against Behzad Mesri, an Iranian who had previously worked for the Iranian military, for hacking into

[67] Christian Berthelsen, Michael Riley & Jordan Robertson, *Mystery JPMorgan Hacker Is in U.S. Hands. What Does He Know?*, BLOOMBERG (Sept. 7, 2018, 2:38 PM), https://perma.cc/WNZ7-ZW6U; Eleni Chrepa, Olga Kharif & Kartikay Mehrota, *Bitcoin Suspect Could Shed Light on Russian Mueller Targets*, BLOOMBERG (Sept. 4, 2018, 1:00 AM), https://perma.cc/EB24-YGSS.

[68] *State Department Report 5: Iran's Threat to Cybersecurity*, U.S. INST. OF PEACE (Sept. 28, 2018), https://perma.cc/MG4M-3296.

[69] Justin Carissimo, *U.S. charges Iranian nationals for hacking and reselling weapon software,* BLOOMBERG (July 17, 2017, 8:10 PM), https://perma.cc/XGK6-3KK7.

[70] Sari Horwitz, Ellen Nakashima & Julie Tate, *What we know about the seven Iranians offered clemency*, WASH. POST (Jan. 17, 2016), https://perma.cc/G43F-PZFF; Gregory Korte, *Obama's Iran pardons have unusual conditions,* USA TODAY (Jan. 19, 2016, 5:20 PM), https://perma.cc/2GGX-HXHJ.

[71] Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES (Jan. 8, 2013), https://perma.cc/M3XQ-JST4.

HBO and threatening to release episodes of "Game of Thrones" unless he was paid $6 million.[72] In March 2018, the Justice Department unsealed another indictment against a group of Iranian hackers called the Mabna Institute linked to the IRGC, in this instance for a spear phishing campaign stealing IP and data from universities, federal and state agencies and global NGOs.[73] According to the indictment, this activity campaign lasted from 2013 through December 2017, and targeted over 176 universities around the world, including 144 based in the U.S.

One major difference between charges against Iran-linked hackers and those against Russian and Chinese-linked hackers is that none of the charges are against officers or officials in the Iranian government. This may be because Iran relies on proxies to a greater degree than China or Russia, and those proxies have a greater degree of freedom from tighter state direction and control.[74] Time will tell whether restrictions on those indicted proxies' abilities to travel and have a career outside of Iran will alter Iran's ability to recruit more young and talented hackers. There is also less of a clear trend in the type of malicious activity – which ranges from DDoS attacks to IP theft to the hack-and-release strategy of the HBO hacker – and consequently, it is harder to make conclusions about the indictments' relevance to the larger U.S-Iran relationship. There are some clear points of correspondence – for instance, the pardon for Golestaneh as part of the détente following the nuclear deal, and the Mabna indictment as tensions increased following the Trump administration's withdrawal from the deal. But there are also outliers, such as the March 2016 DDoS indictment, which as the previous sections discussed, partially responded to pressure from major banks to respond to the attacks on their services. In late 2018 and early 2019, some analysts predicted and then observed more significant Iranian hacking as a response to the withdrawal from the nuclear deal, so more anti-Iran criminal charges may be in the works.[75]

D. Cyber Criminals from Iran and Syria

Two related sets of charges straddle the line between state-orchestrated hacking and cybercrime. First, two criminal complaints unsealed in March 2016 laid out charges against three members of the Syrian Electronic Army, a group of "patriotic" hackers whose operations aimed to build political support for the Assad regime, for attempting to spear phish U.S. government

[72] Jim Finkle, *U.S. prosecutors charge Iranian in 'Game of Thrones' hack*, REUTERS (Nov. 21, 2017, 11:07 AM), https://perma.cc/5QZF-FBJC.

[73] Sean Gallagher, *Nine Iranians indicted by US for hacking to steal research data*, ARS TECHNICA (Mar. 23, 2018, 6:20 PM), https://perma.cc/KTH9-DKAP.

[74] For a discussion of Tehran's coordination with hackers, see Maurer, *supra* note 7, at 81-84; *see also*, Collin Anderson & Karim Sadjadpour, *Iran's Cyber Ecosystem: Who Are the Threat Actors?*, CARNEGIE ENDOWMENT FOR INT'L PEACE, (Jan. 4, 2018), https://perma.cc/ZKQ8-PFRF.

[75] In the summer of 2018, U.S. officials predicted that Iran would respond to the U.S. withdrawal with cyberattacks. Courtney Kube et al., *Iran has laid the groundwork for extensive cyberattacks on U.S., say officials*, NBC NEWS (July 20, 2018, 2:15 PM), https://perma.cc/KM4C-GMDC. In early 2019, analysts reported a new scheme linked to Iran. *See* Lily Hay Newman, *A Worldwide Hacking Spree Uses DNS Trickery to Nab Data*, WIRED (Jan. 11, 2019, 11:34 AM), https://perma.cc/38Y8-JXUW; Ellen Nakashima, *DHS issues emergency order to civilian agencies to squelch cyber-hijacking campaign that private analysts say could be linked to Iran*, WASH. POST (Jan. 22, 2019, 11:12 PM), https://perma.cc/T8XR-KWE7.

computer systems and for running an extortion scheme by hacking U.S. companies from 2011 to 2014. Although the Justice Department did not accuse the Syrian government of direct activity in support of the Syrian Electronic Army, it said they carried out the attacks on behalf of the Assad regime. The charges led to the arrest of one individual, Peter Romar, in Germany, who was extradited to the U.S. to face charges related to the extortion scheme.[76] In May 2018, the Justice Department unsealed a new set of charges against the two remaining Syrians that detailed their efforts to hack U.S. social media organizations and deface their websites.[77]

Second, in November 2018, the Justice Department unsealed an indictment accusing two Iranian men of conducting a ransomware extortion campaign against city governments in Atlanta and Newark, the port of San Diego, U.S. hospitals, and other U.S. nonprofits.[78] The hackers gained access to their victims' networks and deployed malware that encrypted the victims' files and demanded payment in Bitcoin to provide the decryption keys. Similarly to the Syrian Electronic Army case, there was no direct allegation of state sponsorship. This indictment also served as the basis for Treasury Department sanctions against two other Iranians; in a first-time action, Treasury published the address of their Bitcoin wallets, warning U.S. individuals and organizations from transacting with these addresses.[79]

Since both cases involved what may be proxy groups or hacking that the regimes may not have fully known about, one possible purpose for the charges would be to pressure the respective governments to crack down on these groups. It is unlikely this would happen, especially for Syria, considering the ongoing civil war and the Syrian Electronic Army's long-standing focus on targeting opposition activities and anti-regime dissidents, which would disincentivize the regime from curbing their hacking.[80] The main impact of these charges may be in terms of attribution. They showed that the Syrian Electronic Army did not come from Iran or other actors, as some national security officials asserted during the incidents.[81] For the Iranian ransomware indictment, it clearly attributed the string of ransomware attacks to a single actor. Whether the indictment and its accompanying sanctions will disrupt their operations is not yet clear.

---

[76] Ellen Nakashima, *Syrian hacker extradited to the United States from Germany*, WASH. POST (May 9, 2016), https://perma.cc/KAM2-LUVZ.

[77] Press Release, U.S. Dep't of Justice, *Two Members of Syrian Electronic Army Indicted for Conspiracy* (May 17, 2018), https://perma.cc/Q9H8-UMYP.

[78] Press Release, U.S. Dep't of Justice, *Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses*, (Nov. 28, 2018), https://perma.cc/D9ZC-8PHA.

[79] Josephine Wolff, *What's Ransomware Without Cryptocurrency?*, SLATE (Dec. 3, 2018, 12:32 PM), https://perma.cc/87T3-ZCKG.

[80] Research by the Citizen Lab has tracked the SEA's activities going back to 2011. See researchers' comments in Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/3PB7-M2F8; Amitpal Singh, *Citizen Lab Research on Syrian Electronic Army in Politico*, CITIZENLAB (June 16, 2015), https://perma.cc/48BT-RDSK. Research in 2018 indicates that the SEA has continued its anti-activist hacking. Thomas Brewster, *Syrian Electronic Army Hackers Are Targeting Android Phones With Fake WhatsApp Attacks*, FORBES (Dec. 5, 2018), https://perma.cc/P53V-WCBV.

[81] Carlo Munoz, *Hayden: Pro-Syria hacker group working with Iran*, THE HILL (Nov. 21, 2013, 4:27 PM), https://perma.cc/7CCL-TTHK.

E. North Korea

The September 2018 charges against a North Korean hacker reveal an immense amount of information about North Korean tradecraft and planning of the Sony hack, WannaCry, and other cyber incidents.[82] However, they do not reveal much about the sole indictee, Park Jin Hyok. The charges do show that Park worked for the Chosun Expo, a front company in China for North Korean hacking.

The significance of the charges is in their timing more than anything else. The U.S. already publicly attributed the Sony hack and WannaCry to North Korea long ago.[83] The Justice Department brought the charges as nuclear negotiations between the U.S. and North Korea appeared to stagnate.[84] In response to the charges, a North Korean spokesperson said, "[t]he U.S. should seriously ponder over the negative consequences of circulating falsehoods and inciting antagonism against the DPRK that may affect the implementation of the joint statement adopted at the DPRK-U.S. summit."[85] They also denied Park's very existence, saying he was a "non-entity."[86]

The clearest impact of the one set of charges is that it confirmed the original 2014 attribution of the Sony hack to North Korea and added a voluminous amount of technical data reinforcing the U.S. government's attribution of the WannaCry worm. Although the charges did provoke an interesting discussion among the U.S. cybersecurity technical community about their initial approach and the skepticism of some to the FBI's 2014 attribution of the Sony hack, this discussion had little policy relevance because almost four years had passed.[87] In terms of diplomacy, the timing is curious given the ongoing nuclear negotiations. Other than providing justice for victims, any foreign policy purpose is unclear. One early indication in that regard is the FBI's warning to U.S. companies in October that North Korea "will continue to target financial institutions" in spite of the indictment, which supports the argument that the charges had more domestic than foreign policy purposes.[88] Lastly, some commentators raised the potential human rights implications of the charges, arguing that the response of North Korea's regime would be to imprison, disappear, or kill the named hacker to make him a "non-entity."[89]

---

[82] Press Release, U.S. Dep't of Justice, *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Sept. 4, 2018), https://perma.cc/9V2K-NNTW.

[83] WHITE HOUSE, *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*, Press Briefing (Dec. 19, 2017), https://perma.cc/Z7SQ-F7QV.

[84] David Tweed, *Why the U.S.-North Korea Talks Have Stalled*, BLOOMBERG (Aug. 29, 2018, 8:08 AM), https://perma.cc/2H3Q-PYUX.

[85] Simon Denyer, *N. Korea says 'smear campaign' over hacking undercuts Trump-Kim accord*, WASH. POST (Sep. 14, 2018, 1:41 PM), https://perma.cc/B9WN-DL4T.

[86] Eric Talmadge, *North Korea calls Sony and WannaCry hack charges smear campaign*, ASSOCIATED PRESS (Sept. 15, 2018), https://perma.cc/XVC9-73UZ.

[87] *See* Kevin Collier, *The Indictment Of North Korea For The Sony Hack Shows How Cybersecurity Has Evolved*, BUZZFEED NEWS (Sept. 7, 2018, 7:02 PM), https://perma.cc/8KEQ-WEEL.

[88] Sean Lyngaas, *FBI to private industry: Attribution won't deter North Korean hacking*, CYBERSCOOP (Oct. 26, 2018), https://perma.cc/U9G5-P58Z.

[89] Jake Williams, *Don't Punish a North Korean Hacker Just for Following Orders*, DAILY BEAST (Sept. 7, 2018, 9:41 PM), https://perma.cc/KCA5-UGMM.

V. DISCUSSION

This section will apply the conceptual framework selectively to identify important trends in the trajectory of the criminal charges.

First, in terms of attribution, the charges divide neatly into those that the Justice Department brought without the U.S. government having previously attributed the activity and those criminal charges where there was prior attribution. In those that attributed activity to a foreign state for the first time, the criminal charges had a more prominent impact on domestic and international audiences. Internationally, criminal charges like the PLA indictment, the OPCW/WADA indictment, and the Cloudhopper indictment, provoked consequences in the target state and helped to mobilize allies to condemn the target state's behavior. Domestically, the Yahoo! indictment and the Syrian Electronic Army indictment provided attribution of significant cyber incidents, helping to clarify the perpetrators to the public and to victims. For criminal charges that had prior attribution, there were less clear diplomatic impacts – for instance, the Sony and WannaCry indictment and DNC indictment both responded to very significant incidents, but they did not much alter the U.S. relationship with the target state. Their effects may have been more important domestically because of their political salience, but the criminal charges themselves did not reveal much new, relevant information to the public.

Another way to distinguish the criminal charges is by the types of activities – e.g. IP theft or DDoS attacks – that the criminal charges allege. Of the 24 foreign hacking criminal charges brought to date, eight charged defendants related to IP or trade secrets theft. This indicates that the Justice Department has prioritized prosecuting IP theft cases, in part because the U.S. has so strongly opposed state-backed economic espionage. The rest of the criminal charges range from DDoS attacks, to electoral interference via social media, to ransomware, and to extortion schemes. One similarity across cases is a "hack and release" strategy: The hack of the DNC is the most prominent example. Others include the OPCW/WADA hacks, the HBO hack, and the Syrian Electronic Army (which was slightly different in that it involved hacking social media channels and posting disinformation). Although the DNC hack arguably violated the implicit norm against cyber-enabled election interference that has since been reinforced through explicit statements[90] – it is more difficult to delineate exactly what norms each of these activities violates. As discussed above, criminal charges do not necessarily need to aim to punish norm-violating activity, but it is especially interesting that only two indictments (Finance DDOS, SamSam ransomware) came against attacks on critical infrastructure, which is another of the major norms that the U.S. promotes in cyberspace and which the U.S. is most concerned about its adversaries violating.

Examining the underlying activities raises a key question: are criminal charges better suited to respond to certain kinds of cyber activities? One way to answer this is to consider major cyber incidents for which the U.S. has not brought charges. For instance, the hack of the Office of

[90] *See Charlevoix Commitment on Defending Democracy From Foreign Threats*, G7 (2018), https://perma.cc/4T8Q-CE8T.

Personnel Management exposed the records of 21.5 million federal employees – but because the culprit was likely Chinese intelligence services and because they have not released any of the information, U.S. authorities have approached this like a traditional espionage operation and have not taken a law enforcement response. Similar logic may apply to the Shadowbrokers release of NSA toolkits where it is unclear if a nation-state was behind their actions. Of course in this case, the Shadowbrokers did release what they stole. Here, the reason for no charges is likely, in part, that NSA is highly reluctant to allow a public criminal case, which could expose its own intelligence methods and operations. It is puzzling why the U.S. has not brought charges against Russian actors for the NotPetya malware, which the U.S. and allies have already attributed as a clear violation of international norms. Here, the concern about intelligence sources and methods may apply.

One emerging trend is the U.S.' increasing use of criminal charges as a basis for other action – for instance, the imposition of targeted sanctions on the same individuals and their overseas assets or botnet takedowns. See Table 2 for a full list of arrests and other U.S. government actions that have accompanied criminal charges. In the fall of 2018, some of the criminal charges foreshadowed taking this to another degree: the imposition of Commerce export controls on the Chinese firm that benefitted from IP theft set the stage for economic sanctions on Chinese companies that gained an advantage from stolen trade secrets. However, reporting around the December 20 Cloudhopper indictment said that the Justice Department had pushed for sanctions on several firms but that the Treasury Department pushed back, saying sanctions would be too escalatory in the broader U.S.-China trade war.[91]

[91] Dustin Volz, Kate O'Keefe & Bob Davis, *U.S. Charges China Intelligence Officers Over Hacking Companies and Agencies*, WALL ST. J. (Dec. 20, 2018, 10:13 PM), https://perma.cc/9S2C-K92U.

Table 2.

Indictments and Accompanying Actions

Defendants (Case Name)	Date Filed	Date Unsealed	Sanctions Date	Target State	Arrest or Other Actions
Golestaneh	Nov 2013	Dec 2015		Iran	Arrest of Golestaneh
Wang Dong et al.	May 2014	May 2014		China	
Bogachev	May 2014	Jun 2014	Dec 2016	Russia	Botnet takedown
Agha and Dardar	Jun 2014	Mar 2016		Syria	
Su Bin	Jun 2014			China	Arrest of Su Bin
Romar and Dardar	Sep 2015	Mar 2016		Syria	Arrest of Romar
Fathi et al.	Jan 2016	Mar 2016	Sep 2017	Iran	Botnet takedown
Ajily and Rezakhah	Apr 2016	Jul 2017		Iran	
Dokuchaev et al.	Feb 2017	Mar 2017	Dec 2016	Russia	Arrest of Baratov
Pingan	Aug 2017	Aug 2017		China	Arrest of Yu Pingan
Wu Yingzhou et al.	Sep 2017	Nov 2017		China	
Mesri	Nov 2017	Nov 2017	Mar 2018	Iran	
Internet Research Agency	Feb 2018		Mar 2018	Russia	
Rafatnejad et al.	Feb 2018	Mar 2018	Mar 2018	Iran	
Agha and Dardar	May 2018			Syria	
Park	Jun 2018	Sep 2018	Sep 2018	North Korea	Botnet takedown
Netyksho et al.	Jul 2018		Dec 2018	Russia	
Khusyaynova	Sep 2018	Oct 2018	Dec 2018	Russia	
Morenets et al.	Oct 2018	Oct 2018	Dec 2018	Russia	Allies' Statements
Zhang et al.	Oct 2018	Oct 2018		China	
Savandi and Mansouri	Nov 2018	Nov 2018	Nov 2018	Iran	
Zhu and Zhang	Dec 2018	Dec 2018		China	Pompeo and Nielsen Statement
Witt et al.	Feb 2019	Feb 2019	Feb 2019	Iran	Arrest of Witt
Wang and Doe	May 2019	May 2019		China	

Another trend is that the number of individuals accused in an unsealed indictment has somewhat increased over time, up to groups of twelve or thirteen people, which suggests a better attribution capability. However, no set of charges has named a high-ranking state official – a fact that may suggest it is difficult to provide evidence of criminal responsibility for those higher on the chain of command but also may indicate that the U.S. has wished to limit indictments' impact on relations with the target state.

Lastly, the criminal charges differ also by whether they target state officials or their proxies. For criminal charges against proxies, especially those against the Mersad Co. from Iran and the criminals that aided the FSB in hacking Yahoo!, one factor to consider is whether these will dissuade or disrupt further proxy-state cooperation. Since proxies at least have some level of choice greater than state officials, one U.S. aim has been to drive a wedge between the proxies and their masters. U.S. officials have emphasized that defendants named in criminal charges will not be able to travel or store assets abroad, and U.S. authorities have been able to make some arrests of proxies, but it is still an unresolved question whether that will have an effect on the proxies' cooperation with states.

CONCLUSION

This article has proposed a conceptual framework for understanding criminal charges as an instrument of national cyber policy and discussed considerations for policymakers as they look to use criminal charges to respond to major cyber incidents. One clear conclusion that the framework highlights when applied to the case studies is that criminal charges have demonstrated that the United States now has and is willing to use a robust attribution capability. Thus far criminal charges have largely focused on short-term effects related to informing and providing justice for victims and supporting the technical community and foreign states. However, U.S. policymaking has now moved to a new phase, as the accelerated pace of criminal charges in 2018 shows. In this phase, criminal charges fulfill multiple functions: from diplomatic signaling to enabling other U.S. government actions like sanctions to helping construct international norms of behavior.

In September 2018, the Trump administration published its National Cyber Strategy, which outlined an approach to "preserve peace through strength" by attributing and deterring malicious cyber behavior using "all instruments of national power."[92] The Strategy explicitly discusses that "[l]aw enforcement actions to combat cyber criminal activity serve as an instrument of national power by, among other things, deterring [malicious cyber activity]." In practice, the administration turned to criminal charges, many of which had been in the works since the Obama administration, and started unsealing ones previously held in reserve, taking advantage of the lowest hanging fruit for these purposes. It is likely that this reservoir of sealed criminal charges has now become depleted.

Going forward, in light of the diminishing returns of continuously unsealing criminal charges, the U.S. government should develop a more tailored strategy carefully considering which types of behavior criminal charges are best suited to address and then focus on bringing criminal charges against those specific activities, while considering the importance of preserving law enforcement's political independence. This risk may be particularly acute if criminal charges seem either to fail to impose direct penalties on charged hackers or if target states do not appear to change behavior. To safeguard the future value of criminal charges for all of their diverse ends, U.S. policymakers should clarify their policy priorities. They should clearly describe the intended purposes of criminal charges. In cases where they intend to use criminal charges, policymakers should also seek to unseal the charges as soon as possible so that the U.S. response can be timely from a foreign policy perspective.

One could call a strategy based on these considerations a strategy of "persistent enforcement" in that it accepts that it will not achieve all of these purposes or mitigate all risks in one or even several sets of criminal charges. Rather, criminal charges need to be part of broader efforts to consistently enforce violations of domestic criminal law and international norms against adversary states and their proxies.

Analysts should also recognize that criminal charges on foreign hackers affect not just the charged individuals and state backers but also U.S. allies and the private sector. For example, the U.S. extradition request to Canada for the arrest of Huawei executive Meng Wanzhou could

[92] WHITE HOUSE, *supra* note 8.

foreshadow future U.S. law enforcement requests that put U.S. allies into foreign policy dilemmas.[93] The U.S. government should do more to coordinate with its allies about foreign hacking criminal charges, especially when they concern cyber intrusions that affect those allies. Further, criminal charges have a major impact on private actors, for instance, they provide credibility to attribution of state-backed activity that come from private cybersecurity firms, and they may influence which threats private companies prioritize defending against. The Justice Department should work with other U.S. federal agencies to make sure that the private sector has context to make sense of the information delivered in publicized criminal charges. In addition, scholarship has pointed to the possibility that unsealed indictments could become the basis for private civil actions to seize assets held by foreign governments, which could be a way of providing compensation for victims and the imposition of further costs on state actors.[94]

This article has pointed to the value of criminal charges for both disrupting state-backed hacking and contributing to broader international efforts to respond to malicious state activity in cyberspace. But it would be a mistake to believe that criminal charges can stop foreign cyber crime. Instead, a better frame for thinking about the role of law enforcement is to compare it to law enforcement efforts against organized crime – constant efforts to reduce adversary gains and bring them to justice when possible. This persistent law enforcement will be a continuous response to nation states that increasingly turn to hacking to work against U.S. interests.

Several open questions remain – including how best to preserve the independence of law enforcement as it takes part in a contested political activity, what the demonstrable impacts of criminal charges are on foreign states and their proxies, and why the practice of using criminal charges against foreign state-linked hackers has been exclusively a U.S. practice to date and why no U.S. allies or adversaries have brought charges. This last point would be a valuable inquiry for future research, especially to explore whether differences in legal systems or perspectives on the value of such charges differ across countries. Other subjects for future research include exploring the value of sanctions as a policy tool for combating foreign hacking as well as additional law enforcement tools such as domain name seizures and botnet takedowns.

APPENDIX

This appendix provides a list of all known U.S. foreign hacking charges that either explicitly allege foreign state responsibility for the malicious activity (either hacking or online influence) or charges for which there is reasonable suspicion to believe so. It includes source information and explanations of the links to various states in cases where the charges did not explicitly allege state-sponsorship. It also includes charges against foreign state-linked hackers involved in influence

[93] Another example is Russia's efforts to put pressure on countries considering extraditing Russian cyber criminals to the United States. *See, e.g.*, Jan Velinger, *Russia Slams Czech Republic for Extradition of Suspected Hacker to US*, RADIO PRAHA (Apr. 3, 2018), https://perma.cc/2H6J-5BLE**;** *Who is the Russian Cyber Criminal That Escaped from SL?*, SRI LANKA MIRROR (Dec. 22, 2017), https://perma.cc/83MQ-SEXM.

[94] Paige C. Anderson, *Cyber Attack Exception to the Foreign Sovereign Immunities Act,* 102 CORNELL L. REV. 1087 (2017), https://perma.cc/6JC5-M55M.

operations, which is often considered together with hacking in discussions of deterrence and responding to malicious cyber activity.

1. Nima Golestaneh - Arrow Tech IP Theft; U.S. v. Golestaneh
U.S. Dep't of Justice, *Man Pleads Guilty to Facilitating Computer Hacking of Vermont Company*, (Dec. 2, 2015), https://perma.cc/E9EN-WTR5.
Date filed (unclear): Nov. 2013 at least
Date unsealed (unclear): December 2015 at least
1 individual charged, 6 counts.

State link: A later indictment filed in July 2017 alleges that Golestaneh collaborated with two men who sold the stolen IP to Iranian government and military entities and that the stolen IP was related to missile guidance systems.

2. PLA Unit 61398; *U.S. v. Dong et al.*
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), https://perma.cc/4REV-CU66.
Filed: May 1, 2014
Unsealed: May 19, 2014
5 individuals charged, 31 counts.

State link: Indictees were officers in a unit of China's PLA.

3. Evgeniy Bogachev; *U.S. v. Bogachev*
U.S. Dep't of Justice, *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator* (June 2, 2014), https://perma.cc/3CW3-HN4P.
Filed: May 19, 2014
Unsealed: June 2, 2014
1 individual charged, 14 counts.

State link: As discussed in John Carlin's *Dawn of the Code War,* FBI agents observed the GameOver Zeus botnet siphoning data off its infected machines that they concluded was intended for the use of Russian intelligence services. JOHN CARLIN & GARRETT GRAFF, DAWN OF THE CODE WAR (2018). Also see comments in Garrett Graff, *Inside the Hunt for Russia's Most Notorious Hacker*, WIRED (Mar. 21, 2017), https://perma.cc/J6M2-7S3S.

4. Syrian Electronic Army I; *U.S. v. Agha and Dardar et al.*

U.S. Dep't of Justice, *Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army* (Mar. 22, 2016), https://perma.cc/RBG3-YX85.
(Criminal complaint 1), filed: June 12, 2014
Unsealed: March 22, 2016
2 individuals charged, 5 counts.

U.S. Dep't of Justice, *Syrian Electronic Army Hacker Pleads Guilty* (Sept. 28, 2016), https://perma.cc/Z2BE-H7AZ.

State link: Unclear, reporting and investigation by the Citizen Lab found that the Syrian Electronic Army supported the Assad regime. *See* Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/NAF3-P8QK.

5. Su Bin; *U.S. v. Su Bin*
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), https://perma.cc/R6L8-R6FM.
Su Bin Criminal Complaint, June 27, 2014: https://perma.cc/2FWR-N257
1 individual charged, 4 counts. (Criminal Complaint)
Filed June 27, 2014.

State link: Bin helped hackers in China steal military data on the C-17 to help a Chinese defense contractor. *See* Garrett Graff, *How the US Forced China to Quit Stealing – Using a Chinese Spy*, WIRED (Oct. 11, 2018), https://perma.cc/3SK4-YLBJ.

6. Syrian Electronic Army II; *U.S. v. Romar and Dardar.*
U.S. Dep't of Justice, *Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army* (Mar. 22, 2016), https://perma.cc/7BM4-4LP2.
(Criminal complaint 2), filed: September 29, 2015
Unsealed: March 22, 2016
2 individuals charged, 1 count.

U.S. Dep't of Justice, *Syrian Electronic Army Hacker Pleads Guilty* (Sept. 28, 2016), https://perma.cc/T9QX-WXKQ.

State link: Unclear, reporting and investigation by the Citizen Lab found that the Syrian Electronic Army supported the Assad regime. *See* Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/NAF3-P8QK.

7. Mersad Co., IT-Sec: Financial Sector DDoS Attacks; *U.S. v. Fathi et al.*

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://perma.cc/TLA6-YBQM.
Filed: January 21, 2016
Unsealed: March 24, 2016
7 individuals charged, 3 counts.

State link: Indictment alleges the hackers worked with entities affiliated with the Iranian Revolutionary Guard Corps (IRGC).

8. Arrow Tech IP Theft; *U.S. v. Mohammed Saeed Ajily and Mohammed Reza Rezakhah*
U.S. Dep't of Justice, *Two Iranian Nationals Charged in Hacking of Vermont Software Company* (July 17, 2017), https://perma.cc/G5FJ-CGNY.
Filed April 21, 2016.
Unsealed July 17, 2017.
2 individuals charged, 8 counts.

State link: The July 2017 indictment alleges that the two men sold the stolen IP to Iranian government and military entities and that the stolen IP was related to missile guidance systems.

9. Yahoo Hack; *U.S. v. Dokuchaev et al.*
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://perma.cc/RK4E-WLBR.
Filed: February 28, 2017
Unsealed: March 15, 2017
4 individuals charged, 47 counts.

State link: Two indictees were officers in Russia's FSB.

10. Arrest of Yu Pingan - OPM Hack-linked malware; *U.S. v. Yu Pingan*
United States v. Yu Pingan, No. 17MJ2970, 2017 WL 11435260 (S.C. Cal. Aug. 21, 2017), https://perma.cc/7TFP-MWDZ.
(Criminal complaint). Filed: August 21, 2017.
Unsealed: August 22, 2017.
1 individual charged, 1 count.

State link: Pingan employed a malware variant called Sakula - the same type employed in the OPM hack by actors linked to the Chinese government. In the indictment, the FBI calls this malware "rare." For more see: https://perma.cc/HYJ3-2HAY.

11. Boyusec; *U.S. v. Wu Yingzhuo*

U.S. Dep't of Justice, *U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm For Hacking Three Corporations for Commercial Espionage* (Nov. 27, 2017), https://perma.cc/KT2E-P4S3.
Filed: September 13, 2017
Unsealed: November 27, 2017
3 individuals charged, 8 counts.

State link: Cybersecurity industry analysts and reporting indicated Boyusec was affiliated with the Ministry of State Security. See Insikt Group, *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT 3*, RECORDED FUTURE (May 17, 2017), https://perma.cc/J3TU-NN8U.

12. Behzad Mesri; *U.S. v. Mesri*

U.S. Dep't of Justice, *Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO* (Nov. 21, 2017), https://perma.cc/4UMB-SSAM.
Filed: November 8, 2017
Unsealed: November 21, 2017
1 individual charged, 7 counts.

State link: Mesri was formerly an Iranian military hacker. Extent of the Iranian government's involvement in the HBO hack is unclear. *See* Daniel Victor & Sheera Frenkel, *Iranian Hacker Charged in HBO Hacking that Included 'Game of Thrones' Script*, NEW YORK TIMES (Nov. 21, 2017), https://perma.cc/YA4N-XWHJ.

13. Mabna Institute; *U.S. v. Rafatnejad et al.*

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://perma.cc/V6LY-WVA7.
Filed: February 7, 2018
Unsealed: March 23, 2018
9 individuals charged, 7 counts.

State link: Indictment alleges Mabna Institute worked on behalf of the IRGC.

14. Internet Research Agency; *U.S. v. Internet Research Agency et al.*

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. 26, 2018), https://perma.cc/3AC9-X8QG.
Filed: February 16, 2018.

13 individuals charged, 3 companies, 8 counts.

State link: The indictment indicated IRA received its funding from Yevgeny Prigozhin. Press reports detailed his extended service to the Putin government as a contractor. *See* Thomas Grove, *Kremlin Caterer Accused in U.S. Election Meddling Has History of Dishing Dark Arts*, WALL ST. J. (Feb. 16, 2018), https://perma.cc/4BP8-TKQW.

15. Second Syrian Electronic Army Charges; *U.S. v. Agha and Dardar*
U.S. Dep't of Justice, *Two Members of Syrian Electronic Army Indicted for Conspiracy*, (May 17, 2018), https://perma.cc/YL8B-ZQVA.
Filed: May 17, 2018.
2 individuals charged, 11 counts.

State link: Unclear, reporting and investigation by the Citizen Lab found that the Syrian Electronic Army supported the Assad regime. *See* Sarah Fowler, *Who is the Syrian Electronic Army?*, BBC (Apr. 25, 2013), https://perma.cc/NAF3-P8QK.

16. Park Jin Hyok; *U.S. v. Park*
U.S. Dep't of Justice, *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Sept. 4, 2018), https://perma.cc/8E99-VDRY.
(Criminal Complaint.) Filed: June 8, 2018.
Unsealed: September 6, 2018.
1 individual, 2 counts.

State-link: Indictment says Park worked on behalf of the North Korean regime in a front company.

17. GRU DNC Hack; *U.S. v. Netyksho et al.*
U.S. Dep't of Justice, *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election* (July 13, 2018), https://perma.cc/9X3P-824H.
https://www.justice.gov/file/1080281/download
Filed: July 13, 2018.
12 individuals charged, 11 counts.

State link: Indictees were GRU officers.

18. Elena Khusyaynova – Project Lakhta; *U.S. v. Khusyaynova*
U.S. Dep't of Justice, *Russian National Charged with Interfering in U.S. Political System* (Oct. 19, 2018), https://perma.cc/R6AB-NLTM.
(Criminal complaint), Filed: September 28, 2018.
Unsealed: October 19, 2018.

1 individual charged, 1 count.

State link: The indictment alleges Khusyaynova received funding from Prigozhin, see previous note at IRA indictment for his links to the Russian state.

19. GRU OPCW, WADA Hacking; *U.S. v. Morenets et al.*
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://perma.cc/D4BA-6MK3.
Filed: October 3, 2018.
Unsealed: October 4, 2018.
7 individuals charged, 10 counts.

State link: Indictment names all indictees as GRU officers, including some previously indicted in Special Counsel indictment in July 2018.

20. China JSSD Aerospace Hacking; *U.S. v. Zhang et al.*
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), https://perma.cc/M2TW-FBYQ.
Filed: October 25, 2018
Unsealed: October 30, 2018.
10 individuals charged, 3 counts.

State link: Indictment names hackers as working for a regional branch of the MSS (Jiangsu Province Ministry of State Security – JSSD).

21. SamSam Ransomware Attacks; *U.S. v. Savandi and Mansouri*
U.S. Dep't of Justice, *Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses* (Nov. 28, 2018), https://perma.cc/72FX-KQXD.
Filed: November 26, 2018.
Unsealed: November 28, 2018.
2 individuals, 6 counts.

State link: At this time, unclear. Reporting at the time did not uncover a state link. *See* Brian Barrett, *DOJ Indicts Hackers For Ransomware That Crippled Atlanta*, WIRED (Nov. 28, 2018), https://perma.cc/AKP5-KYWU.

22. Cloudhopper MSS IP Theft Campaign; *U.S. v. Zhu and Zhang*

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://perma.cc/L2NQ-53RJ.
Filed: December 17, 2018.
Unsealed: December 20, 2018. 3 counts.
2 individuals charged.

State link: Indictment says the two men were officers in regional branch of the MSS.

23. U.S. Counterintelligence Agent Defector, Four IRGC-linked Iranians; *U.S. v. Witt et al.*
U.S. Dep't of Justice, *Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues,* (February 13, 2019), https://perma.cc/32Z6-T8RG.
https://home.treasury.gov/news/press-releases/sm611
Note: Also published the indictment in Farsi.
Filed: February 8, 2018
Unsealed: February 13, 2018
5 individuals charged, 7 counts.

State link: The indictment alleges the four Iranians were working on behalf of the IRGC.

24. Anthem Hack, *U.S. v. Fujie Wang and John Doe*
U.S. Dep't of Justice, Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People (May 9, 2019), https://perma.cc/DC7T-ECMR.
Filed: May 7, 2019.
Unsealed: May 9, 2019.
2 individuals charged, 4 counts.

State link: None directly alleged in indictment. In 2015, independent security researchers said the Anthem hack had connections to Chinese academics linked to the MSS.