Yale Journal of Law & Technology
Volume 27, Issue 1

Jurisdictional Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdiction

Eli Scher-Zagier[*]

Faced with spiking computer crime, the United Nations adopted a global cybercrime convention in December 2024. This watershed moment was the result of rushed, combative negotiations that involved a wide range of stakeholders. Occupied with contentious fights over overbroad substantive provisions, negotiating states paid little attention to the jurisdictional provisions of the convention.

Yet a provision granting states jurisdiction over crimes committed anywhere in the world against their nationals, known as passive personality jurisdiction, represents a major expansion of jurisdiction under international and domestic law. Adoption of this type of jurisdiction in the treaty consummates a rise that has taken it from spurned to ubiquitous in a few short decades.

Passive personality jurisdiction threatens sovereignty, due process, and human rights. It remains both ill-advised and unnecessary. Other jurisdictional bases better address the jurisdictional challenges posed by cybercrime. But if passive personality jurisdiction is here to stay, states can take steps to mitigate its harm: from limiting it to violent, universal offenses to taking unilateral measures that impose costs on abusive passive personality prosecutions.

---

[*] Yale Law School, J.D., 2025. This paper began in Professor Oona Hathaway's International Law class, and I am grateful for her helpful feedback throughout the drafting and editing process. As part of a writing group in that class, Rossella Gabriele, Madison Rinder, Bill Kerin, and Maggie Mills offered structural suggestions. Nicolas Madan, Alyssa Resar, Arjun Talpallikar, Sam Klein, and others provided incisive, timely feedback during the editing process. Finally, thank you to the editors of the *Yale Journal of Law & Technology*, who have shepherded this piece to publication and offered important edits and comments, big and small.

Article Contents

Introduction

On December 24th, 2024, the United Nations (UN) General Assembly approved a new cybercrime treaty without a vote.[1] Many negotiating states heralded its adoption, while a chorus of businesses and human rights organizations lambasted it.[2] But the treaty, which will go into effect shortly after 40 states ratify it,[3] does much more than either its supporters or opponents realize.

A provision of the convention authorizes states to exercise jurisdiction over any conduct that harms their nationals.[4] This type of jurisdiction is known as passive personality jurisdiction and "historically has been more controversial than jurisdiction based on territory or [the nationality of the perpetrator]."[5] When France suddenly adopted unlimited passive personality jurisdiction—asserting it could try anyone for any crime committed anywhere in the world against any French national—the French justice minister told the legislature in 1989 that it was "manifest imperialism that is

---

[1] Vibhhu Mishra, *UN General Assembly Adopts Milestone Cybercrime Treaty*, UN NEWS (Dec. 24, 2024), https://news.un.org/en/story/2024/12/1158521 [https://perma.cc/9W8J-RM8F].

[2] *See, e.g.*, *Global Business Urges Governments to Reject New International Cybercrime Treaty*, INT'L CHAMBER COM. (Aug. 13, 2024), https://iccwbo.org/news-publications/news/global-business-urges-governments-to-reject-new-international-cybercrime-treaty [https://perma.cc/4BUQ-N876]; Katitza Rodriguez, *The UN General Assembly and the Fight Against the Cybercrime Treaty*, ELEC. FRONTIER FOUND. (Sept. 26, 2024), https://www.eff.org/deeplinks/2024/08/un-general-assembly-and-fight-against-cybercrime-treaty [https://perma.cc/ZFZ5-4L9G].

[3] Mishra, *supra* note 1.

[4] G.A. Res. 79/243, annex, United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes art. 22(2)(a) (Dec. 24, 2024) [hereinafter UN Cybercrime Convention]. This paper interchangeably uses "convention" and "treaty" to refer to the UN instrument.

[5] RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW § 411 cmt. a (AM. L. INST. 2017) [hereinafter RESTATEMENT (FOURTH)]; *see also* Harvard Draft Convention on Jurisdiction with Respect to Crime, 29 AM. J. INT'L L. SUPP. 435, 579 (1935) [hereinafter Harvard Draft] ("Jurisdiction asserted upon the principle of passive personality without qualifications has been more strongly contested than any other type of competence.").

difficult to justify."[6] From that perspective, this treaty makes every state an empire, authorized to extend its law around the world and to intrude into the ordinarily exclusive jurisdiction that other states have to regulate and permit the conduct of citizens in their territory.

What might an exercise of this power look like? Imagine an American journalist, living and working in the United States, discovers a misconfigured U.S. corporate database and reports on the exposure of Russian citizens' personal data (thus harming those citizens).[7] Under the cybercrime treaty's provision for passive personality jurisdiction, Russia could seek Turkey's help in surveilling, arresting, and extraditing the journalist when she passes through Istanbul on vacation. The journalist could try to invoke the treaty's human rights provisions to argue that her conduct should not qualify as illegal access.[8] But even if those provisions were enforceable (which they may not be),[9] the treaty endorses this type of extraterritorial jurisdiction over foreign conduct by foreign nationals in foreign states—even when the conduct has little effect on the prosecuting state.

This overbroad jurisdictional element will thwart, not aid, international cooperation on countering cybercrime, the avowed goal of the treaty since the General Assembly created a committee to negotiate it. The 2019 constituting resolution gave the committee a formal name that is a mouthful: the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes—the Ad Hoc Committee, or AHC, for short.[10]

---

[6] Eric Cafritz & Omer Tene, *Article 113-7 of the French Penal Code: The Passive Personality Principle*, 41 COLUM. J. TRANSNAT'L L. 585, 588 & n.14 (2003) (quoting *Journal officiel de l'Assemblée nationale*, 1st Sess. of Oct. 11, 1989, at 3380 (Fr.)).

[7] Whether such conduct would violate domestic U.S. law is a complicated question. *Cf.* Orin Kerr, *Does Obtaining Leaked Data From a Misconfigured Website Violate the CFAA?*, WASH. POST (Sept. 8, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/08/does-obtaining-leaked-data-from-a-misconfigured-website-violate-the-cfaa [https://perma.cc/743V-NYPQ].

[8] UN Cybercrime Convention, *supra* note 4, arts. 6, 24(1) (defining human rights provisions). Article 7 defines illegal access and provides that states may—but need not—require "dishonest or criminal intent." *Id.* art. 7(2).

[9] *See* Rodriguez, *supra* note 2.

[10] The committee's name and secretariat (the UN Office on Drugs and Crime) are discussed in G.A. Res. 75/282, ¶¶ 1-2 (June 1, 2021).

That resolution warned that digital technologies, or information and communications technologies in the bureaucratese, "create new opportunities for perpetrators and may contribute to a rise in the levels and complexity of crime" and noted the risk to critical infrastructure.[11]

From the beginning, however, many states sought to turn the treaty into a global speech code, part of a well-worn—and often successful—playbook that Moscow has used at the United Nations to repress speech.[12] Russia proposed an expansive convention, including articles that would require each state to establish vague, overbroad speech offenses. For instance, one provision would have required each state to criminalize using technology to "humiliat[e] . . . a person or group of people on account of their race, ethnicity, language, origin or religious affiliation."[13] In the face of strong opposition, Russia—and its authoritarian allies that supported the same language[14]—ultimately failed to include these offenses.

Nevertheless, as this paper shows, these authoritarian states still won tools that will help them gain other nations' assistance in repressing speech, notably the expansive jurisdictional reach of the cybercrime convention. This jurisdictional expansion is part of a growing trend of expanding jurisdictional bases under international

---

[11] G.A. Res. 74/247, at 1 (Dec. 27, 2019).

[12] In drafting meetings for the Universal Declaration of Human Rights, the Soviet Union proposed language modeled on communist constitutions, such as the Soviet Union's criminalization of "[a]ny advocacy of racial or national . . . hatred." NADINE STROSSEN, HATE: WHY WE SHOULD RESIST IT WITH FREE SPEECH, NOT CENSORSHIP 26 (2018). At the UN, American representative Eleanor Roosevelt "warned that incorporating such language in UN instruments was 'extremely dangerous' and 'likely to be exploited by totalitarian States for the purpose of rendering the other [human rights] articles null and void,' because 'criticism of public or religious authorities might all too easily be described as incitement to hatred and consequently prohibited.'" *Id.* (alteration in original). United in opposition, other democratic countries made similar arguments, but the American "warnings proved sadly prophetic." *Id.*

[13] Chargé d'affaires a.i. of Russia to the U.N., Letter dated 30 July 2021 from the chargé d'affaires a.i. of the Russian Federation to the United Nations addressed to the Secretary-General, art. 21, U.N. Doc. A/75/980* (Aug. 10, 2021) [hereinafter Initial Russian Draft Convention].

[14] *See* Russia, Submission to the Second Session of the Ad Hoc Committee also on Behalf of Belarus, Burundi, China, Nicaragua and Tajikistan (Apr. 7, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf [https://perma.cc/WC9Q-Z9KW].

law, a trend that has escaped scrutiny and that, if left unchecked, will erode the traditionally limited bases of jurisdiction and undermine human rights by facilitating a nearly unlimited reach for authoritarian countries' criminal laws. Passive personality jurisdiction is not new, but this treaty—by approving its global use for amorphous cybercrimes—both illustrates the dangers of expanding passive personality jurisdiction and solidifies its emerging place in criminal jurisdiction more than any previous treaty or action. This expansion, unnecessary in the cyber context and elsewhere, has ramifications far beyond the cybercrime convention.

This paper makes three contributions to the literature. First, it focuses attention on the expansion of passive personality jurisdiction, a little-noticed trend in the literature on international jurisdiction.[15] The field of of international jurisdiction is itelf neglected and "not often subjected to sustained inquiry."[16] Second, this paper highlights the momentous implications of the cybercrime convention for the treaty and customary law of international criminal jurisdiction, breaking from the conventional characterization of passive personality jurisdiction as limited.[17]

Finally, it highlights the worrying implications of passive personality jurisdiction for free speech, privacy, and human rights. The cybercrime treaty provides a particularly good case study for this point because the treaty illustrates the broad, expanding range of conduct that passive personality jurisdiction encompasses, often traditionally domestic conduct that now reaches foreign shores. In

---

[15] Kenneth Gallant is one of the few scholars to give international criminal jurisdiction, including passive personality jurisdiction, the attention it deserves. He writes "that common law states may eventually recognize . . . [passive personality] jurisdiction more generally than they traditionally have." KENNETH S. GALLANT, INTERNATIONAL CRIMINAL JURISDICTION: WHOSE LAW MUST WE OBEY? 460 (2022). That moment has arrived with the cybercrime treaty.

[16] Nico Krisch, *Jurisdiction Unbound: (Extra)territorial Regulation as Global Governance*, 33 EUR. J. INT'L L. 481, 481 (2022).

[17] *See, e.g.*, *Report of the International Law Commission to the General Assembly*, U.N. GAOR Supp. No. 10, at 524 n. 23, U.N. Doc. A/61/10 (2006) ("[M]ost of the States, the United States included, give effect to this principle but limit its application to particular crimes . . . ."); GALLANT, *supra* note 15, at 456 ("[I]t is fair to say that the United States and other common law countries adopting such [passive personality jurisdiction] statutes have abandoned their objection to passive personality jurisdiction with respect to terrorist crimes . . . not . . . the persistent objection as to other types of crime.").

announcing its support for the convention, the United States argued that the treaty "cannot prevent" a state from repressing "human rights defenders, journalists, dissidents, and others" but that states "may not invoke this convention to facilitate [those abuses]."[18] In other words, the U.S. government believed that the treaty would neither thwart nor aid repression. This paper demonstrates one mechanism by which the convention could facilitate human rights violations, contrary to proponents' claims.

Part I of this paper describes the substantive scope of the UN cybercrime convention and how it differs from an existing international instrument, the Budapest Convention on Cybercrime, that the Council of Europe created 20 years ago. Part II discusses the rise of passive personality jurisdiction and its seemingly uncontroversial inclusion in the convention. It argues that this inclusion represents a significant expansion, one that was made without considering the long-recognized problems of passive personality jurisdiction. Part III argues that such an expansion is both unneeded in the cyber context, because other jurisdictional bases cover cybercrime, and ill-advised in general. It then outlines systematic and unilateral mitigations that states can take if they retain passive personality jurisdiction.

I. A Convention is Born

Drawing on public negotiating sessions and submissions from parties and stakeholders, this Part describes how the offenses in the UN convention compare to those in the Budapest Convention on Cybercrime, the largest preexisting international agreement on cybercrime. It highlights several substantive and structural innovations in both the convention and the drafting process. The fast, unwieldy negotiating process necessarily focused on the most visible substantive problems, overlooking the key jurisdictional issues.

A. Substantive Innovation

Negotiating states fundamentally disagreed about the ideal

[18] AHC, Explanation of Position of the United States (Aug. 10, 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/US_Statement_with_EOPs.docx [https://perma.cc/5JUG-S76W].

scope of the UN convention. They ultimately settled on substantive offenses that are narrower than some states sought but that remain open to redefinition and expansion by each state.

1. Comparison with the Budapest Convention on Cybercrime

International cybercrime instruments and cooperation are not new. The most important effort occurred more than two decades ago, in November 2001, when the Council of Europe created the Budapest Convention. As of February 2025, the Budapest Convention had 78 parties, including the United States, Canada, nearly every European nation, half of South America, and several nations in Africa and Asia.[19] Seventeen other countries have signed or been invited to accede to it.[20]

Crimes that are only possible to commit with computers are the focus of the Budapest Convention. These include accessing, tampering with, or intercepting electronic information or systems; without computers, these crimes would not exist. Such offenses are known as core cybercrime or cyber *dependent* crimes.[21] A wider range of crimes that use or benefit from computers in their commission include child exploitation and illegal speech, offenses often termed cyber *enabled* crimes.[22] The difference between these types of crimes crystallizes when considering that international criminal treaties generally focus on categories of crime, not the

---

[19] *The Budapest Convention (ETS No. 185) and Its Protocols*, COUNCIL EUR., https://www.coe.int/en/web/cybercrime/the-budapest-convention [https://perma.cc/G57K-Y9BZ].

[20] *Id.*

[21] *See, e.g.*, *Global Cybercrime Treaty: A Delicate Balance Between Security and Human Rights*, UN NEWS (Feb. 25, 2024), https://news.un.org/en/interview/2024/02/1146772 [https://perma.cc/TUJ7-97DX] (describing some of the terminology); AHC, Contribution From the European Union and Its Member States, at 2 (Nov. 2, 2021), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/EU_Position_for_AHC_first_session.pdf [https://perma.cc/U655-C6LH] (calling for criminalization only of "high-tech crimes and cyber-dependent crimes").

[22] *See, e.g.*, Charlie Plumb, *Understanding the UN's New International Treaty to Fight Cybercrime*, UN UNIV. CTR. FOR POL'Y RSCH. (July 30, 2024), https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime [https://perma.cc/9D4S-HUXJ] (describing the difference between cyber enabled and cyber dependent crimes).

means of executing them. There is no international treaty targeting the use of motor vehicles in crime (what we might call vehicle enabled crimes), even though perpetrators of a wide variety of crimes use motor vehicles in the commission of their crimes. The basic problem with targeting material objects used to execute crimes is that it risks criminalizing conduct, such as certain speech, that one state wants to authorize. International law does not treat computers as inherently illicit materials, in contrast to its treatment of narcotic drugs and counterfeit currency, so international criminalization of cyber enabled crimes would create overinclusivity and sovereignty problems.

The Budapest Convention largely maintains the traditional focus on categories of crimes in requiring state parties to criminalize nine categories of substantive offenses: unauthorized access, unauthorized interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child-pornography-related offenses, and copyright-related offenses.[23] The first seven categories are cyber dependent offenses. The latter two are cyber enabled, but the Budapest Convention tightly links the scope of those two offenses with the indispensability of the cyber element. For instance, "producing child pornography *for the purpose of its distribution through a computer system*" is a covered offense.[24] Copyright offenses are limited by requirements of intent, "commercial scale," and computer indispensability,[25] all elements that demonstrate the narrow target of

---

[23] Budapest Convention on Cybercrime, arts. 1-10, Nov. 23, 2001, ETS 185. Beyond criminalizing the substantive offenses, parties to the Budapest Convention must also ensure that liability for the substantive offenses extends to legal persons (i.e., corporations) and to two forms of inchoate offenses (attempt and aiding or abetting). *Id.* arts. 11-12. There are two Additional Protocols to the Budapest Convention, one of which degrades this approach by mandating criminalization of racist and xenophobic speech. Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Jan. 28, 2003, ETS 189.

[24] Budapest Convention on Cybercrime, *supra* note 23, art. 9(1)(a) (emphasis added). A couple of other covered child pornography offenses are arguably less tightly tied, such as possession of electronic child pornography. *Id.* art. 9(1)(e). But states are given the option of establishing those as criminal offenses. *Id.* art. 9(4). Moreover, unlike other crimes, child pornography offenses are neither particularly controversial nor particularly susceptible to overbroad application.

[25] *Id.* art. 10.

these offenses and limit overbroad application.

But disagreement about whether to maintain or discard this approach was at the heart of the UN cybercrime convention's debate between cyber dependent and cyber enabled crime.[26] From the beginning, the scope of the new treaty drew questions. States, especially those that initially opposed the committee's creation, sought to limit the treaty's scope to cyber dependent crime.[27]

The perpetual fight over the UN convention title reflected this contentious debate. Was the treaty about cybercrime (i.e., cyber dependent crime) or about the use of computers for criminal purposes (i.e., cyber enabled crime)? The General Assembly resolution created a committee "to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes."[28] The resolution never stipulated a title for the convention, and the phrase "the use of information and communications technologies for criminal purposes" appeared to evoke the broader category of cyber enabled crimes. When the UN Office on Drugs and Crime (UNODC) Secretariat drafted an agenda for the committee's organizational session, it included a committee title that mirrored the language of the General Assembly resolution.[29] But the European Union (EU) delegation objected, suggesting a "footnote explaining [the title] does not pre-define the title of [the] future

---

[26] Jonathan Greig, *On Eve of Final Negotiations, US Says Consensus Growing Around 'Narrow' UN Cybercrime Treaty*, RECORD (Jan. 23, 2024), https://therecord.media/consensus-growing-around-cybercrime-treaty [https://perma.cc/PU2L-PBZ7] (citing a State Department media briefing referring to it as the core debate).

[27] *See, e.g.*, OFF. OF THE SPOKESPERSON, U.S. DEP'T OF STATE, *Media Note: Ad Hoc Committee to Elaborate a UN Cybercrime Convention Fourth Negotiating Session at the United Nations in Vienna, Austria* (Jan. 9, 2023), https://www.state.gov/ad-hoc-committee-to-elaborate-a-un-cybercrime-convention-fourth-negotiating-session-at-the-united-nations-in-vienna-austria [https://perma.cc/ZUQ4-BPZ8] ("The United States continues to seek a broad consensus for a narrowly focused criminal justice instrument . . . .").

[28] G.A. Res. 74/247, at 3 (Dec. 27, 2019).

[29] AHC, Rolling Text of the Draft Provisional Agenda for the Organizational Session, at 1 (July 17, 2020), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Provisional_agenda_for_meeting_17_July_2020_rolling_text.pdf [https://perma.cc/VY8U-8QY6].

convention."[30]

For several drafts, the committee chair simply omitted any convention title, but eventually the problem came to a head. As the clock ran out on negotiations in February 2024, the chair distributed a draft with the title "United Nations Convention against Cybercrime."[31] Russia and nearly 20 other countries continued to advocate the more expansive title, reflecting their desire to criminalize an array of conduct that simply benefits from computers (e.g., dissident political organizing that occurs online).[32] The treaty text that the committee agreed to submit to the General Assembly sought to please both sides, with the following title:

> Draft United Nations convention against cybercrime
>
> Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for sharing of evidence in electronic form of serious crimes.[33]

The two sentences were the same size and separated by no punctuation, creating visual faithfulness to the idea that they together formed the title. Perhaps because of this, the chair orally revised the draft to include a semicolon after the first line.[34]

The treaty title is only symbolic, but substance mirrored form in the early negotiations. Early on, the United States, United Kingdom, EU, and several other countries proposed offenses and language

---

[30] *Id.*

[31] AHC, Further Revised Draft Text of the Convention, U.N. Doc. A/AC.291/22/Rev.2, at 2 (Feb. 6, 2024) (including a title); *see* AHC, Revised Draft of the Convention, U.N. Doc. A/AC.291/22/Rev.1 (Nov. 6, 2023) (no convention title included).

[32] *Cyber Convention Check-in*, GLOB. INITIATIVE AGAINST TRANSNAT'L ORGANIZED CRIME (Feb. 6, 2024), https://globalinitiative.net/announcements/cyber-convention-check-in [https://perma.cc/H9AU-YM5T] (describing Russia's title proposal on February 5th, 2024).

[33] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft United Nations Convention Against Cybercrime, U.N. Doc. A/AC.291/L.15, at 1 (Aug. 7, 2024).

[34] AHC, Draft Report, A/AC.291/L.14/Add.1, ¶ 12 (Aug. 9, 2024).

largely lifted from the Budapest Convention.[35] And the UN treaty does not drift far from the Budapest Convention's substantive coverage. In fact, its first eight criminalization articles mirror the first eight in the Budapest Convention.[36] The treaty even replicates the order and much of the language of the substantive offenses in the Budapest Convention.[37] However, the UN treaty is not identical in coverage, as it dispenses with the copyright offense. It also adds new offenses covering solicitation or grooming of minors, dissemination of non-consensual intimate images (sometimes imprecisely referred to as "revenge porn"), and money laundering.[38] Nevertheless, the criminalization articles more closely track those of the Budapest Convention than many autocratic states had sought. This substantive similarity to the Budapest Convention is a significant win for democratic states, which focused their efforts on stalling the broadest, most dangerous proposals. But it was hardly preordained.

2. Expansion Proposals

Negotiating documents and early drafts included far more sweeping substantive offenses than appear in the final text. Many countries sought to avoid the stronger human rights protections in the Budapest Convention and introduce broader offenses.[39] Russia

---

[35] Compilation of Draft Provisions Submitted by Member States on Criminalization, General Provisions and Procedural Measures and Law Enforcement, at 6, 8, 10, 13, 16-17, 20-21, 30-31, 33, U.N. Doc. A/AC.291/CRP.11 (May 23, 2022) [hereinafter Second Session Draft Provisions]. The exact configuration varied; for instance, the EU did not propose the Budapest Convention language for child exploitation, copyright, and certain other offenses. *Id.* at 21, 31, 33.

[36] *Compare* Budapest Convention on Cybercrime, *supra* note 23, arts. 2-9 *with* UN Cybercrime Convention, *supra* note 4, arts. 7-14.

[37] *See, e.g.*, UN Cybercrime Convention, *supra* note 4, art. 10 (copying virtually word-for-word the system interference offense from Article 5 of the Budapest Convention, with the main changes being the replacement of "computer system" with "information and communications technology system" and "computer data" with "electronic data").

[38] *Id.* arts. 15-17.

[39] Rishi Iyengar, Robbie Gramer & Anusha Rathi, *Russia Is Commandeering the U.N. Cybercrime Treaty*, FOREIGN POL'Y (Aug. 31, 2023), https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty [https://perma.cc/6B5Z-487J] ("The idea of the new treaty was a brainchild

was the initial sponsor of the UN General Assembly resolution to establish the Ad Hoc Committee,[40] and the countries who joined Russia in sponsoring the resolution were a who's who of autocracies.[41]

Reflecting its strenuous attempt at a general crime treaty, Russia was the only state to submit an entire draft convention before the first substantive negotiating session.[42] It proposed criminalizing unauthorized access to personal data, which, unlike the other proposed offenses, was not limited to electronic access.[43] In other words, this would have created an international, standardless intrusion of privacy crime that would have swept in a significant portion of journalism that involves personal information.

Russia also proposed offenses for content related crimes aimed at policing online speech. One was the creation and use of digital

---

of Russia and some other not-so-democratic countries in a bid that digital rights experts suspect was aimed at supplanting the Budapest Convention with a newer framework that could have more of the Kremlin's influence in its design.").

[40] U.N. GAOR Third. Comm., 74th Sess., 44th mtg ¶ 84, U.N. Doc. A/C.3/74/SR.44 (Feb. 21, 2020).

[41] The original co-sponsors were Belarus, Cambodia, China, North Korea, Myanmar, Nicaragua, and Venezuela, all of which are ranked Not Free by Freedom House. Third Comm., Draft Resolution Submitted by Belarus, Cambodia, China, Democratic People's Republic of Korea, Myanmar, Nicaragua, Russian Federation, and Venezuela, U.N. Doc. A/C.3/74/L.11 (Oct. 11, 2019). Even when additional countries joined, they were largely autocracies. U.N. GAOR Third. Comm., 74th Sess., 44th mtg, *supra* note 40, ¶ 87; Third. Comm., Draft Resolution Submission, U.N. Doc. A/C.3/74/L.11/Rev.1, at 1 (Nov. 5, 2019). Out of thirty-one sponsors, twenty-five are considered Not Free by Freedom House; four Partly Free; and two Free. *Countries and Territories*, FREEDOM HOUSE, https://freedomhouse.org/countries/freedom-world/scores [https://perma.cc/W7JT-FMCU]. Other countries joined later as sponsors of the draft resolution, Rep. of the Third Comm., ¶ 7, U.N. Doc. A/74/401 (Nov. 25, 2019), half of which were countries considered Not Free by Freedom House.

[42] Initial Russian Draft Convention, *supra* note 13. Egypt was the only other country to submit anything even resembling a draft, but it contained only certain elements and was a fraction of the size and detail of the Russian submission. *See* UNODC Secretariat, Compilation of Views Submitted by Member States on the Scope, Objectives and Structure (Elements) of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, at 22-33, U.N. Doc. A/AC.291/4 (Nov. 17, 2021) [hereinafter First Session Compilation of Views].

[43] Chargé d'affaires a.i. of Russia to the U.N., Letter dated 30 July 2021 from the chargé d'affaires a.i. of the Russian Federation to the United Nations addressed to the Secretary-General, art. 12, U.N. Doc. A/75/980* (Aug. 10, 2021).

information to mislead a user,[44] an offense that would have covered any information deemed misinformation. No intent to mislead would have been necessary, so long as the information met the low, amorphous standard of "capable of being mistaken for information already known and trusted by a user."[45] Other content offenses included incitement to subversive or armed activity; terrorism offenses, such as incitement and "justification of terrorism"; and extremism offenses.[46] The extremism offenses included "distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic, or religious hatred or enmity, advocacy and justification of such actions, or . . . provid[ing] access to such materials, by means of [technology]."[47] Also covered was "humiliation by means of [technology] of a person or group of people on account of their race, ethnicity, language, origin or religious affiliation."[48] All of these offenses that Russia proposed were mandatory, meaning countries would have been *required* to establish them as crimes under the treaty.[49]

Russia continued to push for the terrorism and extremism offenses throughout the negotiations.[50] Toward the end of negotiations, Russia defended its advocacy of these provisions, arguing that terrorism relies substantially on the internet and that robust criminalization was necessary to enable "effective international cooperation" against terrorism and extremism.[51]

---

[44] *Id.* art. 18.
[45] *Id.*
[46] *Id.* arts. 19-21.
[47] *Id.* art. 21.
[48] *Id.*
[49] *See id.* art. 12 ("Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law . . ."), arts. 18-21 (using similar "shall" language).
[50] *See, e.g.*, AHC Note by the Chair, Consolidated Negotiating Document on the General Provisions and the Provisions on Criminalization and on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, at 6, 10, U.N. Doc. A/AC.291/16 (Nov. 7, 2022) (including the terrorism, extremism, privacy, and subversion offenses in Russia's negotiating stance at the fourth substantive session).
[51] Russia Submission to the Concluding Session of the AHC, Concept Note on

The offenses would have covered a wide range of speech that is protected by the First Amendment and, until recently, by most democratic countries.[52] Justification or advocacy of resistance movements would have likely fallen under the terrorism offense, sweeping in a large portion of current pro-Palestinian speech.[53] As the UN Office of the High Commissioner for Human Rights observed in its submission to the Ad Hoc Committee, "[c]ybercrime laws have been used to impose overly broad restrictions on free expression, for example by criminalizing various online content related to extremism, terrorism, public morals, or hate speech."[54]

Although Russia championed some of the broadest language, other countries also sought to adopt overbroad offenses. For

---

Terrorism and Extremism ("Why does Russia consistently advocate for the inclusion in the future convention of provisions on countering the use of information and communications technologies (ICTs) for terrorist and extremist purposes?"), at 1, 6 (Mar. 12, 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Concept_paper_on_terrorism_and_extremism_E.pdf [https://perma.cc/HKX5-LFUC].

[52] *See* STROSSEN, *supra* note 12, at 26 (describing how "'hate speech' laws . . . were initially promoted in the then-new United Nations by the Soviet Union and its allies . . . and . . . staunchly opposed by almost all liberal democracies"); JACOB MCHANGAMA, FREE SPEECH: A HISTORY FROM SOCRATES TO SOCIAL MEDIA 294 (2022) (recounting how the British representative to the International Covenant on Civil and Political Rights lambasted the Soviet proposal to ban advocacy of hatred, saying that the UK "would maintain and fight for its conception of liberty as resolutely as it had fought against Hitler" (citing U.N. ESCOR, Comm'n on Hum. Rts., 9th Sess., 379th mtg., U.N. Doc. E/CN/.4/SR.379 at 12-13 (1953))). Mchangama terms the current trend toward speech restrictions a "global free speech recession" and writes that "[a]t times European democratic leaders have sounded more like a distorted echo of the Soviet apparatchiks who warned against the flood of Western 'racisim,' 'fascism,' and 'false propaganda' than the stewards of democracies built upon the central premise of free and open debate for all." *Id.* at 3, 384.

[53] *Cf., e.g.*, Letter from Ray Rodrigues, Chancellor, to State Univ. Sys. of Florida Presidents (Oct. 24, 2023), https://www.flbog.edu/wp-content/uploads/2023/10/Deactivation-of-Students-for-Justice-in-Palestine.pdf [https://perma.cc/5ZRP-W5UH] (deactivating Students for Justice in Palestine chapters for allegedly violating a terrorism statute).

[54] Off. of the High Comm'r on Hum. Rts. Submission to the First Session of the AHC, OHCHR Key-messages Relating to a Possible Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Jan. 17, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf [https://perma.cc/8A6B-CLWY].

instance, India proposed a mandatory offense to criminalize sending electronic messages that are "grossly offensive" or aimed at "causing annoyance or inconvenience."[55]

Ultimately, the treaty omitted the broadest, vaguest offense proposals, including many cyber enabled crimes. Yet the treaty retained several crimes that are not intrinsically tied to computers. Notably, Article 13 of the UN treaty adopted a broad computer fraud offense, effectively mandating something close to an international wire fraud offense.[56]

Article 13 covers "the causing of a loss of property to another person" through three possible prongs.[57] Two of them—data interference and system interference—mirror Article 8 of the Budapest Convention, which is computer-related fraud.[58] Indeed, Brazil, Ghana, Jamaica and a cohort of other countries (including the U.S.) proposed simply copying Article 8 of the Budapest Convention.[59]

But a third deception prong in the UN treaty's Article 13 is totally new: "Any deception as to factual circumstances made

---

[55] Second Session Draft Provisions, *supra* note 35, at 40.

[56] UN Cybercrime Convention, *supra* note 4, art. 13. *Cf.* 18 U.S.C. § 1343 (punishing "[w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice"). Domestic mail and wire fraud statutes are notoriously broad. *See, e.g.*, Jed Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771, 772, 821 (1980) (discussing the "expansive use of the mail fraud statute" and suggesting that "the scope of the mail fraud statute is too great, either in requiring only a very minimal amount of reprehensible conduct to trigger its application or in extending its application to an immensely broad and as yet ill-defined spectrum of intentions and activities").

[57] UN Cybercrime Convention, *supra* note 4, art. 13.

[58] Budapest Convention on Cybercrime, *supra* note 23, art. 8 ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.").

[59] Second Session Draft Provisions, *supra* note 35, at 33 (proposal 1 by Brazil, Ghana, and Jamaica on behalf of the Caribbean Community, New Zealand, South Africa, Switzerland, and the United States).

through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do."[60] Early on, Singapore proposed language that appears to be the origin of this prong.[61] In its final form, the treaty clause criminalizes worldwide any lie sent in a text, email, phone call, or social media post that causes financial loss, provided that the sender intended the loss, sought material gain for *anyone*, and did so dishonestly and "without right."[62]

Other provisions—common to both the UN treaty and the Budapest Convention—cover significant cybercrimes like phishing, spoofing, and identity theft.[63] What does the computer fraud offense add? It covers a wide range of social engineering offenses, which, rather than rely solely on technical exploitation, trick victims into making mistakes. Consider the growing cybercrime known as pig butchering or romance baiting, a relationship scam in which criminals build trust in online interactions, often beginning with a wrong-number text,[64] and then seek monetary transfers.[65] This crime might fall under the data interference prong of computer fraud, as it covers "causing . . . loss of property to another person by means of . . . [a]ny input . . . of electronic data."[66] But pig butchering certainly falls under the deception prong, as it always involves "deception as to factual circumstances . . . that causes a person to do [something] which that person would not otherwise do."

Yet a startling range of conduct seems to fall under the deception

---

[60] UN Cybercrime Convention, *supra* note 4, art. 13(c).

[61] Second Session Draft Provisions, *supra* note 35, at 35 (proposal 6 covering "using a computer system to deceive or induce another person or an entity to do or omit to do anything which the person or entity would not otherwise do or omit to do").

[62] UN Cybercrime Convention, *supra* note 4, art. 13.

[63] *See id.* arts. 11, 12 (criminalizing, respectively, the procurement of access credentials and the alteration of electronic data); Budapest Convention, *supra* note 23, arts. 6, 7 (same).

[64] *See, e.g.*, Demian Bulwa, *He Thought He'd Won Big on Love and Crypto. Instead, He Was 'Pig-Butchered' for $260K*, S.F. CHRON. (Nov. 17, 2023), https://www.sfchronicle.com/politics/article/pig-butchering-scam-18493673.php [https://perma.cc/3KLE-3KTJ].

[65] *See* John M. Griffin & Kevin Mei, *How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering* (Feb. 29, 2024), https://ssrn.com/abstract=4742235 [https://perma.cc/92MQ-4T4G].

[66] UN Cybercrime Convention, *supra* note 4, art. 13(a).

prong's language, and each state's ability to adjudicate what is deception, intent, and "without right" might make this provision practically limitless. If states opted for broad readings of these elements, the following activity might fall under the coverage of this offense:

- A Chinese company, or a foreign one doing business in China, emails concerns about alleged Chinese human rights abuses to a subcontractor and says that it will terminate a contract or not pay for the goods and services already provided if the human rights violations are not addressed. The Chinese government has repeatedly called allegations of forced labor in Xinjiang "lies and false information."[67] Any reputational harm to the owner of the subcontractor that causes financial loss (e.g., lost income) could bring it under Article 13.
- An Israeli citizen, or a foreigner in Israel, makes a social media post claiming that Israel is committing genocide and supporting a boycott against an Israeli business owner. Israel has said that "there can hardly be a charge more false and more malevolent than the allegation against Israel of genocide,"[68] and it has created a civil tort (though not criminal penalties) for successfully supporting boycotts.[69]

While the treaty still requires "fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property,"[70] a domestic court could easily consider

---

[67] *See, e.g.*, *China Rejects Accusations of Abuses in Xinjiang*, AP (Apr. 20, 2021), https://apnews.com/article/china-religion-f5da39345535cc8736f3f3b9a133ab7d [https://perma.cc/C3M5-2T2N].

[68] Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (S. Afr. v. Isr.), Verbatim Record, ¶ 52 (Jan. 12, 2024, 10 a.m.), https://www.icj-cij.org/sites/default/files/case-related/192/192-20240112-ora-01-00-bi.pdf [https://perma.cc/R65J-DLLM].

[69] Revital Hovel, *High Court Largely Upholds Controversial 'Anti-Boycott Law'*, HAARETZ (Apr. 16, 2015), https://www.haaretz.com/2015-04-16/ty-article/.premium/court-upholds-controversial-anti-boycott-law/0000017f-e3f9-d9aa-afff-fbf93abc0000 [https://perma.cc/X87B-PW4W]. A criminal penalty might very well be invalidated by the Israeli Supreme Court, *see id.* (upholding the anti-boycott tort law while noting that it "does not impose any criminal prohibition on political expression"), but that is not a treaty limitation.

[70] UN Cybercrime Convention, *supra* note 4, art. 13.

higher salaries, economic damages, or transfer of land to be "without right." In other words, where a state—rightly or wrongly—does not recognize a human rights violation, any remedy could be interpreted as "without right" by adjudicating courts. The latitude of each state in defining offenses and interpreting treaty provisions is unsurprising, but civil liberties groups have criticized it for allowing states with weak human rights protections "to maintain their lower levels of protection."[71]

B. Structural Innovation

Beyond substantive ambition, the treaty drafting process was notable for its speed and involvement of numerous stakeholders, including non-state organizations and initial opponents. These structural features contributed to a heated dispute over the treaty's purpose that overlooked important details, such as jurisdiction. In other words, the process left little time or space to consider how various treaty provisions interacted.

From the beginning, the negotiations were set to be contentious. The initial 2019 General Assembly resolution creating the committee passed with a small margin of 79 in favor to 60 opposed, with 33 countries abstaining.[72] Before the vote, the only four representatives that spoke were the EU and the United States (in opposition) and China and Russia (in favor).[73] Finland's representative, speaking on behalf of the EU, warned that "launching the negotiation of a new international treaty on cybercrime without a broad consensus would be highly divisive" and lead to "lower standards."[74] For the United States, it would "undermine international cooperation to combat cybercrime."[75] Despite this initial opposition, after the General Assembly adopted the resolution many of these opponents became vice chairs of the Ad Hoc Committee, with a majority of the vice chairs representing countries that opposed the effort.[76]

---

[71] Rodriguez, *supra* note 2.
[72] U.N. GAOR, 74th Sess., 52nd plen. mtg. at 37, U.N. Doc. A/74/PV.52 (Dec. 19, 2019).
[73] *Id.* at 35-36.
[74] *Id.* at 35.
[75] *Id.* at 36.
[76] The vice chairs that opposed the General Assembly resolution were Japan,

The General Assembly set out an ambitious timeline for the committee, instructing it to provide a draft convention to the General Assembly's seventy-eighth session (September 2023 to September 2024).[77] The timeline of sessions was so compressed that the committee could not meet various procedural timelines mandated by UN rules.[78] The first substantive session occurred in February and March 2022, and the committee planned to conclude treaty negotiations in January and February 2024, with only five intervening negotiating sessions.[79] In other words, the planned timeline involved only seven negotiating sessions in less than two years.

Although treaty negotiation timelines vary drastically, and there is little empirical research on their length,[80] less than two years is a relatively short negotiation period, particularly for a treaty so broad in scope. One limited analysis of 41 agreements that did not have expiration dates found that they took 2.5 years to negotiate.[81] But major treaties often take far longer, with the negotiations leading to the World Trade Organization (the Uruguay Round) lasting nearly eight years and those culminating in the International Covenant on Civil and Political Rights taking 20 years.[82]

Speed has its advantages: negotiations are costly and can

Estonia, Poland, the Dominican Republic, Australia, Portugal, and the United States. *Id.* at 37; Arsi Dwinugra Firdausy (Rapporteur), *Report of the Ad Hoc Committee on Its Session on Organizational Matters Held on 24 February 2022*, at 3, U.N. Doc. A/AC.291/6 (Mar. 2, 2022) [hereinafter AHC Organizational Session Report] (listing vice chairs).

[77] G.A. Res. 75/282, ¶ 3 (June 1, 2021).

[78] AHC Schedule of Sessions, at 1 (Oct. 12, 2021), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/AHC_schedule_of_sessions_12_Oct_2021.pdf [https://perma.cc/A7GX-NNG6].

[79] *Id.* The first session was scheduled for late January 2022 but was briefly postponed due to the COVID-19 pandemic. AHC Organizational Session Report, *supra* note 76, at 1. Organizational sessions ultimately took place in May 2021 and February 2022. *Id.*

[80] *See* Nicole M. Simonelli, *Bargaining Over International Multilateral Agreements: The Duration of Negotiations*, 37 INT'L INTERACTIONS 147, 149, 166 (2011) (observing that "[l]ittle empirical work on how multilateral agreements are negotiated exists" and referring to the paper as "the first systematic empirical analysis on the duration of multilateral agreement negotiations").

[81] David H. Bearce, Cody D. Eldredge & Brandy J. Jolliff, *Do Finite Duration Provisions Reduce International Bargaining Delay?*, 69 INT'L ORG. 219, 224-25 (2015).

[82] *Id.* at 219.

burden smaller states.[83] However, speed is also risky. A rushed process will make it likelier that negotiators will overlook the implications of certain treaty provisions. All states, including large, developed nations, have limited resources, so they will only be able to focus their attention on the highest profile provisions. In other words, they must pick their battles, even if the actual text would normally elicit broader scrutiny.[84] Participants recognized the risk of overlooking critical elements, with one organization warning at the concluding session that "a concerted effort is needed to ensure proper scrutiny of proposals by both time-pressed delegates and external stakeholders."[85]

With countries focused on the more visible substantive criminalization provisions, the sprint to finish the cybercrime treaty overlooked jurisdictional provisions that deserved careful thought. Treaty proponents pushed an even faster timeline, with Russia initially proposing a negotiating period of only five sessions across fewer than 18 months.[86] It continued to advocate shortening the negotiations, suggesting in a joint submission with many of the autocratic co-sponsors that as few as four substantive sessions might be "reasonable."[87] Fewer sessions would have limited the ability of other states and stakeholders to scrutinize Russia's proposals. Many states recognized the significance of the cybercrime treaty and

---

[83] *See, e.g.*, Darren Brookbanks & Ana Paula Oliveira, *A Dream Deferred or a Near Miss?,* GLOB. INITIATIVE AGAINST TRANSNAT'L ORGANIZED CRIME (Feb. 15, 2024), https://globalinitiative.net/analysis/un-committee-postpones-decision-cybercrime-convention [https://perma.cc/V8TM-V5YC] ("Liechtenstein also noted that postponing the negotiations was a difficult decision for small states with limited resources, and that the renewed extension has affected its ability to continue to cover the process.").

[84] *See, e.g.*, *Global Cybercrime Treaty: A Delicate Balance Between Security and Human Rights*, *supra* note 21 (interviewing Ramat Jit Singh Chima, of Access Now, who stated that "our biggest fear sometimes is that there's too much agreement in the room on certain provisions; because of the accelerated pace of these negotiations, there is a desire to come to some sort of agreement, even if the language is not good, and even if it harms human rights").

[85] *Cyber Convention Check-in*, *supra* note 32.

[86] AHC Draft Resolution by Russia, ¶ 4, U.N. Doc. A/AC.291/L.3 (May 5, 2021). Russia subsequently suggested a sixth substantive session only "if necessary" in the eyes of the AHC. AHC Revised Draft Resolution by Russia, ¶ 5, U.N. Doc. A/AC.291/L.3/Rev.1 (May 10, 2021).

[87] Joint comment, at 3 (Feb. 9, 2021), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_9_February_2021.pdf [https://perma.cc/DMF5-CA28].

sought to ensure a careful, deliberative process. Early on, the United States expressed "concern[] with the very tight timelines," concern that was heightened "on issues as contentious as these."[88] But the ambitious negotiation timetable complicated these efforts.

The realities of navigating a negotiating process with hundreds of participants also made it difficult to sufficiently discuss and debate the consequences of each provision—and to step back to consider how the treaty provisions interacted, given that the text was continually changing up until the final agreement. The committee provided for the extensive involvement of nearly 200 different "non-governmental organizations, civil society organizations, academic institutions and [companies]."[89] These stakeholders could not vote but could participate in the committee's sessions as observers, submit written comments, and, "[d]epending on the time available," even make oral statements on substantive agenda items.[90] Outside of the main sessions, the committee organized a series of intersessional consultations to gather input from stakeholders.[91]

Many of the initial opponents and stakeholders challenged the more expansive proposals and advocated for a limited, rights protective instrument. For instance, Microsoft "urge[d] states to avoid using this negotiation as a catch-all framework to discuss other topics, such as extremism and terrorism" and warned against it "provid[ing] a pretext for non-democratic regimes to further endanger the free and open internet by closing off their digital

---

[88] U.S. Comment on "Implementation of Operative Paragraph 3 of General Assembly Resolution 74/247 and Next Steps" (Apr. 20, 2020) [hereinafter U.S. Comment], https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/USA.pdf [https://perma.cc/7M29-MLGK]. These states recognized that the scope and unlimited timeframe of this treaty casts "a long shadow of the future" and attempted to negotiate consistent with James Fearon's famous observation that such agreements "give states an incentive to bargain harder, delaying agreement in hopes of getting a better deal." James D. Fearon, *Bargaining, Enforcement, and International Cooperation*, 52 INT'L ORG 269, 270 (1998) (emphasis omitted).

[89] G.A. Res. 75/282, ¶ 9 (June 1, 2021). AHC Organizational Session Report, *supra* note 76, at 5-10 (listing organizations). In the bureaucratic parlance of the UN, these stakeholders were known as "multi-stakeholders" and included "interested global and regional intergovernmental organizations, including United Nations bodies, specialized agencies and funds." *Id.* at 11 n.1.

[90] AHC Organizational Session Report, *supra* note 76, at 11.

[91] *Id.*

borders."[92] But, while scrutinizing the treaty's provisions (a difficult task considering the speed of negotiations), negotiating states and outside stakeholders do not appear to have fully realized the jurisdictional problems in the treaty text. It is to these problems that the next Part turns.

II. Jurisdictional Innovation

Historically, jurisdictional limits constrained the reach of a vague or overbroad treaty. States would individually choose how to transpose a newly agreed norm into their domestic codes, and one state's expansive definition of a crime would not affect the behavior of citizens in another state. Indeed, national variation is a feature of international agreements, and most states and observers probably view the UN cybercrime treaty as following that tradition.[93]

However, the UN cybercrime convention erodes national variation—and thus sovereignty—by endorsing states' application of their expansive offenses to extraterritorial conduct. In particular, the jurisdictional provisions in the treaty represent a vast expansion of the traditionally limited jurisdiction based on harm against a state's nationals, known as passive personality jurisdiction. The treaty allows each state party to exercise extraterritorial jurisdiction over offenses committed against any nationals of that state party.[94] In certain cases, states are obligated to recognize and to provide law enforcement assistance to other states' assertions of long-arm jurisdiction, because the treaty endorses it.[95]

With passive personality jurisdiction, states could extend their overbroad application of cybercrime treaty offenses far beyond their own borders. For instance, recall the examples above of Article 13's

---

[92] Microsoft Submission to the First Session, Upcoming Negotiations on a Possible Cybercrime Convention, at 1-2 (Mar. 1, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Microsoft_position_-_first_session.pdf [https://perma.cc/VMP3-NE9H].

[93] *See, e.g.*, Rodriguez, *supra* note 2 ("The broad discretion granted to states under the UN cybercrime treaty is a deliberate design intended to secure agreement among countries with varying levels of human rights protections. This flexibility, in certain cases, allows states with strong protections to uphold them, but it also permits those with weaker standards to maintain their lower levels of protection.").

[94] UN Cybercrime Convention, *supra* note 4, art. 22(2)(a).

[95] *See infra* notes 161-162 and accompanying text.

deception prong.[96] Now imagine that an American company emails a press release to a U.S. news outlet, testifies at a virtual Congressional hearing, or texts a law enforcement agent about potential human rights violations it has discovered in its or a competitor's foreign supply chain. An investigation or decrease in consumer purchases ensues, causing a loss to owners of the subcontracted foreign company. Accused of making a false allegation and trying to aid American business, the American company faces criminal charges in the foreign country—even if it never had a presence there or enough ties to support traditional jurisdiction. A similar fact pattern could occur with the company employee (or any private individual) who made any such electronic communications. On vacation in a third country, she faces arrest and extradition under the UN cybercrime convention. While the United States could object to that specific application of the convention as violating international human rights law, the convention would limit Washington's basis for fighting the foreign country's prosecution of Americans for conduct outside of the foreign state's territory.

This Part proceeds in four sections. First, it takes a step back to explain the complicated landscape of criminal jurisdiction under international law and describe the rise of passive personality jurisdiction. Second, it outlines the jurisdictional provisions of the UN cybercrime treaty, including their provenance in the negotiations. Third, considering the existing jurisdictional landscape and the nature of the UN cybercrime treaty, this Part argues that inclusion of passive personality jurisdiction in the treaty represents a breathtaking expansion, with significant—and likely unintended—impacts on customary international law. Finally, it cautions against ignoring the longstanding dangers of this form of jurisdiction and argues that the cybercrime treaty demonstrates the risk of abuse.

A. The Rise of Passive Personality Jurisdiction

Under what circumstances can a state create criminal offenses, known as exercising prescriptive jurisdiction?[97] The conventional view is that jurisdiction over extraterritorial conduct must fall under

---

[96] *See supra* Section I.A.2.

[97] *See, e.g.*, RESTATEMENT (FOURTH), *supra* note 5, § 401 (discussing the categories of international criminal jurisdiction as prescriptive, adjudicative, and enforcement).

a specific basis recognized under international law to be valid—a rejection of the Permanent Court of International Justice's 1927 *S.S. Lotus* decision.[98] Historically, international law recognized only jurisdiction based on territory, active personality (conduct by a state's nationals), and universal offenses (such as piracy).[99] These jurisdictional limits reflected the absolute control that states traditionally had over activities within their borders—the classic conception of Westphalian sovereignty.[100]

But states began to recognize additional bases, some of which developed into customary international law.[101] The most notable is the protective principle, which allows jurisdiction when an offense affects the vital interests of a state; examples of permitted offenses are espionage and currency counterfeiting.[102] In some cases, protective jurisdiction is a specific application of the more general effects jurisdiction, which exists when an offense "has a substantial effect" within a state's territory.[103] The expansion of jurisdictional

---

[98] Curtis A. Bradley, *Universal Jurisdiction and U.S. Law*, U. CHI. LEGAL F. 323, 323 (2001). The famous *Lotus* case had held otherwise. *The Case of the S.S. "Lotus" (France v. Turkey)*, 1927 P.C.I.J. (ser. A) No. 10, ¶ 46 (Sept. 7) [hereinafter *Lotus*] ("It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law.").

[99] *See* RESTATEMENT (FOURTH), *supra* note 5, § 402 reporters' note 2 ("During its early years, the United States—consistent with the law of nations at the time—exercised jurisdiction to prescribe only on the basis of territory, active personality, and universal jurisdiction. See The Apollon, 22 U.S. (9 Wheat.) 362, 370 (1824) ('The laws of no nation can justly extend beyond its own territories, except so far as regards its own citizens.'); United States v. Klintock, 18 U.S. (5 Wheat.) 144, 152 (1820) (Pirates 'are proper objects for the penal code of all nations.').").

[100] *See, e.g.*, GALLANT, *supra* note 15, at 182 ("In the modern era, the power to make criminal law was traditionally said to be 'exclusive' in a state's territory."); *id.* at 309 (calling states' "authority to *control* and punish events occurring on their territory which they consider criminal . . . one chief marker of what it means to be a territorial sovereign" (emphasis added)).

[101] Arthur Lenhoff, *International Law and Rules on International Jurisdiction*, 50 CORNELL L. REV. 5, 12 (1964).

[102] RESTATEMENT (FOURTH), *supra* note 5, § 412.

[103] RESTATEMENT (FOURTH), *supra* note 5, § 409. *See Report of the International Law Commission to the General Assembly*, *supra* note 17, at 522 (saying the protective principle "may be viewed as a specific application of the objective territoriality principle or the effects doctrine"). Effects jurisdiction is sometimes

bases has been controversial, and states have disagreed about when certain jurisdictional principles apply.[104]

The most recent basis of jurisdiction recognized by the American Law Institute and the UN General Assembly's International Law Commission is passive personality jurisdiction, which refers to jurisdiction over any offenses committed against a state's nationals. Passive personality jurisdiction represents one of the broadest jurisdictional bases. Other bases often have inherent limitations—for instance, the protective principle is limited to vital interests—but passive personality jurisdiction has no minimum scale or severity.[105]

This type of jurisdiction "historically has been more controversial than jurisdiction based on territory or active personality," as the Fourth Restatement of Foreign Relations Law puts it.[106] Evolution of passive personality jurisdiction has been rapid. Only two editions earlier, in 1965, the Second Restatement had declared that "[a] state does not have jurisdiction to prescribe a rule of law attaching legal consequences to conduct of an alien outside its territory merely on the ground that the conduct affects

---

mistaken for a type of territorial jurisdiction, but it requires a "substantial effect within [the state's] territory" and does not require that an element of the offense occur within the territory. *Id.* at 521-22 (discussing this difference).

[104] *See, e.g.*, RESTATEMENT (FOURTH), *supra* note 5, § 408 cmt. c ("The exercise of territorial prescriptive jurisdiction is sometimes controversial when only part of the regulated conduct occurs on the state's territory."); *id.* § 409 cmt. b ("Effects jurisdiction has been controversial, but it has achieved a wider degree of acceptance over time, though some states continue to object to its exercise in particular cases.").

[105] *See, e.g.*, GALLANT, *supra* note 15, at 443 (2022) (rejecting the argument that passive personality jurisdiction is part of the protective principle, because protecting nationals from crime is not a vital state interest). The protective principle is itself open to significant jurisdictional creep. *See* Alyssa Resar, Note, *Self-Protection in World Society: Reformulating the Protective Principle in International Law*, 134 YALE L.J. 1824 (2025) (demonstrating how states have stretched the protective principle). However, there is an important difference between jurisdictional bases that have no inherent, principled limitations (passive personality jurisdiction) and those that have limitations that states nevertheless choose to ignore or stretch (such as the protective principle's vital-interest element and effects jurisdiction's substantiality requirement).

[106] RESTATEMENT (FOURTH), *supra* note 5, § 411 cmt. a; *see also Report of the International Law Commission to the General Assembly*, *supra* note 17, at 522 ("This principle of jurisdiction, which was contested by some States in the past, has gained greater acceptance in recent years." (citation omitted)).

one of its nationals."[107] Until recently, passive personality jurisdiction was largely limited to civil law states,[108] with many common law states opposing and persistently objecting to it.[109]

Even as passive personality jurisdiction has expanded, most states, including the United States, have limited it to violent or a few other serious crimes, notably terrorism.[110] In the Fourth Restatement's discussion of American exercise of passive personality jurisdiction, every one of the more than dozen statutes it lists as examples involves violence or terrorism.[111] Moreover, many of these statutes, although not all, may be better understood as exercises of the protective principle or other jurisdictional bases.[112]

France is a notable exception in not limiting its expansion. Since 1975, despite strong French opposition to passive personality jurisdiction fifty years earlier in the *S.S. Lotus* case[113] and a year earlier in a terrorism case,[114] the French Penal Code has provided

---

[107] RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW § 30(2) (AM. L. INST. 1965).

[108] GALLANT, *supra* note 15, at 441-42.

[109] Geoffrey R. Watson, *The Passive Personality Principle*, 28 TEX. INT'L L.J. 1, 2 (1993) ("Many countries, including the United States, have traditionally opposed this theory of jurisdiction."); GALLANT, *supra* note 15, at 455-56 (discussing persistent objection).

[110] Terrorism may seem particularly logical because terrorists often target victims on the basis of their nationality. John G. McCarthy, *The Passive Personality Principle and Its Use in Combatting International Terrorism*, 13 FORDHAM INT'L L.J. 298, 318 (1989) ("[I]ncreasingly, terrorist acts are committed on the basis of the victim's nationality."); *id.* at 322 (arguing that the requirement of direction because of nationality reconciles competing jurisdictional interests).

[111] RESTATEMENT (FOURTH), *supra* note 5, § 402 reporters' note 8.

[112] This is because terrorism seeks to coerce the state. *Compare id.* (listing the Hostage Taking Act, 18 U.S.C. § 1203, as an example of passive personality jurisdiction) *with* Watson, *supra* note 109, at 10 ("[T]he Hostage Taking Act may fit under the protective principle as well as the passive personality principle because the security of the state, not just individuals, is at stake."). *See also* 132 CONG. REC. 2356 (1986) (statement of Sen. Arlen Specter) (describing the Terrorist Prosecution Act, 18 U.S.C. § 2332, listed as an example of passive personality in the Restatement, as an exercise of the protective principle). *But see* McCarthy, *supra* note 110, at 311 n.87 (arguing that one statute cannot be understood as an exercise of the protective principle).

[113] Christopher L. Blakesley, *Jurisdiction as Legal Protection Against Terrorism*, 19 CONN. L. REV. 895, 938 (1987); *see Lotus*, *supra* note 98.

[114] *See* Cafritz & Tene, *supra* note 6, at 594 (describing France's refusal in 1974 to extradite the Palestinian terrorist Abu Daoud because Paris said the Israeli request was based on passive personality).

for jurisdiction over almost any crime committed against a French national.[115] However, the French approach to passive personality jurisdiction has drawn broad criticism and reflects a vision of the law that "is manifest imperialism," in the words of the French Justice Minister at the time.[116] It is not clear that France frequently enforces its statute, which would work absurd results. [117] Nonetheless, France was long considered a "uniquely broad" outlier in embracing such broad passive prersonality jurisdiction. [118] In 2006, the International Law Commission concluded that "most of the States, the United States included, give effect to [passive personality jurisdiction] *but limit its application to particular crimes*," particularly terrorism.[119]

France's outlier status may not last much longer. The limits to passive personality jurisdiction are crumbling far faster than is generally understood and, as Section II.C argues, could effectively collapse if states embrace the UN cybercrime treaty's jurisdictional provisions. During the past few decades, several international treaties have begun to allow passive personality jurisdiction. Many of these treaties involve terrorism or serious violence, demonstrating how the increasing international expansion of passive personality jurisdiction has generally still been narrow.[120]

But the treaties under the responsibility of the UN Office on Drugs and Crime illustrate how the limits confining passive personality jurisdiction to certain violent or terrorist acts have quietly faded. Two early UN drug treaties concluded in the 1960s and 1970s did not purport to make any jurisdictional statement, limiting their discussion of jurisdiction to a brief statement that their criminal provisions "shall be subject to the provisions of the criminal [domestic] law of the Party concerned on questions of

---

[115] Blakesley, *supra* note 113, at 938-39 (1987). The current version, covering misdemeanors and not only felonies punishable by at least five years in prison, dates to 1994. CODE PÉNAL [C. PÉN.] [Penal Code] art. 113-7 (Fr.).

[116] Cafritz & Tene, *supra* note 6, at 586, 588 n.14.

[117] *Id.* at 589-92 (describing how the law could be applied to a breathtaking array of common situations, such as the publishing of advertisements—in the United States—that compare competing products).

[118] *Id.* at 586.

[119] *Report of the International Law Commission to the General Assembly*, *supra* note 17, at 524 & n.23 (emphasis added).

[120] *See* GALLANT, *supra* note 15, at 458-60 (discussing passive personality jurisdiction in treaties).

jurisdiction."[121]

By 1988, however, the new UN drug trafficking convention included a broader, extended discussion of jurisdiction. The convention allowed states narrow opportunities to extend their jurisdictional reach to extraterritorial, non-violent crimes. Its second Article, placed only behind definitions, cautioned states to respect other states' sovereignty, "territorial integrity," and right to non-intervention, and it warned parties not to exercise overbroad jurisdiction.[122] Article 3 contained the criminal provisions, and Article 4 contained mandatory and discretionary jurisdictional provisions. The mandatory provisions contained traditional territorial jurisdiction and quasi-territorial jurisdiction over a state's aircraft and ships.[123] The discretionary jurisdictional provisions included active personality (nationality) and inchoate offenses (e.g., attempt, conspiracy) aimed at eventual commission *within* the state's territory.[124] The latter jurisdictional recognition is essentially effects jurisdiction based on intended effect.[125] It is also a narrow category. A typical example of a covered offense might be a foreign drug trafficker attempting to cross into the United States to sell narcotics domestically but who is stopped at a foreign airport. Under the discretionary jurisdictional provision, for instance, the United States could ask the foreign state to extradite the trafficker and exercise jurisdiction on the basis that the trafficker was attempting

---

[121] Single Convention on Narcotic Drugs (1961) as amended by the 1972 Protocol, art. 36(3), Aug. 8, 1972, 976 U.N.T.S. 105; Convention on Psychotropic Substances art. 22(4), Feb. 21, 1971, 1019 U.N.T.S. 175 (identical language, except "domestic" replaced "criminal").

[122] Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances art. 2(2), (3), Dec. 20, 1988, 1582 U.N.T.S. 95 ("A Party shall not undertake in the territory of another Party the exercise of jurisdiction and performance of functions which are exclusively reserved for the authorities of that other Party by its domestic law.").

[123] *Id.* art. 4(1)(a). The International Law Commission has treated jurisdiction over ships and aircraft as part of the nationality principle (active personality jurisdiction). *Report of the International Law Commission to the General Assembly*, *supra* note 17, at 522. Others view it as similar to territorial jurisdiction. *See, e.g.*, Harvard Draft, *supra* note 5, at 509.

[124] Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, *supra* note 122, art. 4(1)(b).

[125] *See* RESTATEMENT (FOURTH), *supra* note 5, § 409 cmt. c ("Some states also regulate conduct that was intended to have, but did not have, a substantial effect within their territory.").

to sell narcotics on U.S. territory—but simply had not completed that inchoate crime.

A decade later, jurisdictional breadth in UN crime treaties took another leap forward. In 2000, the General Assembly adopted a Convention Against Transnational Organized Crime (UNTOC). Its jurisdiction article was largely similar to that of the 1988 drug treaty, but there was a notable addition: signatories now agreed that they could exercise jurisdiction over any criminal offense under the Convention when the offense "is committed against a national of that State Party."[126] Shortly thereafter came the UN Convention Against Corruption (UNCAC), which similarly provides any state party express (but still discretionary) jurisdiction over offenses "committed against a national of that State Party."[127] These two twenty-first-century treaties are major exceptions to the usually carefully confined *substantive* violence-terrorism reach of the treaties that began to recognize passive personality jurisdiction.

B. Jurisdiction in the UN Cybercrime Treaty

The exception now threatens to swallow the rule. The cybercrime convention provides for mandatory jurisdiction over territory and quasi-territory (ships and aircraft) and discretionary jurisdiction based on active personality, passive personality, and the protective principle.[128] The treaty copies word-for-word the language in UNTOC and UNCAC authorizing passive personality jurisdiction where the offense "is committed against a national of that State Party."[129]

How did passive personality jurisdiction appear in the treaty? Negotiating documents suggest that states paid little attention to this brief phrase. Early in the process, the UNODC Secretariat prepared a survey of existing legal instruments and documents on countering cybercrime, as mandated by the General Assembly resolutions

---

[126] U.N. Convention Against Transnational Organized Crime art. 15(2)(a), Dec. 12, 2000, 2225 U.N.T.S. 209 [hereinafter UNTOC].

[127] U.N. Convention Against Corruption art. 42(2)(a), Dec. 9, 2003, 2349 U.N.T.S. 41 [hereinafter UNCAC]. *See* GALLANT, *supra* note 15, at 460 (discussing the significance of passive personality jurisdiction in this convention).

[128] UN Cybercrime Convention, *supra* note 4, art. 22(1), (2). For instance, jurisdiction over offenses "committed against the State Party," *id.* art. 22(2)(d), is an invocation of the protective principle.

[129] *Id.* art. 22(2)(a).

creating the committee.[130] The UNODC Secretariat included in this survey the corruption and organized crime treaties, even though it acknowledged that they do "not specifically concern cybercrime."[131] Within the jurisdiction survey, these were the only two documents that contained passive personality jurisdiction[132]—and neither related to cybercrime. Perhaps tellingly for its decision to go beyond the General Assembly's substantive mandate in assembling this survey,[133] the UN Office on Drugs and Crime serves as the secretariat for the cybercrime treaty—but also for UNCAC and UNTOC. While these two conventions, which also utilized the ad-hoc-committee model, may have provided a valuable procedural roadmap,[134] it is less clear that they should have received substantive deference. At least some participants recognized this, with the United States questioning the UNODC's reference to the drafting of UNCAC as a model, noting that the corruption convention "process was longer" and "was launched based on member state consensus, which is not the case here."[135]

Yet the lifting of jurisdictional provisions from previous UN treaties—and the jurisdictional provisions in general—received little scrutiny during the cybercrime convention drafting process. At an early organizational session, the committee chair proposed a convention structure consisting of a preamble and eight separate

---

[130] UNODC Secretariat, Overview of Existing Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes, U.N. Doc. A/AC.291/CRP.10 (Apr. 20, 2022).
[131] *Id.* at 4.
[132] *Id.* at 36.
[133] The General Assembly directed the committee to "tak[e] into full consideration existing international instruments and efforts at the national, regional and international levels *on combating the use of information and communications technologies for criminal purposes*, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime." G.A. Res. 74/247, at 3 (Dec. 27, 2019) (emphasis added).
[134] *See, e.g.*, AHC Rep. on First Session, at 8, U.N. Doc. A/AC.291/7 (Mar. 24, 2022) (developing a mode of work for the committee "[b]y taking into account the experiences of the Ad Hoc Committee on the Elaboration of a Convention against Transnational Organized Crime and the Ad Hoc Committee for the Negotiation of a Convention against Corruption").
[135] U.S. Comment, *supra* note 88.

chapters,[136] a structure that the committee approved.[137] The treaty nearly perfectly reflects that structure, except for the jurisdiction chapter, apparently considered an afterthought and added only later.[138] When the jurisdiction chapter was added, it was one of several that was negotiated in "informal consultations," which were closed, member-state-only sessions on the margins of the plenary sessions.[139] And its content changed little over the course of negotiations.[140]

Several member states nevertheless raised jurisdictional issues in their early submissions, often advocating for broad extraterritorial jurisdiction or focusing on the difficulties of jurisdiction in cyberspace and the associated need for "mechanisms for obtaining electronic evidence" that may be stored in multiple jurisdictions.[141] For instance, India's remarks at the first substantive session noted that the "increasingly complex exercise to ascertain the jurisdiction of the data on the basis of existing classical territorial models" has

---

[136] UNODC Secretariat, Proposal on the Structure of the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, U.N. Doc. A/AC.291/CRP.7 (Feb. 24, 2022).

[137] AHC Rep. on First Session, *supra* note 134, at 4, 7.

[138] The treaty has nine chapters: the eight originally proposed, plus the jurisdiction chapter. UN Cybercrime Convention, *supra* note 4**.**

[139] *See* AHC, Fourth Session Consolidated Negotiating Document, at 31 (Jan. 21, 2023), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf [https://perma.cc/MQ47-5BYG].

[140] There are only a half dozen changes in the jurisdiction chapter between the consolidated negotiating draft in January 2023 and the convention text approved in December 2024, with the few substantive ones slightly reducing the scope of permissible jurisdiction. These changes eliminated harm *against* a legal person, such as a company, as a basis for passive personality jurisdiction; eliminated harm *by* a legal person as a basis for active personality jurisdiction; and reduced jurisdiction from convention offenses committed outside of a state's territory "with a view to the commission of an offence established in accordance with this Convention within its territory" to inchoate/accomplice convention offenses committed outside of a state's territory "with a view to the commission of [certain specified money laundering, property transfer, or concealment offenses] within its territory." *Compare id.* art. 40(2)(a), (b), (c) *with* UN Cybercrime Convention, *supra* note 4, art. 22(2)(a), (b), (c).

[141] Agnieszka Gryszczyńska, Polish National Public Prosecutor's Office, Statement at the First Session, at 3-4 (Mar. 2, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Poland_item_4.pdf [https://perma.cc/TKF7-T6A7].

led to "enormous delays" in mutual legal assistance in cybercrime cases.[142] The Tallinn Manual, a noted academic treatise on international law in cyberspace, has raised similar concerns.[143]

In light of the potential for jurisdictional conflicts, China advocated for broad effects jurisdiction. "Jurisdiction," it wrote, "should be based on a 'true and sufficient' link with the criminal activity in question, *giving priority to the place where the consequences of the criminal activity occur,* the place where the crime was committed and the place where the person or group that committed the crime is located."[144] But even as China advanced this effects based jurisdiction, it advocated a reduced conception of territorial jurisdiction in cyberspace, rejecting data passage as a sufficient basis for jurisdiction.[145]

Egypt's rough convention draft included a more detailed description of when states would be required to exercise jurisdiction. Beyond the traditional territorial and quasi-territorial (flag ship and registered aircraft) jurisdictional bases, it suggested what was essentially universal jurisdiction for *any* transnational offenses involving an organized criminal group under the convention.[146]

---

[142] Muanpuii Saiawi, Indian Joint Secretary (Cyber Diplomacy), Remarks at the First Session, ¶¶ 3, 5 (Feb. 28, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/India.pdf [https://perma.cc/7GLS-A2XF]; *see also* Brazil, Statement at the First Session, at 2, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Brazil_6.pdf [https://perma.cc/7QG3-J26L] (raising "the issue of possible exceptions to territoriality").

[143] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 54 (Michael N. Schmitt, ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0] ("[C]yber activities pose a number of challenges to the rational and equitable exercise of jurisdiction. This is due, *inter alia*, to their pervasiveness, the fact that they can originate from anywhere on the globe, the relative speed and ease of crossing a State's borders in cyberspace, and the possibility of generating effects in multiple States.").

[144] First Session Compilation of Views, *supra* note 42, at 16 (emphasis added).

[145] *Id.* Beijing may have been been seeking to head off American assertions of territorial jurisdiction based on data flows, given that most internet traffic passes through the United States. *See* Dora Mekouar, *Here's Where the Internet Actually Lives*, VOA (Feb. 17, 2020), https://www.voanews.com/a/usa_all-about-america_heres-where-internet-actually-lives/6184090.html [https://perma.cc/4VNP-K2TY] (stating that 70% of internet traffic passes through Ashburn, Virginia).

[146] First Session Compilation of Views, *supra* note 42, at 23.

Transnational offenses were defined broadly to include any that have "serious consequences in another country."[147] But even Egypt did not endorse unrestricted passive personality jurisdiction, despite including mandatory jurisdiction under territorial, quasi-territorial, active personality, and protective principle bases.[148] In its remarks, Egypt argued that territorial jurisdiction was insufficient and suggested this gap could be filled with investigatory provisions rather than jurisdictional expansion.[149]

As for the European Union, the brief reference to jurisdiction in its submission noted only that it "should be modelled on the approach set out in existing legal instruments, such as in article 15 of the Organized Crime Convention."[150] As discussed, that article includes express, discretionary passive personality jurisdiction.[151] The EU's submission may have reflected a genuine desire for expansive jurisdiction, but it was more likely an effort to focus the drafting process on existing, acceptable language. Indeed, the prior paragraph of the EU's submission emphasized UNTOC as a fallback model for language on punishment,[152] and the EU repeatedly stressed the value of looking at existing instruments, mentioning the Budapest Convention and the UN corruption and organized crime conventions in the same breath.[153]

Russia made by far the longest submission, sending in a forty-page complete draft of the convention.[154] Its jurisdiction element was the most expansive of any of the proposals, endorsing an

---

[147] *Id.*
[148] *Id.* at 28.
[149] Permanent Rep. of Egypt to the U.N., Remarks at the First Session, at 4 (Feb. 28, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Egypt.pdf [https://perma.cc/XF79-LZQK] ("The scope of the convention should include provisions to ensure the establishment of legal jurisdiction not only over the territory of each state party but also provisions to allow for investigations of trans-national cybercrimes that may take place in different territories.").
[150] First Session Compilation of Views, *supra* note 42, at 35.
[151] *See supra* text accompanying note 126.
[152] First Session Compilation of Views, *supra* note 42, at 35.
[153] Ambassador Silvio Gonzato, Statement on Behalf of the EU and Its Member States, at 4 (Feb. 28, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/EU.pdf [https://perma.cc/KV4V-SAWD].
[154] Initial Russian Draft Convention, *supra* note 13.

unprecedented version of passive personality jurisdiction. Under its proposal, a state would be able to exercise jurisdiction over offenses committed against its nationals,[155] the traditional extent of passive personality jurisdiction.[156] But it would also be able to exercise jurisdiction over offenses committed against any legal entities (such as companies) "established or having a permanent representation in its territory" or against state or government facilities.[157] For good measure, Russia added a provision providing broad effects jurisdiction—but devoid of the traditional substantiality requirement.[158]

In a particularly bold move, Russia also sought to make passive personality jurisdiction mandatory. The suggestion was hidden in a cross-reference and conditional language:

> Each State party in whose territory an alleged perpetrator is present and which does not extradite such person shall, in cases provided for in [the provisions outlining when states may exercise jurisdiction], without any exception and regardless of whether the offence was committed in the territory of that State party, submit the case without further delay to its competent authorities for the purpose of legal prosecution in accordance with the law of that State.[159]

Untangled, this language meant Russia's proposal would mandate that a state either fully exercise passive personality jurisdiction over any "alleged perpetrators" or extradite anyone over whom it could exercise such jurisdiction under the convention. The

---

[155] *Id.* art. 39(2)(a).

[156] *See* GALLANT, *supra* note 15, at 448 (noting only "[a] few states treat corporations or other artificial persons . . . as victims who may provide a ground for passive personality jurisdiction").

[157] Initial Russian Draft Convention, *supra* note 13, art. 39(2). The latter seems to be a hybrid application of passive personality jurisdiction and the protective principle, stretching both beyond their traditional limits.

[158] *Id.* art. 39(2)(d) (providing for jurisdiction when an offense is "committed wholly or partly outside the territory of that State party but its effects in the territory of that State party constitute an offence or result in the commission of an offence"). *Cf.* RESTATEMENT (FOURTH), *supra* note 5, § 402 reporters' note 6 (listing American statutes, which generally expressly limit jurisdiction to extraterritorial conduct that has a "substantial effect within the United States").

[159] Initial Russian Draft Convention, *supra* note 13, art. 39(4).

phrasing around not extraditing an *alleged* perpetrator makes clear that a foreign state's allegation, even a spurious one, would have activated this provision. In case a state might try to find some way out of this language, the Russian proposal added that such prosecution "shall" occur "without any exception." The language is so broad that it would have even removed the traditional powers of prosecutorial discretion. This provision would have allowed Russia—or another autocracy—to accuse a political dissident or foreign critic of using a computer to commit a crime that harmed a company or person and then invoke a legal obligation that any convention signatory extradite or try that dissident.

States participating in the negotiations appeared to have little interest in such a sweeping provision, which was more expansive than prior treaties' treatment of passive personality jurisdiction as a discretionary basis for jurisdiction.[160] But under the treaty, states have to provide "the widest measure of" legal assistance and electronic interception in aid of other states' investigations premised on passive personality jurisdiction.[161] Although states could refuse legal assistance on the grounds of a lack of dual criminality (i.e., that the conduct be criminalized in both the country exercising jurisdiction and the country whose assistance is requested), this is not required.[162] Thus, this provision does not protect their nationals from being surveilled, investigated, and extradited by foreign states that can choose under the treaty to not apply dual criminality and other protections. Nor does it allow states to refuse legal assistance on the basis that they disagree with the assertion of passive personality jurisdiction.

C. Jurisdictional Expansion

Recognition of passive personality jurisdiction in the cybercrime convention represents a significant expansion beyond terrorism and violence. It legitimizes the use of passive personality jurisdiction

---

[160] GALLANT, *supra* note 15, at 458.

[161] UN Cybercrime Convention, *supra* note 4, art. 40(1) ("States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences established in accordance with this Convention, and for the purposes of the collection of evidence in electronic form of offences established in accordance with this Convention, as well as of serious crimes."); *id.* arts. 45(1), 46 ("States Parties shall endeavour to provide [assistance with metadata and content interception.]").

[162] *Id.* art. 40(8).

and could remove most limits on its use under international law—even for offenses far outside of the treaty's scope. Individual states have increasingly asserted passive personality jurisdiction, as have two recent UN treaties. But the authorization of such jurisdiction here may confer greater legitimacy benefits than past examples, cementing broad recognition of passive personality jurisdiction rather than granting it ad hoc and in narrow circumstances. Regardless of the number of signatories, a UN treaty "is still a massive signaling force," as one digital rights organization leader put it while describing the impact of the convention's substantive provisions.[163]

More importantly, depending on the number of states that accede to the treaty, unlimited passive personality jurisdiction here may move the jurisdictional base toward becoming customary international law. Most states will likely ratify the UN cybercrime treaty, given that the previous UN criminal justice treaties on corruption and transnational organized crime "enjoy[ed] near universal ratification."[164] And any state that ratifies the cybercrime treaty would effectively be stating that the exercise of passive personality jurisdiction is permissible, even if that state does not itself exercise such jurisdiction. That is significant, because states' understanding of the legality of a practice is a crucial part of customary international law.[165]

It might also be difficult for states to claim that they were endorsing passive personality jurisdiction under only limited circumstances (unless they made a reservation in joining the

---

[163] Iyengar, Gramer & Rathi, *supra* note 39 (quoting Raman Jit Singh Chima, Asia Policy Director and Senior International Counsel, Access Now).

[164] Joint Statement on the Forum for Negotiations and Decision-Making Process Towards the Implementation of United Nations General Assembly Resolution 74/247 on "Countering the use of information and communications technologies for criminal purposes" (Dec. 14, 2020), https://css.unodc.org/pdf/2020/Joint_statement_40_delegations_December_2020.pdf [https://perma.cc/MKX7-X7MN].

[165] *See, e.g.*, Statute of the International Court of Justice, art. 38(1)(b) (referencing, as a source for interpretation, "international custom, as evidence of a general practice accepted as law"); Int'l L. Comm'n, *Draft Conclusions on the Identification of Customary International Law*, G.A. Res. 73/203, Conclusion 11(1) (Jan. 11, 2019) ("A rule set forth in a treaty may reflect a rule of customary international law if it is established that the treaty rule . . . has given rise to a general practice that is accepted as law (*opinio juris*), thus generating a new rule of customary international law.").

treaty),[166] as they could plausibly argue before the UN cybercrime treaty. Unlike past uses of passive personality jurisdiction, its inclusion here is freed from substantive limits (such as terrorism or violence) and functional limits (as in the corruption and organized crime treaties).

Indeed, even the corruption and organized crime treaties endorse passive personality jurisdiction far more narrowly than the UN cybercrime convention does. The transnational organized crime treaty covers participation in an *organized* criminal group, which has many limiting elements (structure, coordination, and purpose of committing a serious crime with the goal of obtaining financial or material benefits).[167] Most crimes are excluded simply by virtue of being individual. The corruption treaty is similarly limited. Most of the UNCAC offenses involve public officials, meaning offenses committed against a state's nationals would most often involve attempted bribes of that state's officials, with passive personality jurisdiction seemingly making only the narrow expansion to bribes of these officials that occur abroad.[168] In this sense, formal application of passive personality jurisdiction in the corruption treaty will almost always be more like an application of a broad protective principle that seeks to protect a government's official functions from the destructive effect of official bribery.

After signing these two treaties, states could plausibly claim that they still objected to most exercises of passive personality jurisdiction. One scholar of international criminal jurisdiction recently reviewed the sweep of passive personality jurisdiction and concluded that "the United States and other common law countries adopting such [passive personality jurisdiction] statutes have abandoned their objection to passive personality jurisdiction with respect to terrorist crimes . . . not . . . the persistent objection as to other types of crime."[169] But accepting a cybercrime treaty that authorizes far broader passive personality jurisdiction could void this persistent objector status, just as it has in the protective principle context. There, the UN Convention Against Corruption's expansion

---

[166] *See infra* Section III.C.

[167] UNTOC, *supra* note 126, art. 2(a) (defining "[o]rganized criminal group"), art. 5 (requiring criminalization of participation in such).

[168] There is only one mandatory, substantive UNCAC offense that implicates only the private sector: money laundering. UNCAC, *supra* note 127, art. 23.

[169] GALLANT, *supra* note 15, at 456.

of the protective principle means that "[t]here can be very little question that this practice is lawful among parties to the . . . treaty."[170] That treaty has 191 parties, reflecting nearly universal adoption.[171]

Moreover, the shift would be particularly significant given the open-ended, flexible nature of the crimes that the UN cybercrime convention covers. This would make passive personality jurisdiction for cybercrime far more vulnerable to abuse, as Section II.D, *infra*, discusses. Only the UN treaty envisions passive personality jurisdiction for a broad range of cybercrimes. Tellingly, the Budapest Convention on Cybercrime contains no endorsement of passive personality jurisdiction over cybercrimes.[172] Nor does the Arab League's Convention on Combating Information Technology Offences.[173] Even commentators that suggested passive personality jurisdiction could be suitable for cybercrimes did so only for terrorism related crimes.[174]

Before the UN treaty, an international instrument had never included unrestricted passive personality jurisdiction for cybercrime. If the UN treaty gains widespread adherence, it will be the last nail in the coffin of limited passive personality jurisdiction. That would open the door to foreign states asserting passive personality jurisdiction over a wide variety of domestic offenses—

---

[170] GALLANT, *supra* note 15, at 439.

[171] United Nations Treaty Collection Chapter XVIII: Penal Matters, 14. United Nations Convention against Corruption, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-14&chapter=18 [https://perma.cc/8HYA-VAP2].

[172] Budapest Convention on Cybercrime, *supra* note 23, art. 22. That Convention does not *prohibit* states from exercising passive personality jurisdiction; as with most international treaties, it avoids altogether any major statement on jurisdictional debates. "This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law," it declares. *Id.* art. 22(4).

[173] Arab Convention on Combating Information Technology Offences art. 30 (2010).

[174] In 2017, the Tallinn Manual's experts suggested that passive personality jurisdiction could serve as the basis for cybercrimes only within "the limited range of acts in respect of which the passive personality principle has been recognized." TALLINN MANUAL 2.0, *supra* note 143, at 65. Its single example of "arguably" covered conduct was "online recruitment abroad of foreign nationals by organisations that conduct terrorist acts against nationals of that State." *Id.* Complicating the analysis, the Tallinn Manual couched this in terms of reasonability terms. *Id. See infra* Section II.D (discussing the reasonability issue).

including broad speech offenses like those that Russia proposed—and justifying their application of offenses to foreigners abroad as endorsed by the treaty's acceptance of passive personality jurisdiction generally.

D. Longstanding Dangers of Passive Personality Jurisdiction Persist

Passive personality jurisdiction has multiple vices, all of which are exacerbated when it is expanded to ordinary, sometimes minor offenses. First, it intrudes upon the sovereignty of a state to regulate the conduct of those within its territory.[175] The United States and many other states "consider passive personality jurisdiction to be more intrusive than nationality or territorial jurisdiction, even if exercised when the conduct is criminal in the state in which the crime occurred." [176] This is because a fundamental part of sovereignty is the ability to exercise prosecutorial discretion within sovereign territory, as well as to set the standard punishment and to waive punishment.[177] Intruding on that sovereignty is particularly questionable when a state is undertaking it to repress ordinary crimes, rather than in the exceptional national security context of terrorism.

Contrary to what some scholars have suggested, [178] passive personality intrudes on a state's sovereignty even when the state where the conduct occurred (or whose national committed the crime) does not prosecute. A state may decide not to punish conduct

---

[175] *See* Watson, *supra* note 109, at 15-21 (discussing the intrusion on sovereignty and arguing that, if limited by dual criminality, it is no more intrusive than nationality or territorial jurisdiction).

[176] Watson, *supra* note 109, at 16 (citing Letter from Janet G. Mullins, Assistant Sec'y of State for Legis. Affs., Dec. 26, 1989, *reprinted in* 137 CONG. REC. 8676-77 (1991)).

[177] *See* GALLANT, *supra* note 100. The pardon power, in monarchical countries referred to as the prerogative of mercy, is a fundamentally sovereign power. *See, e.g.*, 1 FRANCIS LIEBER, CIVIL LIBERTY AND SELF-GOVERNMENT 392 (1st ed. 1853) ("[I]t is clear that the last and highest power, the real sovereign (not only the supreme) power, must include the power of pardoning. . . . [T]he monarch had the pardoning power not because he is the chief executive, but because he was considered the sovereign.").

[178] *See* Watson, *supra* note 109, at 21 ("In principle, however, there is no reasonable basis for a state that does not plan to prosecute an offender to object to another state's exercise of passive personality jurisdiction over that offender. Such an exercise of jurisdiction does not 'intrude' on any state's sovereignty . . . .").

for any number of reasons, including to protect other conduct. This is one rationale for First Amendment speech protections. To avoid chilling some speech that is valuable to society, a state may refrain from punishing even criminalizable speech.[179] Regardless of whether any specific non-prosecution is desirable, enforcement discretion is at the heart of sovereignty.[180] To the extent the international legal system has begun to question the extent of traditional notions of sovereignty, it has been to elevate the importance of domestically binding human rights norms—not to allow states to over-enforce their criminal laws.[181]

Second, passive personality jurisdiction poses a due process concern, as citizens of one state may not be familiar—or reasonably be expected to be familiar—with "the substantive criminal law of the victim's home state."[182] Even if they were or could be familiar with foreign laws, passive personality jurisdiction subjects them "not merely to a dual, but an indefinite responsibility," as the U.S. State Department observed in the Cutting Case, discussed in depth below.[183]

---

[179] *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 341 (1974) ("The First Amendment requires that we protect some falsehood in order to protect speech that matters.").

[180] *See, e.g.*, JOHN BASSETT MOORE, REPORT ON EXTRATERRITORIAL CRIME AND THE CUTTING CASE 125 (1887) ("When a man in his own country violates its laws, he is answerable for his misconduct to those laws alone; and it is his right to be tried under them and in accordance with the methods of procedure they prescribe."). Certainly, as with any area of sovereignty, states may be able to voluntarily consent to its limitation. The *aut dedere aud judicare* ("extradite or prosecute") principle represents one such limitation, but only with respect to certain crimes—and might only bind those who have accepted it. *See* Zdzislaw Galicki (Special Rapporteur of the International Law Commission), *Fourth Rep. on the Obligation to Extradite or Prosecute ("aut dedere aut judicare")* ¶ 87, U.N. Doc. A/CN.4/648 (May 31, 2011) (noting only certain grave international crimes, not ordinary crimes, "may be considered as giving a sufficient customary basis for the application of the obligation"); *id.* ¶ 95 (listing a few potential crimes). That universality requirement avoids the danger of a bilateral requirement without multilateral endorsement.

[181] *See, e.g.*, Prosecutor v Tadić, Case No. IT-94-1-AR72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction ¶ 97 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995), www.icty.org/x/cases/tadic/acdec/en/51002.htm [https://perma.cc/66P3-NQQ2] ("A State-sovereignty-oriented approach has been gradually supplanted by a human-being-oriented approach.").

[182] Watson, *supra* note 109, at 14 (discussing the fairness/abuse concerns).

[183] Watson, *supra* note 109, at 22 (quoting MOORE, *supra* note 180, at 125).

Scholars have long recognized these two issues.[184] But a third issue is often overlooked or downplayed: passive personality jurisdiction is ripe for systematic abuse. Traditional due process concerns focused on states crafting laws that happened to reach foreigners, whereas systematic abuse highlights the risk that targeting foreigners through passive personality jurisdiction will *motivate* states' adoption or enforcement of substantive laws.[185] Without a limitation of passive personality to terrorism and violence, states may criminalize ordinary conduct and abuse their jurisdiction to target foreigners.

Although it involved no computers, the nineteenth century Cutting Case—an early, famous instance of American opposition to passive personality jurisdiction—demonstrates the dangers of passive personality jurisdiction, particularly in cases involving speech. The case involved an American newspaper editor, A.K. Cutting, who published critiques of the character and good faith of Emigidio Medina, a Mexican on the verge of starting a rival newspaper in the same town.[186] The publications appeared in the Mexican press, after which Cutting reached a settlement with Medina, and in the *El Paso Herald*, where he called Medina a coward and contemptible.[187] Upon his return to Mexico, Cutting was arrested for libel, refused bail, and sentenced "to a year's imprisonment at hard labor" for the Texas publication.[188] The prosecution relied on a Mexican statute asserting jurisdiction over crimes committed against Mexicans anywhere in the world.[189]

Back in Washington, Secretary of State Thomas Francis Bayard cabled the American minister in Mexico City to reject the Mexican assertion of jurisdiction over Americans publishing newspapers in

---

[184] *See, e.g.*, Watson, *supra* note 109, at 14 (describing these as two of the three reasons why "[t]he passive personality principle has traditionally been criticized," with the third reason being impracticality).

[185] *See* MOORE, *supra* note 180, at 6 (Secretary of State framing ill-treatment of Cutting as a basis for objecting to his prosecution but not suggesting that Mexico was targeting its laws at Americans); Watson, *supra* note 109, at 25 (referencing a "fear of corrupt foreign prosecutions" but arguing that "passive personality jurisdiction will not make it appreciably easier for states to violate the human rights of foreign nationals").

[186] JOHN BASSETT MOORE, REPORT ON EXTRATERRITORIAL CRIME AND THE CUTTING CASE 3-4 (1887).

[187] *Id.* at 4.

[188] *Id.* at 4-5, 9.

[189] *Id.* at 7.

America and to sound the alarm over its consequences.[190] "If Mr. Cutting can be tried and imprisoned in Mexico for publishing in the United States a criticism on a Mexican business transaction in which he was concerned," Bayard warned, "there is not an editor or publisher of a newspaper in the United States who could not, were he found in Mexico, be subjected to like indignities and injuries on the same ground." [191] Secretary Bayard's complaint raised sovereignty concerns, but it went further, noting the denial of procedural rights that accompanied Cutting's imprisonment and trial.[192]

In a report President Grover Cleveland transmitted to Congress, Secretary Bayard added that the case "affects the underlying principles of security to personal liberty and freedom of speech or expression."[193] Part of the problem was that the offense, if it were one in the U.S., would only be a misdemeanor, but Mexico treated it as a serious felony.[194] "The safety of our citizens and all others lawfully within our jurisdiction would be greatly impaired, if not wholly destroyed," Bayard explained, "by admitting the power of a foreign state to define offenses and apply penalties to acts committed within the jurisdiction of the United States."[195]

This case illustrates the dangers of passive personality jurisdiction, including how those dangers often occur together. When Mexico defined an expansive speech offense and pursued U.S. nationals for conduct in the United States, Mexico intruded on American sovereignty, created secondary procedural justice problems for U.S. nationals, and substantively abused its laws to pursue minor conduct.

If the broad speech offenses had been retained in the UN cybercrime treaty, the Cutting Case could have easily recurred with online speech. Even under the treaty's more limited form, states can use the Article 13 deception prong to reach publications like that of

---

[190] *Id.* at 6.
[191] *Id.*
[192] *Id.* (describing the lack of counsel, interpretation, bail, cross-examination, and sanitary conditions).
[193] *Id.* at 7.
[194] *Id.*
[195] *Id.*

Cutting.[196] States can use passive personality jurisdiction to target foreign dissidents and critics because states are largely free to craft broader offenses. Consider an American journalist in the United States or EU who searches on a U.S. website, discovers a misconfigured database exposing Russian citizens' personal data, and reports on this leak. She could easily be charged with illegal access, and passive personality jurisdiction would suddenly confer jurisdiction on Russia.[197]

These are real threats, as states routinely use their cybercrime laws to target dissidents, journalists, and speech. One example is Pakistan's 2021 arrest of journalists for a variety of cybercrimes.[198] The journalists' conduct seemingly entailed only political commentary (what law enforcement called "scandalous content"), but their arrest was for "alleged electronic forgery; making, obtaining, or supplying a device for an offense; and the transmission of malicious code."[199] All of those offenses could fall under the convention's provisions,[200] and passive personality jurisdiction would facilitate states like Pakistan targeting foreigners for similar overseas criticism.

States made statements in the negotiations that signaled they will leverage the treaty's passive personality provisions. For instance, to a proposal that states could provide mutual legal assistance even when the conduct would not be a crime under the requested party's law, China proposed adding language that those mutual assistance

---

[196] In Cutting's case, had the communication been electronic and the cybercrime treaty in effect, Mexico might have argued that calling someone a "fraud," *id.* at 12 n.1, was false, caused others to stop buying Medina's newspapers, and showed an intent for Cutting to gain business share at Medina's expense (given the context of business competition).

[197] The risk to journalism is not confined to autocracies. *See* Jack Suntrup & Kurt Erickson, *Parson Issues Legal Threat Against Post-Dispatch After Database Flaws Exposed*, ST. LOUIS POST-DISPATCH (Oct. 15, 2021), https://www.stltoday.com/news/local/education/parson-issues-legal-threat-against-post-dispatch-after-database-flaws-exposed/article_93f4d7d6-f792-5b1b-b556-00b5cac23af3.html [https://perma.cc/4R3K-4KDL].

[198] *Pakistan Authorities Detain, Investigate Journalists Amir Mir and Imran Shafqat*, COMM. TO PROJECT JOURNALISTS (Aug. 10, 2021), https://cpj.org/2021/08/pakistan-authorities-detain-investigate-journalists-amir-mir-and-imran-shafqat [https://perma.cc/3SBP-DN7F].

[199] *Id.*

[200] *See* UN Cybercrime Convention, *supra* note 4, arts. 10 (interference), 11 (devices), 12 (forgery).

requests should receive "special consideration . . . when the conduct affects only nationals of the requesting State Party."[201] This proposal suggests that China will use the treaty to target its nationals abroad for conduct that is not criminalized in those foreign states.[202] Instead of inking bilateral extradition deals for fleeing Uyghurs or foreign critics of its crackdown in Hong Kong,[203] China will then be able to combine its continuing overcriminalization[204] with this treaty's endorsement of passive personality jurisdiction to target dissidents and critics around the world. For offenses outside of the cybercrime treaty, states might still extradite based on the newfound legitimacy of passive personality jurisdiction.[205]

Some experts optimistically rely on the goodwill of countries as a constraint on this jurisdictional expansion. The Tallinn Manual understatedly writes that passive personality jurisdiction "was previously considered somewhat controversial" but "has become a generally accepted basis for the exercise of extraterritorial prescriptive jurisdiction in relation to specific types of offences and subject to a number of considerations. These include due regard for the sovereignty of other States, the relationship between those States and their nationals, and due process."[206] The experts say that these considerations translate into a reasonability analysis.[207] But unlike their discussion of other jurisdictional bases, their discussion of passive personality jurisdiction includes no citations to support their

---

[201] Fifth Session Consolidated Negotiating Document, at 21 (Apr. 21, 2023), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf [https://perma.cc/RV53-BAKW].

[202] *But see* GALLANT, *supra* note 15, at 454 n.66 (saying China's statute requires dual criminality if the *minimum* punishment exceeds three years) (citing China Criminal Law (1997) art. 8).

[203] NATE SCHENKKAN & ISABEL LINZER, FREEDOM HOUSE, OUT OF SIGHT, NOT OUT OF REACH 19-20 (2021); Daren Butler, *Looming China Extradition Deal Worries Uighurs in Turkey*, REUTERS (Mar. 8, 2021), https://www.reuters.com/article/idUSKBN2B01E1 [https://perma.cc/32TC-LAZ4].

[204] *See, e.g.*, Hsia Hsiao-hwa, *'Hurting the Feelings of the Chinese People' Could Be Punished by Jail Time*, RADIO FREE ASIA (Sept. 7, 2023), https://www.rfa.org/english/news/china/china-hurt-feelings-09072023123314.html [https://perma.cc/D3BK-QYT3].

[205] At least one scholar has suggested that under a uniform system of passive personality jurisdiction, "countries should be willing to extradite offenders to states asserting such jurisdiction." McCarthy, *supra* note 110, at 320.

[206] TALLINN MANUAL 2.0, *supra* note 143, at 64-65.

[207] *Id.* at 65.

claims.

Indeed, the American Law Institute previously thought that a reasonability analysis was required but has since reversed itself, concluding that "state practice does not support a requirement of case-by-case balancing to establish reasonableness as a matter of international law." [208] Even if international law required a reasonability analysis, it would not place practical limitations on the exercise of jurisdiction.[209] States could assert it subjectively, and those most likely to abuse this jurisdiction are also likely to have courts that will defer to their governments' assessments of reasonableness.

Moreover, no reasonableness limitation exists in the convention, which only imposes the vague requirement that passive personality jurisdiction be "consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States."[210] Existing conventions that have incorporated passive personality jurisdiction do not appear to subject it to due process and reasonability requirements.

In sum, the due process and sovereignty concerns that attach to passive personality jurisdiction have not only persisted but are heightened in the cybercrime context. This treaty leaves states free to define broad crimes and then leverage the treaty's provisions for extradition and legal assistance to target foreign nationals abroad. The treaty did ultimately include human rights provisions, which require compliance with international human rights law, but they offer no independent enforcement mechanism, instead relying on existing (or nonexistent) national safeguards.[211]

Treaty-based protections are an insufficient substitute for persistent objection because they are voluntary, even when treaties do include them. Historically, "many potentially abusive [protective principle] prosecutions fit into categories of crimes for which extradition is not usually granted . . . , such as political offenses, military offenses, or fiscal offenses" or where "the double

---

[208] RESTATEMENT (FOURTH), *supra* note 5, § 407 reporters' note 3.

[209] *See, e.g.*, Susan Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH-TECHNOLOGY L. 1, 42 (2004) ("[T]he reasonableness standard is flexible, and so, national courts may interpret it as they see fit . . . .").

[210] UN Cybercrime Convention, *supra* note 4, art. 5(1).

[211] Rodriguez, *supra* note 2.

criminality doctrine . . . blocks extradition."[212] But the cybercrime convention states that states *cannot* refuse extradition solely on the grounds that an offense is fiscal.[213] While the treaty's provisions allow states to refuse extradition for political offenses or offenses that are not punishable under the extraditing state's laws,[214] those are only *optional* reasons why countries can refuse extradition.[215] Thus, many states may choose to prosecute or extradite in situations that lack these protections, and they may even prosecute or extradite nationals of states that have previously objected to broad passive personality jurisdiction. By recognizing the validity of passive personality jurisdiction in treaties, states are removing a ground for objection to abusive prosecutions and extraditions. Observers have noted that authoritarian states will invariably abuse the treaty.[216] States may not be able to stop this abuse, but they can maintain a principled objection to passive personality jurisdiction, which would at least avoid facilitating the treaty's abuse against their own citizens.

III. Jurisdictional Restraint

This Part argues that recognition and expansion of passive personality jurisdiction is not only troubling but also unnecessary. Other jurisdictional bases adequately address both cybercrimes and traditional crimes, and they are superior (although far from perfect)

---

[212] GALLANT, *supra* note 15, at 439-40.

[213] UN Cybercrime Convention, *supra* note 4, art. 37(16).

[214] *Id.* art. 37(1), (15). Russia, Pakistan, and Uruguay each separately proposed expressly prohibiting states from invoking the political offense exception for any of the broad offenses in the convention. Fifth Session Consolidated Negotiating Document, *supra* note 201, at 9, 15.

[215] UN Cybercrime Convention, *supra* note 4, art. 37(2) ("[A] State Party whose law so permits may grant the extradition of a person for any of the criminal offences established in accordance with this Convention that are not punishable under its own domestic law."); *id.* art. 37(15) (referring to the Convention not "imposing an obligation to extradite" for political offenses).

[216] *See, e.g.*, Alexander Seger, Head of the Cybercrime Division, Council of Europe, LINKEDIN (Feb. 2024), https://www.linkedin.com/feed/update/urn:li:activity:7162361078486626305 [https://perma.cc/6K37-EXX8] ("Statements by and experience with some states suggest that they may misuse this future treaty for criminal purposes no matter safeguards or limitations of scope. Civil society, industry and other stakeholders are right to be concerned.").

because they already contain principles that limit abuse.

However, passive personality jurisdiction appears here to stay. It is cemented into treaties that enjoy near universal adoption,[217] and states have seemed indifferent to its expansion. Therefore, this paper also offers two more-realistic proposals. One is a limited passive personality jurisdiction that would avoid the due process, sovereignty, and abuse risks detailed above. This approach would allow states to retain a small core of passive personality jurisdiction, while at the same time providing them a basis to argue that they have not abandoned principled limits. The second proposal recognizes that the underlying problem extends beyond the existence of passive personality jurisdiction but rests in its *appeal* to states that want to expand their extraterritorial reach and protect their nationals worldwide. This Part concludes with unilateral steps that states can take to limit the use of passive personality jurisdiction against their nationals.

A. The Case for Eliminating Passive Personality Jurisdiction

The cybercrime treaty illustrates how passive personality is almost always unnecessary and unhelpful. An existing multilateral cybercrime regime already exists. Indeed, the Budapest Convention and the Arab League Convention do not endorse or require passive personality jurisdiction.[218] The convention drafting process treated these existing instruments as valuable precisely because of their efficacy. Indeed, more than a dozen countries have requested accession or have acceded to the Budapest Convention since the launch of the UN negotiations in February 2022[219]—despite it only endorsing jurisdiction based on territory, quasi-territory, and active

---

[217] *See supra* notes 164, 171 and accompanying text.

[218] *See supra* notes 172-173 and accompanying text.

[219] COUNCIL OF EUROPE OFFICE ON CYBERCRIME IN BUCHAREST ACTIVITY REPORT FOR 2023, at 9, SG/Inf(2024)12 (Apr. 5, 2024), https://rm.coe.int/sg-inf-2024-12-c-proc-activity-report-for-2023/1680af3510 [https://perma.cc/26MY-C3T5] ("Since the start of that process in February 2022, Cameroon, Côte d'Ivoire, Ecuador, Grenada, Kazakhstan, Kiribati, Korea, Mozambique, Rwanda, São Tomé and Príncipe, Sierra Leone, Timor Leste and Uruguay requested accession to the Convention on Cybercrime. Brazil, Cameroon and Nigeria also became parties to it.").

personality (nationality).[220]

To be clear, international cybercrime creates difficult problems. The fundamental issue in cyberspace jurisdiction is that it has become relatively easy for a person acting in cyberspace to have effects in a foreign state without ever setting foot on that state's territory. But passive personality jurisdiction is a crude tool to deal with the jurisdictional issues in cyberspace, as it is simultaneously overinclusive and underinclusive.

Imagine a Brazilian man and an American woman are both living in Germany when the Brazilian man, stalking the woman, guesses the password to her phone and illegally accesses personal data on the device. In this hypothetical situation, passive personality jurisdiction would provide the United States jurisdiction, despite no relevant conduct or effect occurring on American territory.[221] There is no meaningful state interest served by international law suddenly giving the United States (or any state in similar circumstances) jurisdiction over this type of ordinary misconduct. In this sense, passive personality jurisdiction is overinclusive, reaching foreign conduct that a state should not be able to criminalize.

On the other hand, passive personality jurisdiction is also underinclusive of much transnational cybercrime that states should be able to criminalize. Imagine patriotic but non-state Russian ransomware actors, using Russian infrastructure and operating from Russian territory, remotely install encryption malware on the phone of a Japanese citizen traveling to the United States to meet with members of Congress to advocate sanctions on Russia for its invasion of Ukraine. The goal of encrypting the phone is to hinder the Japanese national's ability to coordinate those meetings. That conduct, if committed in the United States, would be illegal and would easily clear the jurisdictional bar. But here, no element of the

---

[220] Budapest Convention on Cybercrime, *supra* note 23, art. 22. The Arab League Convention is identical to the Budapest Convention but also added the protective principle as a jurisdictional basis ("if the offence affects an overriding interest of the State"). Arab Convention, *supra* note 173, art. 30.

[221] To prosecute the Brazilian in a domestic court, the United States would have to gain physical custody. But does Washington really have an interest in extraditing the Brazilian from Germany in this case? Or (should the man land in the United States on a layover to São Paolo) in trying him in U.S. courts rather than in letting a Brazilian or German court adjudicate the case?

crime took place on American territory[222] and the victim is not American, so passive personality jurisdiction cannot be invoked.

There are alternative bases of jurisdiction under international law that would adequately convey extraterritorial jurisdiction in this area: the effects doctrine and the protective principle. The protective principle is included in the convention as a discretionary base of jurisdiction, but the effects doctrine is not.[223] Because a ransomware act that seeks to interfere with Congressional meetings has a substantial effect *in the United States*, the effects doctrine would convey jurisdiction even if the encryption occurred aboard a Japanese flag carrier in international airspace. In this sense, it is a better basis for cybercrime jurisdiction. It would address the effects linked issues of cybercrime jurisdiction while avoiding the overinclusive reach of passive personality jurisdiction: notice that effects jurisdiction would not reach the earlier stalking example, as there would be no substantial effect in the U.S. The effects doctrine of jurisdiction is superior because it ensures a strong connection between a state and the regulated subject—a connection at the root of prescriptive jurisdiction under international law.[224]

Effects jurisdiction is the approach that the U.S. Computer Fraud and Abuse Act takes. It defines a class of offenses as involving "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[225] Effects as the proper frame for evaluating actions in cyberspace has also drawn praise in the armed conflict context.[226]

---

[222] Assuming that the actual ransomware encryption occurred while the Japanese citizen was in flight to the United States on a Japanese carrier.

[223] UN Cybercrime Convention, *supra* note 4, art. 22.

[224] *See* RESTATEMENT (FOURTH), *supra* note 5, § 407 reporters' note 3 ("Although often treated independently, the specific bases of jurisdiction set out in §§ 408-413 reflect a broader principle requiring a genuine or sufficiently close connection to justify or make reasonable the exercise of prescriptive jurisdiction.").

[225] 18 U.S.C. § 1030(e)(2)(B). This is actually an attenuated version of effects jurisdiction because a "protected computer" is defined based on its effect on commerce with or in the U.S., but some of the offenses do not themselves have an effects requirement. *See, e.g.*, *id.* § 1030(a)(2)(C) (obtaining information from a protected computer without authorization). *See* United States v. Ivanov, 175 F. Supp. 2d 367, 370 (D. Conn. 2001) (finding jurisdiction over a § 1030 offense "because the intended and actual detrimental effects of [the defendant's] actions in Russia occurred within the United States").

[226] *See, e.g.*, Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 848 (2012).

The protective principle is similarly suited to cybercrimes, as cybercrimes of high severity or systemic reach are the ones that most worry states. Nearly two decades ago, the International Law Commission recognized that the protective principle "may be of particular relevance to new types of cyber crimes."[227]

In its 2006 report, the International Law Commission explained that the unifying principle underlying every non-territorial jurisdictional basis "is the valid interest of the State in asserting its jurisdiction in such a case on the basis of a sufficient connection to the persons, property or acts concerned."[228] Unlike passive personality jurisdiction, which allows jurisdiction based on a tenuous connection, at best constrained only by an amorphous reasonableness standard, the effects doctrine and protective principle have inherent limits: requirements that the effect be substantial and involve vital interests, respectively. They thus are better suited to ensuring this "sufficient connection" and harder for states to abuse.[229] Of course, the substantiality and vital-interest requirements should be made express in any treaty to minimize the ability of states to abuse these bases of jurisdiction. These limits cannot stop a state from questionably invoking a jurisdictional base, but they delegitimize and raise the cost of such assertions. Finally, to the extent the jurisdictional bases nevertheless remain overly broad, states should seek to cabin them—not to endorse yet another jurisdictional basis with even fewer limits.

***

It is also important to consider what passive personality jurisdiction does *not* do. First, it does not create substantive offenses for conduct online, the most critical part of ensuring a state can

---

[227] *Report of the International Law Commission to the General Assembly*, *supra* note 17, at 525.

[228] *Id.* at 521.

[229] These limits suggest that it is too sweeping to claim, as Watson does, that it is just as easy for a state to "declare that conduct violates 'universal' norms, that it implicates the state's 'national security' or that the conduct has 'effects' within the state's security" as it is for that state to invoke passive personality jurisdiction. Watson, *supra* note 109, at 25. For instance, universal jurisdiction is limited to "offenses widely recognized by states as being of universal concern," RESTATEMENT (FOURTH), *supra* note 5, § 413 cmt. a, so a state cannot simply declare a crime universal.

actually exercise jurisdiction over computer crimes.[230] Second, it does not address other jurisdictional issues in cyberspace, such as the competing jurisdictional claims that arise because a cybercrime may involve elements that occur or have effects in multiple states' territory.[231] In fact, by expanding when countries can claim jurisdiction, passive personality jurisdiction would worsen the problem of competing jurisdictional claims, otherwise known as concurrent jurisdiction.[232] Passive personality jurisdiction undermines the fundamental treaty purpose of unifying the cybercrime regime. Rather than encouraging cooperation on a shared core of cybercrimes, the treaty permits fragmented criminal enforcement that legitimizes states exercising jurisdiction over any cyber offense—defined as each state chooses—against any of their nationals.[233] Where states have competing claims of jurisdiction, the treaty provides only for essentially optional consultation.[234]

Third, passive personality jurisdiction does nothing to counter the difficulty of determining where cybercrime has taken place, key to establishing a jurisdictional base and resolving concurrent jurisdictional claims.[235] It can be quite difficult to determine a territorial connection for cybercrime, so dispensing with any such

---

[230] Brenner & Koops, *supra* note 209, at 7 (describing how the Philippines's lack of criminalization of disseminating computer viruses prevented prosecution of the person who distributed the major Love Bug virus).

[231] TALLINN MANUAL 2.0, *supra* note 143, at 54 (acknowledging that many states may "attempt to assert different types of jurisdiction over particular cyber activities"). *See* Brenner & Koops, *supra* note 209, at 3 (emphasizing the scale of jurisdictional conflicts).

[232] *See* Blakesley, *supra* note 113, at 939 (describing how passive personality jurisdiction in the French context may lead to "problems of concurrent jurisdiction").

[233] Recall that undermining cooperation was one of the concerns that the United States initially raised about the negotiations. *See supra* note 75 and accompanying text.

[234] UN Cybercrime Convention, *supra* note 4, art. 22(5) (outlining that in cases of concurrent "investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, *as appropriate*, consult one another with a view to coordinating their actions" (emphasis added)).

[235] *See, e.g.*, Watson, *supra* note 109, at 27 (describing how bilateral extradition clauses typically put states asserting territorial jurisdiction first in line for extradition).

requirement is understandably attractive.[236] But such a determination is usually necessary to attribute the cybercrimes to perpetrators, a prerequisite to enforcing the specific criminal prohibitions. At that point, other jurisdictional bases will ensure that a victim state can exercise jurisdiction. Indeed, effects jurisdiction may itself be useful in determining where the cybercrime took place, as effect is often a proxy for location.[237]

If passive personality jurisdiction is not necessary in cyberspace, where territorial limits most plainly break down, then it is doubtful whether passive personality jurisdiction is necessary in other areas where traditional bases of jurisdiction more readily apply. Indeed, passive personality jurisdiction is also unnecessary outside of the cybercrime context. In the 1930s, the Harvard Law faculty organized research on criminal jurisdiction in international law and prepared an influential draft convention, known as the Harvard Draft.[238] It rejected passive personality jurisdiction in its draft, explaining that that other bases of jurisdiction were sufficient:

> Since the essential safeguards and limitations are precisely those by which the principle of universality is circumscribed in the present article, and since *universality thus circumscribed serves every legitimate purpose for which passive personality might be invoked* in such circumstances, it seems clear that the recognition of the latter principle in the present Convention would only invite controversy without serving any useful objective.[239]

The Harvard Draft endorsed a version of universal jurisdiction that allowed jurisdiction over offenses committed against a state's national "[w]hen committed in a place not subject to the authority

---

[236] *Cf.* GALLANT, *supra* note 15, at 444 (noting a classic case for passive personality jurisdiction is "where the place of the act is unknown").
[237] *See* Brenner & Koops, *supra* note 209, at 44 ("[T]he effect will likely often be used in determining the location of the *act*.").
[238] Dan Jerker B. Svantesson, *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft*, 109 AJIL UNBOUND 69, 69 (2015) ("The influence of the Harvard Draft has been nothing but phenomenal . . . . [I]t is fair to say that the structure put forward in the Harvard Draft has represented public international law's approach to jurisdiction ever since.").
[239] Harvard Draft, *supra* note 5, at 579 (emphasis added).

of any State."[240] In other words, this was an escape clause to ensure that criminal conduct did not go unpunished simply due to attempts to evade *every* state's jurisdiction, for instance if someone committed a murder on an unregistered boat on the high seas. But because it would require the conduct to occur outside the territory of any state, it largely avoided the problems of passive personality jurisdiction (intrusion of sovereignty, due process, and substantive abuse).

When a new problem arises, states often seek to expand jurisdiction. In the 1970s, France endorsed broad passive personality jurisdiction after an act of terrorism led to French hostages and property damage. [241] In that case, the fear was that other jurisdictional bases would fail to reach that type of conduct.[242] But was that necessary? Scholars have observed that many commonly cited examples of passive personality jurisdiction are better understood as exercises of different jurisdictional bases, such as the protective principle in the case of terrorism offenses.[243] Posing the same question with today's precipitous expansion, the answer is unchanged: passive personality jurisdiction is unnecessary.

B. Toward Principled Passive Personality Jurisdiction

Despite its flaws and redundancy, passive personality jurisdiction is undeniably on the rise. Instead of resisting it outright, states could proactively endorse a limited version and make clear that further expansion is not consistent with their understanding of treaty obligations and customary international law. Twin requirements of violence and universality for any crime subject to passive personality jurisdiction would help address due process,

---

[240] *Id.* at 573 (art. 10(c)).

[241] Blakesley, *supra* note 113, at 940.

[242] *Id.*

[243] *Id.* at 941-42 (arguing that passive personality jurisdiction was not necessary even "to address growing contemporary problems with terrorist violence" because the protective principle already covered those crimes); Watson, *supra* note 109, at 9 (explaining that many multilateral terrorism conventions that the United States joined in the 1970s "can be understood as examples of the protective principle . . . rather than the passive personality principle because they protect senior officials of the government, and thus, arguably, the security of the state").

sovereignty, and abuse concerns.[244]

Scholars have proposed various solutions, such as dual criminality and a degree of seriousness (perhaps even violence), to address the due process and sovereignty concerns.[245] But left unexplained is *why* requiring an element of violence is preferable. Nor are requirements of dual criminality and seriousness sufficient to address the substantive risk of abuse.

Universality, essentially a strong version of dual criminality, would incorporate human rights protections into the jurisdictional base itself, rather than relying solely on separate human rights provisions. This novel approach to jurisdictional expansion is both normatively advisable and legally sound, given that most of the expansion of passive personality jurisdiction has been treaty based and even customary international law rests on state practice. Under this approach, passive personality jurisdiction would become a lagging indicator of global criminal law. Passive personality's heightened risks and limited practical necessity justify this approach.

1. Violence

Limiting passive personality jurisdiction to violent crimes would partially address the accompanying due process and sovereignty concerns. Violence is something that states universally criminalize; differences usually turn on the severity of the penalty for violence, not its illegality. Thus, assertion of jurisdiction over a bombing or assassination that occurs in another state's territory disturbs very little the regulatory choices of the state where the conduct occurred. Similarly, anyone who commits that type of violence knows it will be illegal and heavily punished *wherever* it is committed and has no need for special knowledge of foreign criminal codes.

Requiring more than an element of seriousness avoids the problem of states disagreeing on what crimes they consider serious,

---

[244] To the extent the sovereignty concern is about jurisdictional conflicts—who should prosecute, not whether to prosecute—a requirement that the violent conduct be directed at a victim *because of* that person's nationality might be an advisable third criterion. *See* McCarthy, *supra* note 110, at 322 (advocating for this limitation to passive personality jurisdiction to reconcile jurisdictional conflicts).

[245] *See, e.g.*, Watson, *supra* note 109, at 16, 23.

even when both states criminalize the conduct.[246] For instance, even if all states criminalized illegal access and attached a high prison sentence—not an unrealistic possibility given the near universal ratification of past UN crime treaties[247]—they would assuredly disagree on what conduct should be covered under that offense, as disparate implementation of cybercrime offenses demonstrates.[248] An additional element is needed to ensure any exercise of passive personality jurisdiction is appropriate. Violence provides a discrete and relatively straightforward standard to apply.[249]

A limitation to violent crimes could still cover some cyber dependent crimes (such as system interference) and cyber enabled crimes, to the extent they lead to physical injury or death but are simply carried out via cyber means. For instance, after a 2020 ransomware attack on a hospital in Düsseldorf forced the hospital's emergency room to close and turn away an ambulance, German prosecutors sought to hold the attackers responsible for the patient's death under a theory of negligent homicide.[250] They ultimately concluded that the element of causation was too tenuous,[251] but manslaughter and murder prosecutions for cyberattacks are only a matter of time.[252] Unauthorized interference with a medical device,

---

[246] *See* Watson, *supra* note 109, at 22 ("Even if two states both treat certain conduct as criminal, they may punish it in radically different ways."). For instance, in limiting its electronic evidence sharing requirements to serious crimes, the cybercrime treaty defines seriousness by the prison term each state attaches to proscribed conduct, allowing complete domestic control over what conduct constitutes a "serious crime." UN Cybercrime Convention, *supra* note 4, art. 2(h).

[247] *See supra* text accompanying note 164.

[248] *Cf. supra* notes 198-199 and accompanying text (discussing Pakistan's prosecutions of journalists).

[249] Defining violent crimes may be harder than it seems, as the domestic experience with what a "crime of violence" illustrates. *See* Robert A. Zauzmer, *Fixing the Categorical Approach "Mess,"* 69 DEP'T OF JUST. FED. L. & PRAC. 3 (2021). But violence is more objective than many standards, and its combination with universal criminalization would likely leave few edge cases.

[250] William Ralston, *The Untold Story of a Cyberattack, a Hospital and a Dying Woman*, WIRED (Nov. 11, 2020), https://www.wired.com/story/ransomware-hospital-death-germany [https://perma.cc/S4HR-WETQ].

[251] *Id.*

[252] *See, e.g.*, Maggie Miller, *The Mounting Death Toll of Hospital Cyberattacks*, POLITICO (Dec. 28, 2022),

such as a pacemaker or insulin pump, could similarly be a violent crime. In 2017, the Food and Drug Administration recalled nearly 500,000 pacemakers due to a vulnerability that could have allowed attackers to gain control of a device and then to exhaust the battery or change the patient's heartbeat.[253]

Because a requirement of violence would encompass instances of physical harm, this element would allow passive personality jurisdiction to reach some of the more worrisome instances of cybercrime.

2. Universality

A second requirement should be that the conduct be punished universally by UN member states.[254] Although violence and universality probably overlap in most cases, that is not always the case. States' criminal codes sometimes excuse or justify specific instances of violence (e.g., self-defense), and those defenses vary by state. Therefore, universality is an important limiting element that should be ensured separately from the violence element. Universality also avoids the abuse problems that would be created by allowing passive personality jurisdiction simply based on unilateral assertion or bilateral agreement.

Dual criminality is a common proposal to avoid sovereignty concerns.[255] Importantly, however, provisions of the cybercrime convention contain no *requirement* of dual criminality for any

---

https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638 [https://perma.cc/M99S-YDSP] ("A 2021 study . . . which surveyed more than 600 health care facilities, found that mortality rates increased at a quarter of the facilities following a ransomware attack.").

[253] Alex Hern, *Hacking Risk Leads to Recall of 500,000 Pacemakers Due to Patient Death Fear*, GUARDIAN (Aug. 31, 2017), https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update [https://perma.cc/2FKW-4KFA].

[254] Universal criminalization is different from existing universal jurisdiction, which is currently limited to a short list of crimes. GALLANT, *supra* note 15, at 463 (noting customary international law limits universal jurisdiction to "piracy . . . and . . . genocide, crimes against humanity, war crimes, and probably torture").

[255] *See, e.g.*, Watson, *supra* note 109, at 16 ("[I]t seems unlikely that the international legal system will ever approve of passive personality jurisdiction unless there is at least some element of 'dual criminality' built into it.").

jurisdictional assertion—or even for extradition,[256] and the convention allows states to extradite even non-resident foreign nationals for conduct that is not criminalized by the extraditing state. France's expansive passive personality statute, and those of many other states, also lack mandatory dual criminality.[257] Nonetheless, mandatory dual criminality would theoretically be enough to avoid the unilateral assertion problem. For instance, dual criminality would prevent State X from charging a national of State Y for most conduct that State Y does not crimianlize.

But even if it were in the cybercrime treaty and made a requirement of passive personality jurisdiction, dual criminality is an insufficient safeguard. As the cybercrime treaty makes clear, passive personality jurisdiction would allow two states to agree to criminalize innocent conduct and rely on the other for enforcement against non-nationals. What would this look like in practice? Repressive states, such as Russia and Nicaragua, could both have laws that criminalize dissenting speech online, in violation of international human rights law but enforced by their domestic courts. A recognition of passive personality jurisdiction with only a requirement of dual criminality and seriousness would allow Russia to prosecute Nicaraguan nationals for this conduct in its domestic courts. These courts would probably not recognize a defense grounded in international human rights law, but a defense of lack of jurisdiction, because it is based on bedrock principles of international law, might be accepted. Unlimited passive personality jurisdiction would remove that defense.

Thus, although a universality requirement sets a high bar, it is necessary to avoid bilateral agreements that would undermine human rights. By incorporating human rights considerations about what extraterritorial conduct states should be able to criminalize into the bedrock of international law—jurisdiction—this approach treats the fundamental procedural rules as ones that should reflect substantive concerns about risk of abuse. Normally, international human rights law is limited to separate treaties or separate standards within a treaty. While it may not prevent abuses, this approach goes further than existing international human rights law by withholding international endorsement and recognition of potential abuses on

---

[256] UN Cybercrime Convention, *supra* note 4, arts. 22, 37(1), 37(2) (allowing states to waive dual criminality).

[257] Cafritz & Tene, *supra* note 6, at 588; GALLANT, *supra* note 15, at 452.

grounds independent of the human rights objection itself.

These limits to passive personality jurisdiction, if adopted by states, could prohibit most of the potentially concerning exercises of passive personality jurisdiction described in this paper. In the cybercrime treaty context, questionable prosecutions that targeted speech under Article 13 would run up against the requirements of violence and universality, as would prosecutions that targeted journalism.[258]

C. Unilateral Mitigations

Even though individual states can play an important role in organizing support and laying down a marker on this issue, the previous two proposals—abandoning or limiting passive personality jurisdiction—depend in large part on collective action. Such is the nature of international law and the decentralized system of criminal law. Therefore, this Section offers brief proposals for unilateral measures that a state can take to mitigate the harm of passive personality jurisdiction over its nationals.

Early on, a state can refuse to extradite any person sought based on passive personality jurisdiction,[259] and it can intervene in cases in foreign courts to object to assertions of passive personality jurisdiction over its nationals. For instance, a state could argue that state parties' obligation under the convention to act "consistent with their obligations under international human rights law" [260] incorporates some degree of foreseeability[261] and perhaps even dual criminality.

As a legal matter, these types of jurisdictional objections would

---

[258] *See supra* notes 96, 196-197 and accompanying text (discussing how passive personality jurisdiction and cybercrime offenses could apply to these scenarios).

[259] Some, but not all, exercises of passive personality jurisdiction would fall under a treaty provision that allows a state to decline extradition "if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons." UN Cybercrime Convention, *supra* note 4, art. 37(15).

[260] *Id.* art. 6(1).

[261] *See, e.g.*, KENNETH S. GALLANT, THE PRINCIPLE OF LEGALITY IN INTERNATIONAL AND COMPARATIVE CRIMINAL LAW 359 (2009) ("What the current system of international law does require is that the act have at least been foreseeably criminal – reasonably likely to be held criminal – under existing law applicable to the actor when the act is done.").

be particularly effective if the state, when signing or ratifying the cybercrime convention, made a reservation regarding its acceptance of passive personality jurisdiction.[262] Such a reservation would likely be permissible because it is compatible with "the object and purpose of the treaty,"[263] which is to improve international cybercrime cooperation.[264] A reservation would bolster a state's argument that passive personality jurisdiction is not permitted under customary international law or that the state has persistently objected to passive personality jurisdiction—at least with respect to certain applications.

Even where a foreign government or foreign court refuses to consider a state's objection to the prosecution, the act of lodging the objection will simultaneously raise the reputational cost of bringing the prosecution and provide a basis for the state to take more coercive measures.

A state can then back up these objections with diplomatic and economic leverage, ranging from conditioning cooperation to implementing countermeasures. For instance, the U.S. provides extensive cyber support to foreign states, including operational military support and law enforcement assistance and training. The Department of Justice's (DOJ) Office of Overseas Prosecutorial Development, Assistance and Training has stationed prosecutors in 40 countries around the world, with nearly a dozen focused on cybercrime.[265] Another part of DOJ processes foreign requests for U.S. electronic evidence, which have soared so "dramatically" that they are "straining [Justice Department] resources."[266] At the Defense Department, the U.S. military's Cyber Command has conducted "Hunt Forward" defensive cyber operations on at least 27

---

[262] *See supra* note 165.

[263] Vienna Convention on the Law of Treaties art. 19, May 23, 1969, 1155 U.N.T.S. 331 (allowing reservations that are not prohibited by the treaty and that are not "incompatible with the object and purpose of the treaty"). The United States is not a party to the Vienna Convention but has indicated that the Convention's reservation rules reflect customary international law. *See* RESTATEMENT (FOURTH), *supra* note 5, § 305 cmt. e.

[264] *See supra* note 33 and accompanying text.

[265] Global Cyber and Intellectual Property Crimes, U.S. DEP'T OF JUST. (Nov. 8, 2024), https://www.justice.gov/criminal/criminal-opdat/global-cyber-and-intellectual-property-crimes [https://perma.cc/J9VW-C8PZ].

[266] CLOUD Act Resources, U.S. DEP'T OF JUST. (Oct. 24, 2023), https://www.justice.gov/criminal/cloud-act-resources [https://perma.cc/KK2V-7NMR].

foreign states' networks.[267] The United States could condition all of this support on states' refusal to bring or aid abusive passive personality prosecutions, just as it conditions much of its security support on human rights compliance.[268] Any other state that is concerned about harmful jurisdictional creep could take similar actions with its funding and assistance.

Conditioning legal assistance takes on particular significance in states where companies frequently receive requests for electronic evidence from foreign nations. For instance, U.S. technology companies are on the receiving end of many requests. The convention expressly allows states to refuse legal assistance requests "made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions."[269] And it also allows states to refuse any request for mutual legal assistance, including for electronic evidence, where "the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests."[270] A state can argue that fulfilling the request, even if not part of an individually persecutory prosecution, would harm its sovereignty by aiding a foreign penal system that is being turned against the first state's own nationals for domestic conduct.[271]

To the extent a prosecution violates the prosecuting state's international, bilateral, or multilateral human rights obligations, another state could also invoke the prosecuting nation's responsibility and implement countermeasures. These could include ceasing all cooperation under the cybercrime treaty, as well as suspending the state's obligations toward the prosecuting state under

---

[267] Eduard Kovacs, *US Cyber Force Assisted Foreign Governments 22 Times in 2023*, SEC. WK. (Apr. 11, 2024), https://www.securityweek.com/us-cyber-force-assisted-foreign-governments-22-times-in-2023 [https://perma.cc/MR4J-YM74].

[268] Under the "Leahy Laws," the U.S. Departments of State and Defense cannot provide assistance to foreign security or military units that have engaged in certain human rights abuses. *See generally* NINA M. SERAFINO ET AL., CONG. RSCH. SERV., R43361, "LEAHY LAW" HUMAN RIGHTS PROVISIONS AND SECURITY ASSISTANCE: ISSUE OVERVIEW (2014).

[269] UN Cybercrime Convention, *supra* note 4, art. 40(22).

[270] *Id.* art. 40(21)(b).

[271] It might be difficult for a state to square its assertion that passive personality jurisdiction violates its sovereignty with its acceptance of passive personality jurisdiction as a permissible basis in Article 22(2)(a), unless the state made a reservation as to passive personality jurisdiction during ratification.

other bilateral or international treaties.[272] Such tools would be particularly useful when a state's nationals are facing passive personality prosecutions that do not depend on that state's cooperation.

Cooperation conditioning, countermeasures, and other unilateral responses could also target any states that extradite foreign nationals to face passive personality prosecutions.[273] Indeed, a state may have a greater choice of responses in responding to extraditing states than in responding to prosecuting states, at least where the states bringing abusive passive personality prosecutions have little cooperation with the national's home state.

Of course, it might not be in a state's interests to refuse legal assistance requests when they involve criminal activity that the state wants to repress. Similarly, there may be other reasons for states to sustain military, law enforcement, or other cooperation with foreign states. But these options are available and should receive consideration.

Conclusion

Amid the heated debates over the cybercrime treaty—in which one outside group warned that the treaty risks "becoming a

---

[272] *See* Int'l L. Comm'n, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* art. 49(2), U.N. Doc. A/56/10 (2001) ("Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State."). Note that countermeasures may not be permissible where there is a dispute-settlement mechanism for the internationally wrongful act. *Id.* art. 55. The cybercrime treaty provides for the International Court of Justice (ICJ) to hear disputes, unless a state makes a reservation to ICJ jurisdiction. UN Cybercrime Convention, *supra* note 4**,** art. 63. Countries invoke these opt-out clauses routinely (but, on average, only among 20% of the state parties). Jean Galbraith, *Treaty Options: Towards a Behavioral Understanding of Treaty Design*, 53 VA. J. INT'L L. 309, 330 (2013). In any event, a prosecution that is internationally wrongful for violating human rights standards often will be internationally wrongful under other treaties, not just the cybercrime convention.

[273] *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 272, art. 16 (outlining when "[a] State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so").

global surveillance pact"[274]—treaty negotiators, proponents, and opponents have all paid insufficient attention to how the expansion and legitimization of extraterritorial jurisdiction will threaten speech and lawful dissent not only in repressive countries, but also in free democracies. This paper outlines the dangers of this extraterritorial expansion, argues that jurisdictional restraint better protects human rights and promotes efforts to combat cybercrime, and suggests both systematic and unilateral steps that states can take to resist jurisdictional creep.

[274] Katitza Rodriguez, *Proposed UN Cybercrime Treaty Threatens to be an Expansive Global Surveillance Pact*, ELEC. FRONTIER FOUND. (Aug. 22, 2023), https://www.eff.org/deeplinks/2023/08/proposed-un-cybercrime-treaty-threatens-be-expansive-global-surveillance-pact [https://perma.cc/GE4P-V8MS].