RESPONSE

FOREIGN AFFAIRS PROSECUTIONS AND CYBERCRIME[†]

MAILYN FIDLER[*]

CONTENTS

[†] An invited response to Steven Arrigg Koh, *Contested Criminalization*, 105 B.U. L. REV. 1799 (2025).

[*] Assistant Professor of Law (Visiting), Harvard Law School; Assistant Professor of Law, University of New Hampshire Franklin Pierce School of Law. Thank you to Steven Koh and Asaf Lubin for helpful feedback.

INTRODUCTION

In his article *Contested Criminalization*, Professor Steven Koh advances a theory of how the United States sets its global criminal justice policy, in which it uses criminal law alongside or instead of tools like diplomacy or sanctions.[1] This article builds on Koh's previous work, in which he makes the case for the existence of U.S. global criminal justice policy and explores one particular expression of this policy—foreign affairs prosecutions—in depth.[2] In this new article, Koh puts forward an account of how U.S. global criminal justice policy gets made. Koh's answer is that changes to this policy happen when the divergent equities of the Departments of State, Justice, and Defense align.[3] And these shifts ultimately happen through the following pathways: codification in domestic law, cooperation with foreign entities, or support for creation of new forms of prosecution such as ad hoc tribunals.[4]

As Koh notes, the U.S. government only inconsistently pursues such criminalization, making this policy tool hard to theorize.[5] Koh's account is an important and helpful contribution in understanding the internal mechanics of these often-opaque decisions. Rather than positioning U.S. global criminal justice policy as solely carceral or solely diplomatic, Koh offers an integrated account, allowing a new view of interagency affairs and how they affect this policy.[6]

But Koh's account does not mine the rich body of evidence from the past decade of cybercrime indictments[7]—U.S. indictments of foreign nationals who have committed criminal cyber acts against the U.S. and its interests. Investigating the cybercrime context reveals additional complexity in the process of foreign affairs criminalization. Examining these indictments reveals that cybercrime foreign affairs prosecutions do not always follow the model Koh

[1] Steven Arrigg Koh, *Contested Criminalization*, 105 B.U. L. REV. 1799 (2025) [hereinafter Koh, *Criminalization*].

[2] *See* Steven Arrigg Koh, *Foreign Affairs Prosecutions*, 94 N.Y.U. L. REV. 340, 341-46 (2019) [hereinafter Koh, *Prosecutions*] (arguing that "foreign affairs prosecutions represent a consequential shift in U.S. criminal law"); Steven Arrigg Koh, *The Criminalization of Foreign Affairs Relations*, 90 FORDHAM L. REV. 737, 740-41 (2021) (arguing that American foreign affairs is experiencing criminalization through a broad range of law and policy choices, including but not limited to foreign affairs prosecutions).

[3] *See* Koh, *Criminalization*, *supra* note 1, at 1802.

[4] *See id.* at 1801-03.

[5] *See id.* at 1806 ("This contested criminalization produces contingency: an ad hoc—as opposed to systematic—approach to U.S. global criminal justice policy . . . .").

[6] *See* Koh, *Criminalization*, *supra* note 1, at 1801 (characterizing scholarship as either resorting to broad labels like "carceral" or focusing on the interagency process, overlooking carcerality).

[7] *See, e.g.*, Garrett Hinck & Tim Maurer, *What's the Point of Charging Foreign State-Linked Hackers?*, LAWFARE (May 24, 2019, 11:20 AM), https:// www.lawfaremedia.org/ article/ whats-point -charging -foreign-state -linked- hackers [https://perma.cc/E729-GCA9] (documenting twenty-four separate cases charging ninety-three foreign nationals for state-linked cybercrime).

advances. Instead, additional pathways for foreign affairs criminalization exist. In turn, these additional pathways reveal that global criminal justice policy can be used to pursue a much broader range of aims than Koh's account suggests, including stymying international cooperation rather than aiding it.

First, most of the global cybercrime charges the U.S. has brought did not involve *codification*, which Koh defines as "amendment of the U.S. Code [to] substantively criminaliz[e] individual conduct arising in geopolitical conflict."[8] Instead, the cybercrime indictments primarily relied on charges already in common use in domestic prosecutions.[9] This feature suggests that foreign affairs criminalization can occur through *redeployment* of domestically-oriented statutes in outward-facing ways rather than through new codification.

Second, these indictments sometimes precede rather than follow *cooperation* with foreign governments. Koh specifically defines cooperation in this context as material change to "executive federal practice that facilitates exchange of evidence or fugitives to foreign national jurisdictions or international criminal tribunals."[10] Instead, the cybercrime indictments reveal that foreign affairs prosecutions can be the *basis* for further international cooperation, rather than the *result* of it.[11] Foreign affairs prosecutions can serve as a leading edge of what will become, but did not necessarily begin as, a coordinated policy response. Criminal law can be the gateway to standard foreign policy responses, rather than substituting for them.

Last, the cybercrime indictments did not involve *creation*, which Koh defines as "establishment of new criminal justice tribunals and mechanisms worldwide."[12] Indeed, during this time, the U.S. actively worked against development of a United Nations ("U.N.") treaty on cybercrime, opposing development of new means of prosecution.[13] Instead, the cyber indictments show that foreign affairs prosecutions may ultimately thwart effective international responses to problems. Connecting to my work on fragmentation of international law and cybercrime,[14] I show that foreign affairs prosecutions can strategically substitute for creation of new legal responses that may be less

[8] Koh, *Criminalization*, *supra* note 1, at 1819.

[9] *See* Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31 EURO J. INT'L L. 969, 971-73 (2020) (highlighting that victim nations of state-sponsored cyber operations avoid invoking international law).

[10] Koh, *Criminalization*, *supra* note 1, at 1824.

[11] *See infra* Part III.

[12] Koh, *Criminalization*, *supra* note 1, at 1830.

[13] *See generally* Mailyn Fidler, *Fragmentation of International Cybercrime Law*, 2025 UTAH L. REV. 737, 744-46 [hereinafter Fidler, *Fragmentation*] (discussing efforts by the United States to support a regional cybercrime agreement over a universal U.N. agreement).

[14] *See id.*; *see also* MAILYN FIDLER, SCIENCES PO, INTERNET FRAGMENTATION'S OUTWARD TURN (June 2025), https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2025/ 06/ The- Splinternets- Outward -Turn_ JUNE-3.pdf [https://perma.cc/ 8ZTR-S9ZY]; Mailyn Fidler, Cybercrime Convergence 1-3 (Sept. 1, 2025) (unpublished manuscript) (on file with author).

subject to U.S. control. By stymying development of international responses, foreign affairs prosecutions can deepen impunity gaps as well as close them.

But the cybercrime literature also benefits from being examined through the lens of Koh's work. Viewing these cybercrime indictments through Koh's account positions them as part of a broader foreign policy goals, not as merely in the business of attribution by indictment.[15] The cybercrime indictments are not just indictments—they are foreign affairs prosecutions, capable of playing a role in architecting and frustrating international cooperation.

I. CYBERCRIME INDICTMENTS AND CRIMINALIZATION LEVERS

In 2014, the United States initiated a new practice by indicting five members of the Chinese People's Liberation Army ("PLA") for hacking into U.S. computers and stealing trade secrets.[16] This indictment was the first of many cybercrime indictments, which have become a crucial part of U.S. cyber policy. The U.S. has continued this practice. For example, in 2017, the U.S. indicted Russian Federal Security Service ("FSB") officers for a hack of Yahoo email accounts.[17] In 2018, Special Counsel Robert Mueller indicted a dozen Russian intelligence officers for attacks leading up to the 2016 elections.[18] In 2019, the U.S. indicted a Chinese national for the 2015 hack of health insurer Anthem.[19] In 2020, the U.S. again indicted PLA members for hacking the credit reporting agency Equifax.[20] Also in 2020, the Department of Justice unsealed another indictment against Russian intelligence officers for the NotPetya attack.[21] In yet another 2020 indictment, the DOJ indicted Chinese nationals Li Xiaoyu and Dong Jiazhi for hacking into a wide variety of networks, including those handling COVID-19 vaccine information.[22] In 2024, just before the U.S. presidential election, the DOJ indicted three Iranian nationals for hacks that

[15] *See, e.g.*, Chimène I. Keitner, *Attribution by Indictment*, 113 AJIL UNBOUND 207, 207-09 (2019) (theorizing that the United States has developed an "attribution by indictment" response to cybercrimes to shame perpetrators, reassure the domestic public, and warn other potential adversaries).

[16] *See* Indictment at 1, United States v. Dong, No. 2:14-cr-00118 (W.D. Pa. May 1, 2014).

[17] *See* Indictment at 2, United States v. Dokuchaev, No. 17-cr-00103 (N.D. Cal. Feb. 28, 2017).

[18] *See* Indictment at 1-2, United States v. Netyksho, No. 1:18-cr-00215 (D.D.C. July 13, 2018).

[19] *See* Indictment at 5-6, United States v. Wang, No. 1:19-cr-00153 (S.D. Ind. May 7, 2019).

[20] *See* Indictment at 1-2, United States v. Zhiyong, No. 1:20-cr-00046 (N.D. Ga. Jan. 28, 2020).

[21] *See* Indictment 1-4, United States v. Andrienko, No. 2:20-cr-00316 (W.D. PA. Oct. 15, 2020).

[22] *See* Indictment at 2, United States v. Xiaoyu, No. 4:20-cr-6019 (E.D. Wash. July 7, 2020).

targeted political discourse prior to the election.[23] The indictments have only continued; for instance, in March 2025, the U.S. indicted twelve Chinese nationals in a new hacking prosecution.[24]

The cybercrime indictments did not come about using any of the levers outlined in Koh's account. The first lever in Koh's account is *codification*.[25] Koh gives the example of amendment of the federal war crimes statute to allow prosecution of individuals present in U.S. territory who perpetrated war crimes, removing the requirement that either the perpetrator or victim be an American national.[26]

But the cybercrime indictments rely on *existing* charges. Moreover, most of the charges in the indictments reflect charges commonly used in domestic criminal prosecutions.[27] For instance, most rely on the federal Computer Fraud and Abuse Act,[28] legislation that was developed primarily with domestic targets in mind.[29] Few of its drafters probably envisioned the use of this law in prosecutions so inflected by world politics.[30]

The second lever in Koh's account is cooperation. In particular, Koh highlights instances in which the U.S. changes its own processes to enable this cooperation. For example, the U.S. amended its laws to allow greater information sharing with the International Criminal Court relating to prosecutions of foreign persons alleged to have committed war crimes in Ukraine.[31]

Some cybercrime prosecutions were built on or involved substantial international cooperation. Consider the 2020 NotPetya indictment,[32] which

---

[23] *See Three IRGC Cyber Actors Indicted for Hack-and-Leak Operation Designed to Influence the 2024 U.S. Presidential Election*, FBI (Sept. 27, 2024), https://www.fbi.gov/video-repository/director-wray-on-indictment-of-iranian-cyber-actors-092724.mp4/view (announcing indictments of three members of Iran's Islamic Revolutionary Guard Corps who targeted a political campaign, current and former U.S. officials, and media outlets).

[24] *See* Devlin Barrett, *Justice Dept. Indicts 12 Chinese in Hacking Plot Against U.S. Targets*, N.Y. TIMES (Mar. 5, 2025), https://www.nytimes.com/ 2025/ 03/05/us/politics/china-hackers-justice-dept.html.

[25] Koh, *Criminalization*, *supra* note 1, at 1819.

[26] *See id.* at 1819-21; Justice for Victims of War Crimes Act, Pub. L. No. 117-351, 136 Stat. 6265, 6265 (2023).

[27] However, reliance on existing law does not preclude arguments that the U.S. should change or expand its laws for prosecuting certain types of cybercrime.

[28] 18 U.S.C. § 1030.

[29] *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563-71 (2010) (describing evolution of the statute from narrow to international).

[30] *See id.* at 1567-68, 1570 (describing how the scope of computers covered under certain sections of the Computer Fraud and Abuse Act expanded from narrowly defined "Federal interest computers" to encompass "protected computers," which include computers abroad that affect U.S. commerce).

[31] *See* Koh, *Criminalization*, *supra* note 1, at 1823-24.

[32] Indictment, *supra* note 21, at 2.

came after the U.S., the other Five Eyes countries, and much of the EU publicly attributed attacks on the country of Georgia to Russia.[33] Or take the example of the Avalanche indictment,[34] in which the U.S. successfully extradited an individual from Bulgaria and worked with European partners to arrest and try related individuals in Georgia and Ukraine in-country.[35]

But the U.S. also pursues many cybercrime indictments where the chance of international cooperation, at least in certain forms, seems all but impossible. Consider that the U.S. does not have extradition treaties with China or Russia, whose nationals make up a considerable proportion of the individuals named in U.S. cybercrime indictments. But perhaps indictment without incarceration actually serves the underlying goal. Indictments can be invitations to other countries to condemn perpetrators or enact sanctions. For instance, at the announcement of the Li and Dong indictment, Assistant Attorney General John Demers remarked that "we are appreciative of the statements that are going to be made by several [like-minded] countries in the coming hours."[36] However, this collective response did not actually materialize.[37] Cooperation, as Koh defines it, sometimes seems incidental, not essential, to these cybercrime prosecutions.

Koh's third lever is support for creation of new means of prosecuting crimes, including support for new ad hoc tribunals. For example, the U.S. supported creation of an ad hoc tribunal to adjudicate alleged war crimes incidents in the Ukraine conflict.[38]

Yet this lever was not used in the context of the cybercrime indictments. Indeed, during this time, the U.S. opposed creation of a new means of prosecution.[39] Most notably, the U.S. voted against the creation of a United Nations ad hoc intergovernmental committee of experts to draft a U.N. cybercrime convention, while continuing to pursue its own cybercrime

[33] *See* David Hechler, *What Is the Point of These Nation-State Indictments?*, LAWFARE (Feb. 8, 2021, 12:21 PM), https://www.lawfaremedia.org/ article/ what-point-these-nation-state-indictments [https://perma.cc/Y589-JS9H] (reporting that the NotPetya indictment "was preceded by a monthslong effort to build a coalition of countries to call out Russia").

[34] *See* Indictment, United States v. Nikolov, No. 2:16-cr-00218-NBF (W.D. Pa. Oct. 4, 2016).

[35] *See* Hechler, *supra* note 33.

[36] *Id.* However, many states did enact sanctions without public condemnations. *See id.*

[37] *See* Stefan Soesanto, *Europe's Incertitude in Cyberspace*, LAWFARE (Aug. 3, 2020, 8:01 AM), https://www.lawfaremedia.org/article/europes-incertitude-cyberspace [https://perma.cc/SPN8-8L3P] (reporting that European nations refused to vocally condemn hacking by Chinese nationals even when European interests were affected).

[38] *See* Koh, *Criminalization*, *supra* note 1, at 1830; Beth Van Schaack, Ambassador-at-Large for Glob. Crim. Just., Off. of Glob. Crim. Just., Remarks on the U.S. Proposal to Prosecute Russian Crimes of Aggression at the Nuremburg Principles Meeting at Catholic University of America (Mar. 27, 2023), https://2021-2025.state.gov/ambassador-van-schaack s-remarks [https://perma.cc/Y2JT-NSY4].

[39] *See* Fidler, *Fragmentation*, *supra* note 13, at 744-46 (noting U.S. support for expanding a regional cybersecurity agreement at the expense of an international U.N. agreement).

indictments.[40] The politics surrounding this lack of support are complicated, but a substantial factor is that the U.S. already supported a different purportedly global mechanism—the 2001 Council of Europe's Budapest Convention on Cybercrime. Despite the Convention's European name, the U.S. had a significant hand in its drafting, shaping it in ways that reflected its own interests.[41]

What emerges from this review of cybercrime indictments alongside Koh's levers is that these levers do not cover the full range of ways the U.S. makes global criminal justice policy. Instead, the cybercrime context demonstrates three additional levers. First, the U.S. can *redeploy* primarily domestic criminal charges in new, outward-facing ways. Second, the U.S. sometimes pursues foreign affairs prosecutions *unilaterally*, either inviting later cooperation or standing in where such cooperation might be difficult. Third, the U.S. can use its prosecutorial power in foreign affairs as a tool to *frustrate* new avenues for prosecution at odds with its interests. The implications of these levers are explored in the next Parts.

II. EXISTING UNDERSTANDINGS OF CYBERCRIME INDICTMENTS

The above narrative of cyber indictments presents a picture of prosecutions that result from redeploying domestic law, acting without guarantee of cooperation, and/or using indictments to slow development of international law. That narrative looks quite different from one centered on codification, cooperation, and creation of new forums. This difference may indicate that additional or different aims might motivate global criminal justice policy. But before advancing my own arguments about what those aims are, I will review the primary explanations given by existing scholarship on cybercrime indictments.

This scholarship looks at these indictments primarily through the lens of attribution—establishing what actor carried out a particular cyber act. Attribution was a central concern of much cyber policy conversations in early years because of the initial technical difficulty of properly attributing attacks. This conversation and related scholarship correctly notes that attribution plays important and foundational roles for states in responding to cyber incidents.[42] Professor Chimène Keitner frames the benefits of attribution by indictment in

[40] *See* Rep. of the Third Comm. on Its Seventy-Fourth Session, U.N. Doc. A/74/401, ¶ 10 (2019) [hereinafter Rep. of the Third Comm.] (recording that the United States voted against the committee recommending ratification of the convention).

[41] *See* Fidler, *Fragmentation*, *supra* note 13, at 745.

[42] *See* Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. Rev. 520, 522 (2020) ("Figuring out who's doing what to whom and publicly identifying those responsible for bad acts in cyberspace are key elements of increasing efforts to hold those actors more accountable.").

terms of its incapacitative, deterrent, and expressive functions, all functions that will be familiar to domestic criminal legal theorists.[43]

First, using indictments to attribute cybercrime can incapacitate the named actors by raising the costs of continuing their attacks through revealing details about their activities.[44] Defenders can use information contained in indictments to strengthen their networks, factoring into future attackers' cost-benefit calculations about attacks.[45] If apprehension and extradition are possible, indictments can also eventually lead to incapacitation by incarceration.[46]

Second, attribution by indictment can serve deterrence purposes. Professor Kristen Eichensehr splits deterrence-by-indictment into two types. First, indictments can serve macro-level deterrence purposes.[47] Public accusation may discourage the named state, and potentially other states, from pursuing further attacks.[48] Second, indictments can have micro-level deterrent effects, discouraging particular actors within targeted countries, both named and similarly positioned, from committing similar acts.[49] The indictments do so by imposing personal costs, such as threat of extradition and incarceration, if they travel to countries that would cooperate with the U.S.[50]

The success of deterrence-by-indictment is contested. Professor Jack Goldsmith has been a prominent critic since the earliest indictments, arguing that the indictments accomplish very little.[51] Others have argued that the

[43] *See* Keitner, *supra* note 15, at 210. Keitner uses "coercive" instead of "incapacitative," but I use the second term because it is more in line with criminal legal scholarship.

[44] *See id.* at 210. Professor Kristen Eichensehr calls this function "deterrence-by-denial." *See* Eichensehr, *supra* note 42, at 555.

[45] *See* Keitner, *supra* note 15, at 210-11.

[46] *See* Hechler, *supra* note 33 (reporting that ringleader of the Avalanche cyberattack was extradited, convicted, and incarcerated).

[47] *See* Eichensehr, *supra* note 42, at 552.

[48] *See, e.g.*, Press Release, U.S. Dep't of Just., Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamicrevolutionary-guard-corps-affiliated-entities-charged [https://perma.cc/ S9ME-HYCK] ("By calling out the individuals and nations who use cyber attacks to threaten American enterprise, as we have done in this indictment, we will change behavior.").

[49] *See* Eichensehr, *supra* note 42, at 554.

[50] *See id.*

[51] *See, e.g.*, Jack Goldsmith, *Why Did DOJ Indict the Chinese Military Officers?*, LAWFARE (May 20, 2014, 6:55AM), https://www.lawfaremedia.org/article/why-did-doj-indict-chinese-military-officers [https://perma.cc/GF42-WRZK]; Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2018, 9:00AM), https://www.lawfaremedia.org/article/failure-united-states-chinese-hacking -indictment -strategy [https://perma.cc/ U8EL-UAPW]; Jack Goldsmith, *The DNC Hack and (the Lack of) Deterrence*, LAWFARE (Oct. 9, 2016, 6:27 PM), https://www.lawfareblog.com/dnc-hack-and-lack-deterrence [https://perma.cc/BGU8-CWZH].

indictments, when paired with broader policy responses, do deter state actors, or at least encourage them to come to the negotiating table.[52]

Indictments also can serve an expressive function, communicating what actions a state considers acceptable in cyberspace.[53] In turn, this communication can contribute to development of international norms.[54] Indictments can do this in multiple ways. Their construction can offer interpretations of existing norms in the cyber context.[55] Indictments can also serve as "an opening bid" from a state about how international legal norms should evolve with respect to new cyber conduct.[56] These "bids" at least open the door to dialogue and possible buy-in from other states.[57]

These scholarly accounts, however, spend little time looking at what happens beyond the moment of indictment. This framing is reflected in the terminology: These accounts all focus on cybercrime *indictments*. Reframing cybercrime indictments as part of a larger phenomenon of global criminal justice policy allows us to look beyond the indictment and at the broader and more structural foreign policy work these prosecutions might be doing. And that work goes beyond the typical incapacitative, deterrent, and expressive aims of criminal law.

III. CYBERCRIME INDICTMENTS AS FOREIGN AFFAIRS PROSECUTIONS

Cybercrime foreign affairs prosecutions can do much more than the work of attribution. They can also play a coordinating function, serving as the foundation for international cooperation. These prosecutions, which might initially look like a unilateral exercise of power, may instead serve as the "tip of the spear" of a broader, coordinated international policy response. In this way, deployment of domestic criminal law can be a gateway to implementing coordinated foreign policy responses, rather than substituting for them.

---

[52] *See, e.g.*, Hechler, *supra* note 33; Benjamin Wittes, *Maybe Those Chinese Cyber Espionage Indictments Weren't So Dumb*, LAWFARE (Dec. 1, 2015, 3:15 PM), https://www.lawfaremedia.org/article/maybe-those-chinese-cyber-espionage-indictments-werent-so-dumb [https://perma.cc/H5RK-59HV]; Benjamin Wittes, *James Lewis on the China Cyber Deal*, LAWFARE (Oct. 5, 2015, 5:42 PM), https://www.lawfaremedia.org/article/james-lewis-china-cyber-deal [https://perma.cc/K6AM-82KF].

[53] *See* Keitner, *supra* note 15, at 211-12.

[54] *See* Finnemore & Hollis, *supra* note 9, at 981-82; Keitner, *supra* note 15, at 211-12; Eichensehr, *supra* note 42, at 556-57 (explaining that attribution allows "states to undertake the process of applying principles to facts that leads to the creation of primary rules to govern state behavior—rules in the form either of norms or, more robustly, as customary international law").

[55] *See* Finnemore & Hollis, *supra* note 9, at 981-82.

[56] *Id.* at 982.

[57] *See e.g.*, Daniel Paltiel, *G20 Communiqué Agrees on Language to Not Conduct Cyber Economic Espionage*, CTR. FOR STRATEGIC & INT'L STUD. (Nov. 16, 2015), https://www.csis.org/blogs/strategic-technologies-blog/g20-communique-agrees-language-not-conduct-cyber-economic [https://perma.cc/TX3F-A7FN] (coming in the wake of the 2014 PLA indictment).

The 2014 indictments of PLA members demonstrate this coordinating function. After issuing the indictments, the U.S. also threatened economic sanctions on China.[58] Instead, the U.S. and China concluded an agreement on cyber espionage, which leaders of the G20 later joined.[59] One domestic indictment set the groundwork for a cooperative international response. In other words, the U.S. deploying its own domestic criminal law sparked an international solution.

This coordinated response often takes the form of economic sanctions. Indictments provide an evidentiary basis not only for domestic prosecutions but also sanctions, domestic and otherwise.[60] For instance, after indicting Islamic Revolutionary Guard Corps-linked hackers in 2016 for distributed denial of service ("DDoS") attacks, the U.S. also imposed economic sanctions on those same individuals.[61] Other countries also enact sanctions after a U.S. indictment. For instance, in 2020, after the U.S. indicted two Chinese nationals for a decades-long computer intrusion campaign, which was encouraged by a Chinese government entity, many European Union member states issued sanctions on the named entities and individuals.[62] Indictments provide this basis for coordinated sanctions in large part because they provide detailed evidence of wrongdoing, allowing countries that do not have the resources or will to investigate to act.[63] The U.S., then, can sometimes achieve international cooperation on matters by first leveraging its domestic law.

But the resulting international cooperation has a particular feature. Using domestic law to set up an international response allows the U.S. to remain somewhat more in charge of the response. It decides who to indict and what details to include and can domestically enact the sanctions response it might prefer other countries emulate. This allows the U.S. a leading voice without having to negotiate the dynamics of international institutions. This way of

[58] *See* Hechler, *supra* note 33.

[59] *See id.*; *see also* Paltiel, *supra* note 57.

[60] *See* John Carlin, Assistant Att'y Gen., Remarks at the Brookings Institute's Emerging National Security Threats Forum (May 22, 2014), https://www.justice.gov/nsd/pr/assistant-attorney-general-john-carlin-delivers-remarks-brookings-institutes-emerging [https://perma.cc/UWP7-BJY8] ("Criminal charges can justify economic sanctions . . . .").

[61] Hinck & Maurer, *supra* note 7.

[62] *See* Soesanto, *supra* note 37.

[63] *See* Eichensehr, *supra* note 42, at 556-57 ("Publicly providing evidence about state behavior can help not just to provide greater information about states' actions, but also to foster *agreement* about the factual reality of what states are doing."). Eichensehr also argues that international law should develop evidentiary standards for attribution. *See id.* at 559-65. In the context of human rights abuses and spyware, it is interesting to note that the U.S. has been hesitant to pursue criminal indictments and has instead preferred to issue only sanctions. This variation in when indictments helpfully precede sanctions deserves more investigation. *See, e.g.*, Mailyn Fidler, *Sanctions for Spyware*, LAWFARE (June 13, 2024, 2:19 PM), https://www.lawfaremedia.org/article/sanctions-for-spyware [https://perma.cc/2LJ6-FNWH]; Mailyn Fidler, *Zero Progress on Zero-Days: How the Last Ten Years Created the Modern Spyware Market*, 102 NEB. L. REV. 713, 750-54 (2024).

coordinating is, then, a kind of projection of power through foreign affairs prosecutions.

The U.S. also projects power through these prosecutions in a second way. The U.S. can deploy cybercrime prosecutions with hopes of frustrating development of less preferred international responses to cybercrime. Just as Koh theorizes that foreign affairs prosecutions occur through creation of new avenues of prosecution, such prosecutions can also be used to discourage creation of such avenues. In this way, cybercrime prosecutions can function as a different exercise of U.S. power on the global stage.

The U.S. cemented its policy of cybercrime indictments during the same years that a global tug-of-war over international cybercrime law occurred. In 2014, when the U.S. issued its first cybercrime indictment, the African Union adopted its Convention on Cybersecurity and Data Protection.[64] This adoption followed two other regional cybercrime conventions.[65] These adoptions are notable because Western powers had already developed the Budapest Convention on Cybercrime and sought global accession of that instrument.[66] Elsewhere, I have argued that these regional conventions were a form of resistance, through fragmentation of international law, to the Western-led Budapest Convention.[67]

Eventually, this resistance coalesced in the United Nations. In 2019, the United Nations General Assembly voted to begin the process of drafting a U.N. Cybercrime Convention.[68] Russia and China prominently supported the convention, as did many countries that had been courted for Budapest Convention accession.[69] Many others notably abstained from the vote, allowing

[64] *See* African Union [AU], African Union Convention on Cybersecurity and Personal Data Protection (June 27, 2014), https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [https://perma.cc/3X9G-8M38].

[65] *See* Shanghai Cooperation Organization, Agreement on Cooperation in Ensuring International Information Security Between the Member States of the Shanghai Cooperation Organization (June 16, 2009), https://eng.sectsco.org/files/207508/207508; League of Arab States [LAS], Arab Convention on Combating Information Technology Offenses (Feb. 15, 2012), https://nsarchive.gwu.edu /document/ 18573- national- security- archive- arab-convention.

[66] Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. 13174, E.T.S. No. 185.

[67] *See* Fidler, *Fragmentation*, *supra* note 13, at 741-42; *see also* Mailyn Fidler, *Infrastructure, Law, and Cyber Instability: An African Case Study*, in CYBERSPACE AND INSTABILITY 281, 289-92 (Robert Chesney et al. eds., 2023) ("[I]nterviewees invariably cast the African Union's launch of this Convention as a kind of response to a perceived sense of vulnerability in a new issue area—cyberspace—and a desire to assert some form of control.").

[68] *See* G.A. Res. 74/247 (Jan. 20, 2020).

[69] *See* Rep. of the Third Comm., *supra* note 40, ¶ 10 (documenting that Russia and China voted for the U.N. convention); *see also* Fidler, *Cybercrime Convergence*, *supra* note 14 (manuscript at 3-4) (noting that Russia and China rejected the cybercrime convention drafted by Western nations and led other nations to favor other agreements).

its success.[70] This Convention was ultimately adopted in 2024 and opened for accession in late 2025.[71]

The U.S. cybercrime prosecutions, although domestic in nature, actually underscore the Budapest Convention approach endorsed by the U.S. The indictments can be seen as proof of concept for the Budapest Convention's "ordinary crime" approach. As I have argued elsewhere, the ordinary crime approach embodied by the Budapest Convention relies on the standard tools of criminal law to address cyber incidents, centering criminal legal actors and institutions rather than those of foreign affairs.[72] In contrast, other regional cybercrime conventions elevate the state's concerns and diplomatic institutions over harms to particular people or entities.[73] By relying on cybercrime indictments, the U.S. was practicing what it preached and treating these incidents as crimes, not as diplomatic incidents more suited to specially applicable law. Certainly, these crimes may entail diplomatic consequences—sanctions, for instance—but cybercrime indictments anchor the response in domestic law. U.S. reliance on cybercrime indictments displays a measure of confidence in the ordinary crime approach and communicates a belief that alternative international models are not needed.

Put differently, the U.S. was, essentially, deploying its own criminal law in part to forestall development of forums poised to develop beyond its control or contrary to its interests. Essentially, the U.S. forum shopped by positioning its own domestic criminal law as a substitute for development of new international forums.[74] Just as the regional conventions fragmented international law in favor of their regions' priorities, doubling down on domestic cybercrime prosecutions likewise reflects American interests and reflects a fragmentation of a sort. Anchoring cybercrime foreign affairs in domestic criminal law keeps the issue flexible: An indictment can stay narrow functionally focused on carceral outcomes, or it can be leveraged into the cornerstone of something bigger.[75]

---

[70] *See* Rep. of the Third Comm., *supra* note 40, ¶ 10.

[71] *See* G.A. Res. 79/243 (Dec. 31, 2024).

[72] Fidler, *Fragmentation*, *supra* note 13, at 750 ("The 'ordinary crime' approach . . . treats cybercrime as an ordinary technocratic issue addressable through existing bureaucratic approaches to transnational crime—charge, extradite, and prosecute . . . .").

[73] *See, e.g.*, *id.* at 751 (explaining that other agreements "broaden what counts as a cybercrime to include a wider range of threats to the state itself").

[74] *See generally* Hannah Murphy & Aynsley Kellow, *Forum Shopping in Global Governance: Understanding States, Businesses and NGOs in Multiple Arenas*, 4 GLOB. POL'Y 139, 145-46 (2013) (highlighting that states engage in international forum shopping to build momentum for their proposed regimes and to avoid opposition to their policy goals); Julia C. Morse & Robert O. Keohane, *Contested Multilateralism*, 9 REV. INT'L ORGS. 385, 393 (2014) (discussing how states pick forums to establish favorable multilateral rules of order).

[75] *See* Eyal Benvenisti & George W. Downs, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STAN. L. REV. 595, 599 (2007) (theorizing hegemonic use of fragmentation, typically marked by narrowly defined agreements, avoidance of formality, and abandoning forums when they begin to favor weaker states).

CONCLUSION

Looking at the cybercrime context through the lens of Koh's work reveals that cybercrime prosecutions accomplish more than attribution alone. Rather, cybercrime foreign affairs prosecutions can also coordinate preferred international responses and strategically substitute for creation of legal responses that may be less subject to U.S. control. In turn, this cybercrime context brings more complexity to Koh's account of global criminal justice policy. Not only can the U.S. enact criminal foreign policy through newly codified crimes, but it can also redeploy already codified domestic crimes. Not only can this policy be shaped through cooperation, but this policy can also coordinate cooperation. Not only can this policy support creation of new means of prosecuting international wrongs, it can also block development of legal responses less subject to U.S. control.

This resulting picture is a messier one: The same tool, foreign affairs criminalization, can be used for a range of ends. But this complexity reveals an important feature of U.S. global criminal justice policy. It can be used to project power and pursue a broad range of interests. The means might be domestic, but the ends can be structural, international, and power political.