SEIZING THE MEANS OF DISRUPTION: INTERNATIONAL JURISDICTION AND HUMAN RIGHTS IN THE EXPANDING FRONTIER OF CYBERSPACE

DANIEL ROSENBERG*

The rise of State-sponsored and rogue botnet-based cyberattacks has presaged a significant expansion in States' willingness to take drastic enforcement measures in cyberspace. While these measures nominally protect civilians from ransomware, malware, and other malicious cyber nuisances, they threaten to erode international principles of extraterritorial jurisdiction and individuals' right to privacy. Neither the Budapest Convention on Cybercrime nor the Tallinn Manual 2.0, the only major international law sources on point, have adequate provisions on jurisdiction and cyberspace. Accordingly, States have begun to disregard international law in cyberspace because of the lack of an effective governance regime. Two recent State disruptions of malicious global botnets, the EMOTET and HAFNIUM operations, reveal the dangers of expanded enforcement jurisdiction in cyberspace. As States are beginning to negotiate a new potential cybercrime treaty, three regulatory principles should be introduced into the cyber enforcement regime: substantial effects jurisdiction, a least intrusive means test as an assessment of cyber operations, and a new optional protocol for the review of individual complaints arising from infringements of human rights during cyber enforcement operations.

* The author is a third year candidate for Juris Doctor at New York University School of Law. He would like to thank Professors Stephen Holmes, David Golove, and Rachel Goldbrenner for their assistance in the development of this paper. The author can be reached at daniel.rosenberg@law.nyu.edu.

I. INTRODUCTION

The internet has shattered traditional conceptions of territorial sovereignty. Today, physical borders are open to the near instant transit of information and commerce. Traditional tools of border control, like checkpoints and customs officers, cannot stop floods of data, originating extraterritorially, from being beamed straight to personal devices.

While this information sharing revolution generated new markets for businesses and new sources of goods and information for consumers, global connectivity carries risks and engenders unforeseen extraterritorial threats. Hacking, disinformation campaigns, ransomware, and malware all manifest from shadowy corners of cyberspace that are often spurred on, at least partially, by malicious State actors. The porous borders of cyberspace present a problem for international law, an inert set of rules and customs ill-suited to addressing these new technologies and transgressions.[1] The rules of how, when, where, and to whom States may direct and enforce their laws in cyberspace are murky at best, and international norms on this topic have not developed sufficiently to provide States with certainty in responding to threats. States face the question of how to protect their people, territory, and infrastructure in an environment where their territorial borders do not exist and accurate attribution of actions is arduous.[2]

---

1. *See, e.g.*, Michael Fischerkeller, *Current International Law Is Not an Adequate Regime for Cyberspace*, LAWFARE BLOG (Apr. 22, 2021), http://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace (discussing the failures of international law to adapt to emerging threats in cyberspace).

2. *See* William Banks, *Cyber Attribution and State Responsibility*, 97 INT'L L. STUD. 1039, 1046 (2021) (noting that while recent technological advances

As the problem grows, States are beginning to recognize the threat that malicious cyber actors pose to key domestic structures. The Tallinn Manual reflects the broad understanding that certain cyberattacks unquestionably rise to a "use of force" under international law, especially those that have a major kinetic effect on territorial people or structures.[3] The official position of many States is that a State actor may respond to cyberattacks with a kinetic effect under a theory of self-defense.[4] However, most cyberattacks and operations fall far short of having a kinetic impact and into a gray area which has been neither well-defined nor well-legislated.[5]

Over the past decade, the proliferation of botnet attacks, one type of "gray area" operation, has exposed deficiencies in the current international law of cyberspace.[6] Both State-sponsored hacking groups and independent criminal organizations now use botnet operations, infecting cloud-based data storage infrastructure, to steal and ransom individual and government information.[7] These attacks have not only caused billions of

---

have made attribution of cyberattacks marginally easier, "knowing the machines or IP addresses responsible for the hack is often difficult, costly, and time-consuming, and knowing those things does not necessarily lead easily to the responsible State.").

3. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 84, r. 14 ¶ 4 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL] (stating that cyber-attacks can violate the prohibition on the use of force); *see also* G7, *G7 Declaration on Responsible States Behavior in Cyberspace* 3 (Apr. 11, 2017), https://www.mofa.go.jp/files/000246367.pdf [https://perma.cc/5PYA-ZW6N] ("In 2016, we affirmed that, under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law.").

4. *See generally* G.A. Res. 76/136 (July 13, 2021) (compiling voluntary national contributions on State perception of the role of international law in cyberspace).

5. *See* François Delerue, *The Threshold of Cyber Warfare: from use of Cyber Force to Cyber Armed Attack, in* CYBER OPERATIONS AND INTERNATIONAL LAW 273, 342 (2020) (concluding that most cyberattacks do not meet the thresholds to fall under the legal framework of *jus contra bellum*).

6. *See infra* Part II-B for a detailed description of a botnet attack.

7. Justin K. Haner & Robert K. Knake, *Breaking Botnets: A Quantitative Analysis of Individual, Technical, Isolationist, and Multilateral Approaches to Cybersecurity*, 7 J. OF CYBERSECURITY 1, 2 (2021).

dollars in damage,[8] but have also destabilized any nascent semblance of a rules-based order in cyberspace.[9]

In the absence of an effective governing framework dictating responses to such attacks, States covertly expand their enforcement jurisdiction in cyberspace, undertaking operations that fail to appropriately respect individuals' rights or classic ideas of territorial sovereignty. A reformulation of the laws governing States' jurisdiction to enforce in cyberspace is necessary to avoid further descent into a chaotic system of retaliation and reaffirm the importance of individuals' freedoms in the digital age.

Part II-A of this paper will explore the current legal regime, discussing the strengths and deficiencies of both the Budapest Convention on Cybercrime (the Budapest Convention) and the Tallinn Manual 2.0 (the Tallinn Manual). Part II-B discusses the rise of the botnet attack as a threat to State security, articulating the definitions for what conduct falls into the gray area that is this paper's focus. Part III discusses recent State practice and *opinio juris* in responding to botnet attacks, highlighting enforcement operations conducted in 2021 against the EMOTET (Part III-A) and HAFNIUM (Part III-B) botnets, and the troubling trends those disruptions reflect. Part IV proposes modifications to the international cybercrime legal regime, both updating its jurisdictional grant and the effectiveness of its human rights protections, ensuring that States can protect their national security interests without infringing upon the sovereignty of other States or the rights of individuals worldwide. Part V concludes with a brief overview of the near future of cyber enforcement, and the benefits and drawbacks of pursuing this paper's proposals.

---

8. James Andrew Lewis et al., *The Hidden Costs of Cybercrime*, CTR. FOR STRATEGIC & INT'L STUDIES 1, 3 (December 9, 2020), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf [https://perma.cc/CZ2E-8ZCD] (noting that in 2018, for the first time, the total "cost of global cybercrime reached over $1 trillion").

9. *See* Asaf Lubin & Joao Marinotti, *Why Current Botnet Takedown Jurisprudence Should Not Be Replicated*, LAWFARE BLOG (July 21, 2021) ("The existing framework of botnet takedowns relies on an ad hoc system of judicial intervention that resembles a game of whack-a-mole. Given the global nature of botnets, various commentators have questioned the efficacy of this framework, with some cybersecurity firms even predicting 'little medium- to long-term impact.'").

II. The Existing Architecture of Cyberspace Law

The very nature of cyberspace has proven difficult for international law to respond to. The traditional underpinning of the international legal regime, the primacy of sovereignty and importance of territorial borders, is almost impossible to apply strictly in cyberspace.[10] Ever-changing technological developments mean that legal modernization, a particularly slow process, lags behind the current problems States face in the digital sphere.[11] Existing frameworks, namely the Budapest Convention and the Tallinn Manual, fail to set adequate jurisdictional limits or protect human rights in cyberspace.

A. *International Frameworks for Cybersecurity Jurisdiction*

The classic formulation of international jurisdiction arose out of the Permanent Court of International Justice's decision in *The Case of the S.S. Lotus*. The Court infamously held that because international law emanates from the consent of States in the system, "[r]estrictions on the independence of States cannot therefore be presumed."[12] The thrust of the *Lotus* principle became that States are free to adopt their own understanding of extraterritorial application of their laws, absent an international rule to the contrary.[13]

The *Lotus* principle has generally gone out of favor as a theory of jurisdiction, even in the International Court of Justice's own jurisprudence.[14] As an alternative, some States still

---

10. *See* Milton L. Mueller, *Against Sovereignty in Cyberspace*, 22 Int'l Studs. R. 779, 788–791 (2020) (discussing the difficulties of applying the principles of sovereignty and territoriality in cyberspace).

11. Dan Efrony & Yuval Shany *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 Am. J. Int'l L. 583, 588 (2018) (noting that "the combination of silence and ambiguity in state practice and their reluctance to articulate their official policy in cyberspace prevents or, at least, slows the development of global norms of conduct.").

12. S.S. Lotus (Fr. v. Turk.), Judgement, 1927 P.C.I.J. (Ser. A) No. 10 at 19 (Sept. 7).

13. *See, e.g.*, Armin von Bogdandy, Markus Rau, *The Lotus*, Max Planck Encyclopedia of Pub. Int'l L. ¶ 15 (June 2006), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e162 [https://perma.cc/YS92-GKF7] (noting that in modern legal thought, the Lotus principle refers to the idea that "States have the right to do whatever is not prohibited by international law.").

14. *See, e.g.*, Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.), Judgement, 2002 I.C.J. 3, 63, ¶ 51 (Feb. 14) (joint separate opinion of Hig-

consider the absolute nature of territorial sovereignty as the primary rule of international jurisdiction. China, for instance, maintains a strict definition of sovereignty, proscribing any incursion into the essential sovereign functions and territory of another State.[15] Many States, however, especially those which legislate in a common law tradition, now follow a more malleable definition of territorial sovereignty, applying laws extraterritorially under five general principles of jurisdiction: territoriality, protection of national interest, active nationality, passive nationality, and universality.[16] These principles provide a more cohesive structure for the application of domestic laws to extraterritorially located people and property. States often, for instance, collect taxes from extraterritorially located nationals,[17] implement antitrust regulations against companies affecting their domestic commerce,[18] or enforce counterterrorism laws against extraterritorially located threats to national security.[19]

Even States with absolutist approaches to sovereignty have begun to acknowledge that the inexorable interconnectedness of the digital world means that sovereignty "does not establish an absolute bar against individual or collective state cyber op-

---

gins, Koojimans & Buergenthal, Js.) (noting that the *Lotus* principle "has been significantly overtaken by other tendencies."); *see also* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶¶ 21–22 (July 8) (dismissing the nuclear weapons possessing States' arguments based upon the *Lotus* principle, despite simultaneously concluding that there was no specific international norm prohibiting the threat or use of nuclear weapons).

15. Yanzhong Huang et al., *China's Approach to Global Governance*, COUNCIL ON FOREIGN RELS. (2022), https://www.cfr.org/china-global-governance/ [https://perma.cc/L8XS-WNTN] (noting that in the seminal "Five Principles of Peaceful Coexistence" enumerated by China, both sovereignty and noninterference in domestic affairs are highlighted).

16. *See* CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 29, 36–38, 101 (2d ed. 2015) (discussing the territoriality principle and extraterritorial exertion of power); *see also* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 407–13 (AM. L. INST. 2018) (explaining the United States' approach to the classic principles of extraterritorial jurisdiction).

17. *See* RYNGAERT, *supra* note 16, at 107 (2d ed. 2015) (applying the nationality principle to tax policy).

18. *Id.* at 143 (discussing the protective principle's application in an antitrust setting).

19. *Id.* at 111 (discussing the application of universality in response to terrorism).

erations that affect cyberinfrastructure within another state."[20] The United Nations commissioned a Group of Governmental Experts Report in 2015 which juxtaposed the continued application of the norm of sovereignty in cyberspace against the "need for further study" on how States may respond to cyberattacks originating extraterritorially.[21] As evidenced from both the Budapest Convention and the Tallinn Manual, the rules-based order of cyberspace remains in flux, and limitations on jurisdiction and rights in "remotely conducted cyber intrusions" are nebulous.[22]

i. *The Budapest Convention*

In cyberspace, the classic formulations of jurisdiction fail to provide adequate restraint on State action. The only multilateral treaty on point,[23] the Budapest Convention, does not sufficiently clarify when and how States may enforce their cybersecurity laws extraterritorially.

The Budapest Convention was concluded in 2004 and currently has sixty-seven parties.[24] Through the Budapest Convention, the States Parties hoped to create "a common crimi-

---

20. Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INTL L. UNBOUND 207, 208–209 (2017); *see also* Roger Creemers, *China's Approach to Cyber Sovereignty*, KONRAD-ADENAUER-STIFTUNG at 19 (2020) ("As a result of decades of comparatively borderless development [in China], in which software, hardware and online services, their supporting business sectors and infrastructures, and flows of data and information are intertwined in complex ways.").

21. Rep. of the Group of Gov't Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., ¶ 28, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter GGE Report].

22. *See* Michael Schmitt, *In Defense of Sovereignty in Cyberspace*, JUST SECURITY (May 8, 2018), https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/ [https://perma.cc/V3PX-VG2D] (stating that "*rules* of international law that address remotely conducted cyber intrusions have yet to emerge from the *principle* of sovereignty . . . .").

23. *See 20 Years of the Convention on Cybercrime*, COUNCIL OF EUROPE (2021), https://www.coe.int/en/web/cybercrime/20th-anniversary-budapest-convention [https://perma.cc/7QEY-HTJM] (stating that after 20 years, the Budapest Convention "remains the most relevant treaty on cybercrime and electronic evidence.").

24. *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*, COUNCIL OF EUROPE [hereinafter Budapest Convention Parties], https://www.coe.int/en/web/cybercrime/parties-observers [https://perma.cc/5995-ZHDG] (last visited Oct. 18, 2022).

nal policy aimed at the protection of society against cybercrime" through the harmonization of laws across member countries and implementation of a regulation scheme.[25] Article 22 of the Budapest Convention addresses jurisdiction, limiting States' jurisdiction to enforce to their territory, aboard their ships and aircrafts, and to offenses "by one of [their] nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."[26]

Article 22 has two main deficiencies. First, the Budapest Convention was drafted at a time when data and computers accessed in one State were still primarily physically located in that State's territory.[27] The advent of cloud storage and the explosion in the sheer mass of data transmitted across borders every day means that this is no longer the case, and the Budapest Convention fails to adequately regulate States' access to data and devices located outside of their territory.[28] This undefined territorial limitation is unmoored from the reality of the cyber enforcement space, and States have instead turned back to the *Lotus* principle, exerting jurisdiction liberally in the absence of an effective contrary international rule.[29] As data's "location" becomes increasingly detached from a single physical anchor, States use that uncertainty as a grant of jurisdiction.[30] Even the Budapest Convention, if read broadly, in-

---

25. Budapest Convention on Cybercrime, pmbl., *opened for signature* Nov. 23, 2001, T.I.A.S. No. 13,174, 2296 U.N.T.S. 167 (entered into force July 1, 2004) [hereinafter Budapest Convention].

26. *Id.* art. 22.

27. Jennifer Daskal & Debrae Kennedy-Mayo, *Budapest Convention: What Is It and How Is It Being Updated?*, CROSS-BORDER DATA FORUM (July 2, 2020), https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/ [https://perma.cc/T9K2-PW2G].

28. *See id.* ("The disconnect between territorial jurisdiction of states and the ways in which data moves and is held across national borders poses significant challenges for law enforcement. Even when law enforcement knows where to go to request that data, and even in situations in which the relevant countries have friendly relations, the multiple steps required to access the data often lead to lengthy delays.").

29. Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, 6 STRATEGIC STUDS. Q. 126, 141 (2012) (noting that due to the lack of an effective international legal regime in cyberspace, "for better or worse, the default—permissive international law regime—governs.").

30. *See Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal*

cludes this "loophole" by allowing for "any criminal jurisdiction exercised by a Party in accordance with its domestic law."[31] Also left unanswered is the question of how far a State's territory extends in a space without physical borders, essentially leaving States unconstrained in this new legal frontier.[32]

Compounding this problem is the inadequacy of the Budapest Convention's provisions on human rights in cyberspace. Article 15 is the only provision that addresses human rights and simply states that the implementation and application of the Convention's provisions "are subject to conditions and safeguards" under a State's domestic law, including rights arising under the European Convention for the Protection of Human Rights and the International Covenant on Civil and Political Rights (the ICCPR).[33] This protection is insufficient in two ways.

First, the Budapest Convention fails to implement any standalone rights for individuals affected by cyber enforcement operations. Article 15 does "incorporate the principle of proportionality" with regard to the application of its principles,[34] but unlike the Human Rights Committee, the Cybercrime Convention Committee has not adopted a determinate standard for proportionality.[35] The Budapest Convention does not safeguard any specific right to privacy, protect against the access by a State to personal data, or provide a standardized

---

Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, at 28, COM (2018) 226 final (Apr. 17, 2018) ("Member State[s] assert[ ] jurisdiction over data for which it is not possible to determine its location, and accesses it directly from an information system within its territory, without the assistance of an intermediary.").

31. Budapest Convention, *supra* note 25, art. 22.

32. *See infra* Part III for a full discussion of the failures of international law to constrain jurisdiction in cyberspace.

33. Budapest Convention, *supra* note 25, art. 15.

34. *Id.*

35. *See, e.g.*, U.N. Hum. Rts. Comm. [UNHRC], General Comment No. 27, ¶ 14, CCPR/C/21/Rev.1/Add.9 (Nov. 2, 1999) (discussing the least intrusive means test as an element of proportionality); *see also* Douwe Korff, *The Rule of Law on the Internet and in the Wider Digital World*, COUNCIL OF EUR. COMM'R FOR HUM. RTS. at 94 (Dec. 2014), https://rm.coe.int/16806da51c [https://perma.cc/C5YD-P7LL] (discussing how despite the mention of proportionality in the Budapest Convention, "it does not clarify such matters in any more specific way.").

test to determine when rights may be limited in the interest of cybersecurity.[36] Instead, proportionality is "implemented by each Party in accordance with relevant principles of its domestic law."[37]

Second, the passing reference to the ICCPR in Article 15 is not a sufficient bulwark against human rights violations. The scope of the ICCPR is limited to "all individuals within [a State's] territory and subject to its jurisdiction,"[38] potentially excluding swaths of people outside a State's territory or jurisdiction who might nonetheless be affected by that State's cyber enforcement actions.[39] As States become more willing to fight botnet attacks through intrusions into unaware individuals' devices around the world,[40] this gap in the ICCPR's application undermines human rights in cyberspace. Furthermore, the applicable substantive provisions of the ICCPR have not been developed sufficiently regarding cyberspace. Despite calls for an updated Comment by the Human Rights Committee,[41] the last interpretive exercise done regarding the right to privacy and the home occurred in 1988.[42] Accordingly, this Comment fails

---

36. *See Abuse of Cybercrime Measures Taints UN Talks*, HUM. RTS. WATCH (May 5, 2021), https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks [https://perma.cc/NJF3-2XSQ] (noting that "human rights experts have long pointed out that [the Budapest Convention] should incorporate stronger safeguards for human rights.").

37. Explanatory Report to the Convention on Cybercrime, ¶ 146, *opened for signature* Nov. 23, 2001 [hereinafter Explanatory Report].

38. International Covenant on Civil and Political Rights, art. 2(1), *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

39. *See, e.g.*, Ashley Deeks, *Does the ICCPR Establish an Extraterritorial Right to Privacy?*, LAWFARE BLOG (Nov. 14, 2013), https://www.lawfareblog.com/does-iccpr-establish-extraterritorial-right-privacy [https://perma.cc/3NQE-AAPG] (noting that while there are differing interpretations of the scope of application of the ICCPR, some States, including the United States, argue that "the ICCPR does not apply extra-territorially, because [. . .] the scope requirement [limits] the treaty to activity within U.S. territory.").

40. *See infra*, Part III.

41. *See generally Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights*, ACLU (2014) [hereinafter ACLU Proposal], https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf [https://perma.cc/F7PV-NWGN] (detailing the need for the Human Rights Committee to issue a new Comment interpreting the right to privacy).

42. UNHRC, General Comment No. 16, CRC/C/GC/16 (Apr. 8, 1988).

to even reference the internet and reflects an outdated understanding of the right to privacy in a modern context.[43]

The Budapest Convention, however, is a success in its forward-looking drafting, which was intended to allow for evolution of the treaty in response to technological change.[44] The development over time of Chapter II of the Budapest Convention, outlining its substantive criminal provisions, demonstrates the progressive malleability of the treaty. The drafters' use of "technology-neutral" language ensures that "the substantive criminal law offences may be applied to both current and future technologies,"[45] and the Council of Europe continues to issue Guidance Notes that update the Budapest Convention's application to modern cybercrimes.[46] In 2013, for example, the Cybercrime Convention Committee issued guidance that the "common understanding of the Parties" was that the Budapest Convention's substantive criminal provisions applied to the operation of botnets.[47] Still, the usefulness of the Budapest Convention's criminal standards is undermined by its failure to adequately regulate State responses to cybercrime.

The Budapest Convention's provisions on jurisdiction and human rights leave too much discretion to domestic legal schemes and outdated international frameworks. Therefore, the Budapest Convention serves as a weak operational framework to address cyberspace concerns.

ii. *The Tallinn Manual 2.0*

One attempt at reformulating international cyber enforcement law is the Tallinn Manual. Published in 2017, the Tallinn Manual reflects the second attempt by a large group of cybersecurity experts to collect and analyze existing customary

---

43. *Id.*

44. *See* Explanatory Report, *supra* note 37, ¶ 36.

45. *Id.*

46. *See* Cybercrime Convention Committee (T-CY), *T-CY Guidance Notes*, T-CY (2013) 29rev (July 8, 2019) (compiling all guidance notes adopted by the Committee).

47. Cybercrime Convention Committee (T-CY), *Guidance Note #2: Provisions of the Budapest Convention Covering Botnets*, COUNCIL OF EUROPE at 3 (June 4–5, 2013), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7094 [https://perma.cc/RLA8-NG78].

international law norms in cyberspace.[48] While States have generally not accepted the Tallinn Manual as constitutive of international law,[49] NATO States have at least indicated public support for the "underlying premise of this project" and participated in its drafting.[50] This iteration of the Tallinn Manual had the benefit over its predecessor of over fifty State advisors, including those from NATO States, as well as India, China, and South Korea, giving input on the drafting under a "Chatham House Rules" process.[51]

Though States have yet to accept the Tallinn Manual as legally binding, it represents a modern attempt to apply international law in a world increasingly connected by the internet. Chapter 3 of the Tallinn Manual is especially relevant, as it elucidates a jurisdictional framework for cyberspace.

The Tallinn Manual adopts a basic theory of jurisdiction that is consistent with the Budapest Convention, declaring that States' jurisdiction to enforce "is generally limited to the territory of the State that is exercising the jurisdiction" unless the exercise of jurisdiction is otherwise authorized, either by a distinct rule of international law or by the consent of another State.[52] The Tallinn Manual also expands upon the Budapest Convention's definition of territoriality. Recognizing the deficiencies in the Budapest Convention, and the difficulties of defining territorial borders in a cloud-based world, the Tallinn Manual asserts that States may access data that is available publicly in their territory but is hosted on servers abroad through the "exercise[e] [of] territorial, as opposed to extraterritorial, enforcement jurisdiction."[53] As long as the data is stored in a cloud server which has a connection to a State, the Tallinn Manual contemplates that State's enforcement against that

48. TALLINN MANUAL, *supra* note 3, at 3–5.

49. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law of Cyber Operations: What it Is and Isn't*, JUST SECURITY (Feb. 9, 2017), https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ [https://perma.cc/9AEB-LG9M] (noting that while State views were considered in the drafting of the Tallinn Manual, "*Tallinn 2.0* does not reflect the views of any State or group of States.").

50. Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 171 (Nov. 10, 2016).

51. EMILY CRAWFORD, NON-BINDING NORMS IN INTERNATIONAL HUMANITARIAN LAW: EFFICACY, LEGITIMACY, AND LEGALITY 127–128 (2022).

52. TALLINN MANUAL, *supra* note 3, at 66–7, r. 11, ¶ 1.

53. *Id.* at 69, r. 11, ¶ 12.

data to be territorial. Furthermore, the Tallinn Manual would also grant States territorial jurisdiction in situations in which there are "cyber activities having a substantial effect in [their] territory."[54] This "objective territorial" jurisdiction aligns with recent State treatment of botnets,[55] and the Tallinn Manual proposes concurrent enforcement jurisdiction in such situations: "if individuals in State A deploy a botnet by taking control of cyber infrastructure in State B in order to conduct a DDoS operation against systems in State C, all three States will possess jurisdictional competence."[56]

The benefit of the Tallinn Manual's definition, as opposed to that of the Budapest Convention, lies in its date of creation. Unlike the Budapest Convention, cloud-based computing had emerged as the dominant form of data storage by the time the drafters of the Tallinn Manual began negotiating its terms.[57] The Tallinn Manual notes that cloud computing is "[a] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction."[58] Unlike the device-specific model of data storage and usage contemplated within the Budapest Convention, the Tallinn Manual recognizes that the cloud-based computing model creates an interlocking global web of data sharing ill-suited to traditional concepts of "location" for State action.[59]

If the Tallinn Manual's definition of jurisdiction is the future of cyberspace enforcement, however, a pair of issues must be addressed. First, there should be a threshold established for when a State may reasonably exercise its territorial jurisdiction. Given the near impossibility of disentangling the transit

54. *Id.* at 55, r. 9.

55. *See infra*, Part III.

56. TALLINN MANUAL, *supra* note 3, at 69, r. 9, ¶ 2.

57. *See* Primavera De Fillippi & Smari McCarthy, *Cloud Computing: Centralization and Data Sovereignty*, 3 EUR. J. L. & TECH. at 2 (Nov. 2012), https://ejlt.org/index.php/ejlt/article/download/101/245 [https://perma.cc/DH4X-JHUM] (noting that cloud computing as a concept gained mainstream popularity in 2006).

58. TALLINN MANUAL, *supra* note 3, at 563.

59. Jan Spoenle, *Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?*, COUNCIL OF EUROPE PROJECT ON CYBERCRIME 5–6 (Aug. 31, 2010) (discussing how cloud computing complicates the concept of location in regard to criminal law enforcement).

of data in cloud systems across territories, a *de minimis* standard for exerting jurisdiction over data touching one's territory does not provide sufficient regulation on State action.[60] Second, the Tallinn Manual's address of human rights, that "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy,"[61] is insufficiently precise to protect against the potential deluge of State action this expansion of jurisdiction portends. These two issues could be addressed either through an updated interpretation of the Budapest Convention or the negotiation of a new multilateral treaty.

In the last several years, both States and private parties began calling for a legitimate international framework to govern cyber enforcement, and preliminary negotiations on a new treaty began in 2022.[62] In the past decade, the rise of botnet attacks has made the problem even more salient. Even countries traditionally resistant to such international agreements have signaled a willingness to come to the negotiating table,[63] confirming that the time to strike on updating the legal regime is now.

B. *The Rise of the Botnet Attack*

Updating the rules of State enforcement in cyberspace has become so important because of the increasing scale and sophistication of cyberattacks and States' utilization of such attacks as a geopolitical tool. As discussed above, certain types of cyberattacks would almost certainly allow States to respond de-

---

60. TALLINN MANUAL, *supra* note 3, at 55, r. 9, ¶ 3 ("[T]he International Group of Experts was split with respect to whether a State may exercise jurisdiction on the basis of the territorial principle when there is only minimal connection with cyber infrastructure on that State's territory.").

61. *Id.* at 187, r. 35.

62. *See, e.g.,* PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE (Nov. 12, 2018), https://pariscall.international/en/call [https://perma.cc/T2ZT-V7W5] (comprising 81 States, 706 companies, and 390 Civil Society Organizations); *see generally* Rep. of the Ad Hoc Comm. to Elaborate a Comprehensive Int'l Convention on Countering the Use of Info. and Commc'ns Techs. for Crim. Purposes [AHC] on its Session on Organizational Matters held on 24 February 2022, U.N. Doc. No. A/AC.291/6 (Mar. 2, 2022) (discussing the initial agenda and discussants for the potential new cybercrime treaty framework).

63. *See* CRAWFORD, *supra* note 51, at 128 (highlighting China's participation in creating the Tallinn Manual 2.0).

cisively, even extraterritorially.[64] Attacks with kinetic effects such as human fatalities, the destruction of physical facilities, or the debilitation of critical infrastructure would activate a State's inherent right to self-defense,[65] enshrined in the Charter of the United Nations.[66] But few, if any, attacks have ever reached this threshold. A 1982 covert operation by the United States that overloaded the computing ability of a section of the Trans-Siberian oil pipeline using a "logic bomb," which resulted in a large explosion, is one example of a cyberattack that might be equivalent to a kinetic military operation.[67] Another is the Stuxnet operation, allegedly conducted by Israel in the mid to late-2000s, which reportedly infected Iran's Natanz nuclear facility and sabotaged the centrifuges housed within the plant.[68] However, the vast majority of cybercrime has fallen into a gray area short of actions recognized as use of force.[69]

Perhaps the most dangerous type of attack in this gray area is a botnet attack. Botnets work by exploiting loopholes in computers' protection systems, either by actively hacking into programs like Microsoft Exchange,[70] or by utilizing phishing attacks to dupe individuals into giving the botnet access to their device.[71] Once the botnet has access to a device, it can set up a webshell, which essentially operates as a "code skeleton"

---

64. *See supra* Part II-A.

65. *See, e.g.*, *Use of Force*, INTERNATIONAL CYBER LAW IN PRACTICE TOOLKIT, https://cyberlaw.ccdcoe.org/wiki/Use_of_force#Australia [https://perma.cc/PX7S-R8QP] (Sept. 12, 2022, 3:49 PM) (describing Australia's national position on the right of reprisal in response to a cyberattack with significant infrastructural effects).

66. U.N. Charter, art. 51.

67. Marco Roscini, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 53 (2014).

68. *Id.* at 7, 53.

69. *See id.* at 104 (stating one could claim that "low-intensity cyber attacks are the most common form of cyber force between states.").

70. *See, e.g.,* Gordon Corera, *China Accused of Cyber-Attack on Microsoft Exchange Servers*, BBCNEWS (July 19, 2021), https://www.bbc.com/news/world-asia-china-57889981 [https://perma.cc/5UKK-D429] (explaining how a recent cyberattack allegedly originating from China infiltrated individual devices through a security flaw in Microsoft's email servers).

71. Chuck Brooks, *When Botnets Attack*, FORBES (Apr. 22, 2022), https://www.forbes.com/sites/chuckbrooks/2022/04/22/when-botnets-attack/?sh=588813b144df [https://perma.cc/XZP5-445W].

on the infected device.[72] From there, botnet operators working from command-and-control servers can utilize these webshells to propagate further cybercrimes, including ransomware attacks, disinformation spreading, and identity theft.[73] This modern form of cyberattack, described as "Malware-as-a-Service," allows botnet operators to sell access to millions of computers worldwide for nefarious purposes.[74] Criminal groups, governments, and other malicious actors can pay the command-and-control server operator to use these existing botnet webs to facilitate criminal activity.[75]

Criminal groups and State actors have demonstrated over the past decade that botnet attacks are the new "weapon of choice" for cybercrime.[76] In the years preceding the Russian invasion of Ukraine, Ukraine experienced several botnet attacks, likely sponsored by Russian State actors, which spread propaganda and facilitated ransomware operations.[77] In the months of war following Russia's invasion, the Russian State actors have allegedly used botnets to attack both Ukrainian infrastructure and to continue to spread malicious propaganda within Ukraine.[78] When Russian forces invaded Kharkiv, for

---

72. Merritt Baer, *Do Russian-Backed Bots Qualify for Free Speech?*, THE DAILY BEAST (Oct. 29, 2017), https://www.thedailybeast.com/do-russian-backed-bots-qualify-for-free-speech [https://perma.cc/FH28-D6WZ].

73. *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 113th Cong. 891 (2014) (opening statement of Sen. Sheldon Whitehouse) [hereinafter *Taking Down Botnets*] (describing how "[b]otnets enable criminals to steal individuals' personal and financial information, to plunder bank accounts, [and] to commit identity theft on a massive scale. For years, botnets have sent most of the spam that we all receive.").

74. Christopher Wray, Dir., FBI, Remarks on Tackling the Cyber Threat Through Partnerships and Innovation (Mar. 4, 2020) (transcript available at https://www.fbi.gov/news/speeches/tackling-the-cyber-threat-through-partnerships-and-innovation [https://perma.cc/W428-HNEJ]).

75. *See id.* (explaining how otherwise unsophisticated criminals can "rent" botnets "to paralyze entire hospitals, police departments, and businesses with ransomware.").

76. *See Taking Down Botnets*, *supra* note 73, at 891.

77. Alert AA22-110A, United States Cybersec. & Infrastructure Sec. Agency, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (Apr. 20, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-110a [https://perma.cc/C8FE-CCGY].

78. Press Release, Sec. Serv. of Ukr., SSU Shuts Down Million-Strong Bot Farm the Destabilized Situation in Ukraine and Worked for One of Political Forces (Aug. 2, 2022, 1:30 PM), https://ssu.gov.ua/en/novyny/sbu-

instance, a botnet server in the region "spam[med] cell phones with malicious text messages."[79] Ukrainian officials estimate that since the beginning of the invasion, cyberattacks by Russian State entities, both within Ukraine and worldwide, have increased threefold.[80]

Botnet attacks are also proliferating outside of Russia. A North Korean botnet attack in 2017 led to the largest ransomware event in history, affecting companies and individuals in over 150 countries.[81] The EMOTET and HAFNIUM attacks, discussed below, affected millions of devices across dozens of countries. Due to the widespread scale and reach of these types of attacks, States face difficulties in adequately suppressing a sprawling botnet infection in their territory in accordance with the existing principles on territoriality. As Part III will discuss, State enforcement operations are growing exponentially in scale to combat these attacks, and the resulting disregard of States' and individuals' rights in cyberspace in pursuit of cybercriminals threatens to chip away at both human rights and extraterritorial enforcement jurisdiction standards. Analysis of the EMOTET and HAFNIUM disruptions demonstrates that absent an effective legal regime, the cure may be worse than the disease.

III. Recent Enforcement Operations and the Deficiencies of the Current International Legal Regime

For decades, common law States have proposed that extraterritorial enforcement against certain types of crimes is permissible if there is a "'real and substantial link' between an

---

likviduvala-milionnu-botofermu-yaka-rozkhytuvala-obstanovku-v-ukraini-na-zamovlennia-odniiei-z-politsyl-video.

79. Kenneth Rosen, *The Man at the Center of the New Cyber World War*, Politico (July 14, 2022, 4:30 AM), https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486 [https://perma.cc/D35T-MN9M].

80. *Id.*

81. Alert TA17-132A, United States Cybersec. & Infrastructure Sec. Agency, Indicators Associated with WannaCry Ransomware (June 7, 2018), https://www.cisa.gov/uscert/ncas/alerts/TA17-132A [https://perma.cc/K6AS-92F9].

offence and th[e] country."[82] English courts, for instance, have historically held that "nothing in precedent, comity or good sense . . . should inhibit the common law from regarding as justiciable in England inchoate crimes committed abroad which are intended to result in the commission of criminal offences in England."[83] Often applying the protective principle or the "objective territoriality" noted in the Tallin Manual,[84] many States, especially in the West, have been willing to act against crimes which threaten their perceived national interest.[85] Even the traditionally conservative civil law country of Japan[86] has begun to extend its reach extraterritorially for cyber enforcement.[87] These are not necessarily new doctrines of extraterritorial enforcement, but they are now being applied against new threats. Two major enforcement operations in 2021, the EMOTET and HAFNIUM disruptions, demonstrate the new paradigm of enforcement jurisdiction in cyberspace, and the challenges it poses to both individuals' and States' rights.

---

82. Libman v. the Queen, [1985] 2 S.C.R. 178 (Can.) (addressing fraud allegedly originating from outside of Canada's territory).

83. R v. Smith, [2004] EWCA (Crim) 631 [55], [2004] QB 1418 (Eng.).

84. *See* Wolff Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, *in* 2012 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 7, 13-15 (C. Czosseck et al. eds., 2012) (noting that the protective principle or objective territoriality "may give rise to the exercise of jurisdiction over individuals who have conducted cyber operations against the cyber infrastructure in another State.").

85. *See, e.g.*, Intelligence Services Act 1994, c. 13, § (3)(2)(a–b) (UK) (permitting British authorities to exercise jurisdiction over electronic operations "in relation to the actions or intentions of persons outside the British Islands" when it would be "in the interests of national security . . . or "the economic well-being of the United Kingdom.").

86. Makoto Yazawa, *Interim Report by the Committee on Extraterritorial Effects of Trade Regulation*, 7 JAPANESE ANN. INT'L L. 80, 83 (1963), https://heinonline.org/HOL/P?h♂in.journals/jpyintl7&i=88 [https://perma.cc/4AQC-W5BJ] (noting the traditional conception of extraterritoriality in Japanese law was that "[a] country does not have regulatory jurisdiction over foreigners, acting in a foreign country, even though the act eventually brings economic injury to the former country.").

87. *See generally* Tomoki Ishiara, *The Privacy, Data Protection, and Cybersecurity Law Review: Japan*, THE LAW REVIEWS (Nov. 6, 2021), https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/japan (discussing how a 2020 amendment to Japan's Act on the Protection of Personal Information has significantly expanded extraterritorial Japanese enforcement in cyberspace).

A. *The EMOTET Disruption*

EMOTET is a malware distributing botnet, first detected in 2014, which has infected well over a million devices worldwide.[88] It infiltrates devices through several avenues, including Trojan horse email messages, and then converts those devices into a worldwide network of inert tools which can be ransomed or used to then pursue further criminal activities.[89] EMOTET was responsible for several serious breaches of security in a number of nations, including an attack which forced the German city of Frankfurt to shut down its entire information technology network,[90] a ransomware attack on a North Carolina school district that succeeded in stealing $1.4m,[91] and thousands of other attacks of varying severity worldwide.[92]

This type of botnet works by establishing a connection between the main command-and-control server (or servers) and the webshells installed on the infected devices, allowing those devices to receive communications, additional malware, and other data from the originating server.[93] In January 2021, a group of eight countries[94] took action against EMOTET, loading disruptor files onto infected devices which prevented the

---

88. *See* Press Release, Europol, World's Most Dangerous Malware EMOTET Disrupted Through Global Action (Jan. 27, 2021) [hereinafter Europol Press Release], https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action [https://perma.cc/8TJW-LGJ2]; Press Release, Dep't of Just., Emotet Botnet Disrupted in Int'l Cyber Operation (Jan. 28, 2021), https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation [https://perma.cc/VP5A-Z265].

89. Alert AA20-280A, U.S. Cybersec. & Infrastructure Sec. Agency, Emotet Malware (Oct. 24, 2020) [hereinafter EMOTET Alert], https://www.cisa.gov/uscert/ncas/alerts/aa20-280a [https://perma.cc/G52Y-EC5D].

90. Frederic Gilles Sourgens, *Cyber-Nuisance*, 42 U. PA. J. INT'L L. 1005, 1035 (2021).

91. Affidavit in Support of an Application for a Search Warrant ¶ 9, *In re* Info. Associated with Three IP Addresses that is Stored at Premises Controlled by Digitalocean, LLC, No. 21-mj-00036-LPA (M.D.N.C. Jan. 27, 2021) [hereinafter EMOTET Affidavit].

92. *See* EMOTET Alert, *supra* note 89 (noting the detection of roughly 16,000 individual instances of EMOTET activity).

93. *Id.* (providing a timeline of how EMOTET infects devices).

94. *See* Europol Press Release, *supra* note 88 (the countries involved were the Netherlands, Germany, France, Lithuania, Canada, the United States, the United Kingdom, and Ukraine).

command-and-control server from communicating with those devices.[95] This first step was relatively unproblematic, at least as a matter of jurisdiction, as each of the acting countries' domestic law enforcement agencies only acted on the infected devices within their sovereign territory.[96]

The problem with this limited action, however, was that it left the malware on the infected devices, and merely disabled communications between those devices from the command-and-control server.[97] In April 2021, several of the enforcing States[98] took a much more effective but considerably more controversial step, activating EMOTET deletion files which had been loaded onto infected devices worldwide to destroy the malware.[99] This was done without the knowledge or consent of the affected individuals, and the responsible State agencies obfuscated the scope and nature of the operation.[100]

---

95. Press Release, Dep't of Just., *supra* note 88.

96. *Id.* (noting the initial disruption of communications with EMOTET command-and-control servers and targeted devices was done by foreign law enforcement and the FBI only "on servers located in their jurisdiction").

97. EMOTET Affidavit, *supra* note 91, ¶ 19 (noting that "the law enforcement file does not remediate malware that was already installed on the infected computer . . . .").

98. It remains unclear exactly which States participated in the kill switch operation but appears to be at least Germany and the United States, and likely the Netherlands. *See* Gareth Corfield, *Emotet Malware Self-Destructs after Cops Deliver Time-Bomb DLL to Infected Windows PCs*, The Register (Apr. 26, 2021) [hereinafter *Emotet Self-Destructs*], https://www.theregister.com/2021/04/26/emotet_sunday_25_april_killswitch_date/ [https://perma.cc/L4YQ-9A88].

99. *Id.*

100. *Id.*; *see also* Andre Meister, *BKA uses Emotet-Takedown as a Door Opener for More Powers and New Laws*, Netzpolitik, Mar. 22, 2021, https://netzpolitik.org/2021/schadsoftware-bereinigung-bka-nutzt-emotet-takedown-als-tueroeffner-fuer-mehr-befugnisse-und-neue-gesetze/ [https://perma.cc/88F9-D2L8] ("[d]ie Betroffenen wurden nicht gefragt, ob das BKA Software auf ihren Computern ver. . .ndern soll oder nicht" [those affected were not asked whether the BKA could alter software on their computers]); EMOTET Affidavit, *supra* note 91 (making no mention of a notification process for individuals affected by EMOTET); Sven Herpig & Dennis-Kenji Kipke, *Issue: German Emotet takedown in the legal gray zone*, Transatlantic Cyber Forum (Mar. 30, 2021) (translation at https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DMar3021%E2%80%9D [https://perma.cc/J8UE-KQ3M]) (arguing that the EMOTET disruption is an example of "police general clauses [. . .] being adduced to justify intrusive official measures" that not only "erode the guarantee of a central fundamental right of the information age, but also threatens to promote increasing

They did not disclose the number of devices accessed, the IP addresses affected, nor which State actually deleted the malware from the affected individuals' computers.[101]

The underlying legal justifications presented regarding the EMOTET disruption juxtaposes States' increased willingness for extraterritorial enforcement in cyberspace against their discomfort in these uncharted waters. Each State's actions remain veiled in secrecy, as Germany, the Netherlands, and the United Kingdom have publicly released little information regarding the EMOTET takedown.[102] A partially unsealed affidavit in support of a search warrant filed by the American Federal Bureau of Investigation in the Middle District of North Carolina, however, sheds some light on the actions taken by the involved States, and the legal foundation for the enforcement.

While EMOTET's presence on devices was disrupted worldwide, including in American territory, the American affidavit references the covert access of American devices by "foreign law enforcement agents," maintaining obscurity over exactly who activated the kill switch in devices located on American territory.[103] The American affidavit qualifies the statement that "[f]oreign law enforcement agents, not FBI agents, replaced the Emotet malware," with the caveat that the U.S. government only applied for an affidavit at all "out of an abundance of caution," and not because of their direct involvement in the takedown.[104] Because "[d]isrupting a botnet from the inside by gaining control of the infrastructure has great legal

---

indifference on the part of the authorities and habitualness on the part of citizens for interventions in IT systems.").

101. *Emotet Self-Destructs*, *supra* note 98 (noting that American authorities "did not mention anything about a delayed uninstall routine" in their botnet disruption announcements); *see also* Europol Press Release, *supra* note 88; Press Release, Dep't of Just., *supra* note 88 (making no disclosure of the specifics of the disruption operation).

102. *See* Herpig & Kipke, *supra* note 100 (highlighting that information about the exact actions and nature of the EMOTET enforcement operation remains not fully public).

103. EMOTET Affidavit, *supra* note 91, ¶ 13; *see also* Lindsey O'Donnell-Welsh, *Law Enforcement Update Kills EMOTET on Infected Devices*, DECIPHER (Apr. 26, 2021), https://duo.com/decipher/law-enforcement-update-kills-emotet-on-infected-devices [https://perma.cc/2JQN-QETM] (discussing the uncertainty of which nation was behind the uninstaller).

104. EMOTET Affidavit, *supra* note 91, at 9 n. 2.

implications . . . US Department of Justice made it clear that it was 'foreign law enforcement agents.' "[105]

According to the unsealed affidavit, the United States relied upon 18 U.S.C. § 1030 (Section 1030) to legally support its actions against EMOTET.[106] Section 1030 is notable in its extraterritorial prescription, allowing the United States to bring a criminal action against an individual who "damages"[107] not only a device in the United States, but also a device "which is used in or affecting interstate or foreign commerce or communication, *including a computer located outside the United States* . . . ."[108] This language was added as an amendment through the passage of the Patriot Act in the United States,[109] and has been construed by United States' federal courts as an express grant of extraterritorial jurisdiction by Congress.[110]

The broad and opaque language of Section 1030 provides United States authorities with significant scope to act against malicious actors in cyberspace, without providing much guidance as to what is proscribed. The statute utilizes the carve out provided in Article 22 of the Budapest Convention and is at least partially at odds with the classic interpretation of territoriality.[111] Devices affecting "foreign commerce or communication" encompass most internet-connected devices worldwide, and the express grant to enforce against actors who have affected computers located outside the United States results in expansive international jurisdiction for United States authorities.[112] Still, the American request to permit *foreign* law en-

105. O'Donnell-Welch, *supra* note 103.

106. EMOTET Affidavit, *supra* note 91, ¶ 15.

107. 18 U.S.C. § 1030(e)(8) (defining damages as "any impairment to the integrity or availability of data, a program, a system, or information").

108. 18 U.S.C. § 1030(e)(2)(B).

109. USA Patriot Act of 2001, Pub. L. No. 107-56, § 814(d)(1), 115 Stat. 272, 384 (2001).

110. *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367, 374–375 (D. Conn. 2001) (finding that the plain language and legislative history of the statutory language "used in interstate or foreign commerce or communication," clearly indicated that Congress intended Section 1030 to apply extraterritorially).

111. *See* Budapest Convention, *supra* note 25, art. 22 ("This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.")

112. Ivanov, 175 F. Supp. 2d at 370 (noting that for Section 1030, despite not explicitly applying extraterritorially, "the intent to cause effects within

forcement agents to take such enforcement action in the United States extends even beyond the generous jurisdictional grant of Section 1030, which helps explain the contradictory and confusing language employed by the FBI in its affidavit in support of the search warrant.

This expansion of cyber enforcement powers is also reflected in the modern practice of the other EMOTET disruptor States and highlights the need for a new international framework in this realm. The United Kingdom has similar enforcement provisions to Section 1030 in its Intelligence Services Act[113] which could be used as legal justification to covertly delete such files from British computers.[114] And while they have been unwilling to confirm the scope of their responsibility for loading the EMOTET deletion files onto affected devices, the German Bundeskriminalamt federal police force also undertook some semblance of a deletion operation in April 2021.[115] Like the Americans, German law enforcement has obscured the specifics of the operation.[116]

---

the United States . . . makes it reasonable to apply to persons outside United States territory a statute which is not expressly extraterritorial in scope." (citation omitted)).

113. *See* Intelligence Services Act 1994, c. 13 §§ 3(1)(a)–3)(2)(b) (UK) (granting Government Communication Headquarters the power to "interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions" if the interference would be "in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Island").

114. Gareth Corfield, *Brit Authorities Could Legally Do an FBI and Scrub Malware from Compromised Boxen without Your Knowledge*, THE REGISTER (Apr. 19, 2021), theregister.com/2021/04/19/ncsc_exchange_server_legal_powers_question/.

115. *See* Herpig & Kipke, *supra* note 100 (noting that the President of the Bundeskriminalamt described the eventual deletion of the EMOTET files as an evidence preservation measure rather than a standalone enforcement action, admitting there was "no legal basis for a complete cleanup of the infected systems through emergency response measures as they are not within the current powers of the BKA.").

116. Press Release, German Bundeskriminalamt, YARA Signature to Identify the Emotet Malware (Apr. 16, 2021), https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/210416_Emotet.html [https://perma.cc/27MN-RTXM] (describing an operation for "beweissicherung," or the aptly vague "preservation of evidence").

The consistent vagueness between Europol, German, Dutch,[117] and American statements regarding the disruption shows States' dubiousness regarding the legality of the operation, both in domestic and international law. The approximate date and scale of the deletion of EMOTET webshells from infected devices was only detected by independent cyber security firms monitoring the botnet.[118] Individuals were not notified of the intrusion into their devices.[119] Exactly which State authorities accessed which devices remains unclear.[120] Furthermore, the effectiveness of the initial operation is in question, as EMOTET has now resurged as an operational botnet.[121]

One driving factor dictating the secretiveness of this operation even months after its completion is the lack of clearly defined standards and operating procedures prescribed by international law. This incentivizes States to enforce against malicious cyber actors in the shadows, without notice to the affected individuals, and without sufficient regard to the consequences of the operation.

B. *The HAFNIUM Disruption*

In the same month as the EMOTET disruption, the FBI conducted a similar operation against a different botnet, set up by a group referred to as HAFNIUM. HAFNIUM is allegedly a Chinese state-affiliated espionage group, which discov-

---

117. *See Internationale Politieoperatie LadyBird: Wereldwijd Botnet Emotet Ontmanteld*, POLITIE (Jan. 27, 2021) (only noting that with the removal of servers, and not any intrusion into personal devices).

118. Threat Intelligence Team, *Cleaning Up After Emotet: The Law Enforcement File*, MALWAREBYTES LABS (Apr. 25, 2021), https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/ [https://perma.cc/FR6K-6G38] (noting that a researcher discovered the code to remove the malware as opposed to the device owners).

119. *See* Herpig & Kipke, *supra* note 100 ("it is highly likely that the BKA has interfered – without prior knowledge or consent of the respective owners – with the integrity of the Emotet victims' computer systems. . ."); *accord* Meister, *supra* note 100 (noting that the German authorities did not notify individuals that they were affected).

120. *Emotet Self-Destructs, supra* note 98.

121. *The Return of Emotet and the Threat to the Health Sector*, U.S. DEP'T HEALTH & HUM. SERVS. 16 (June 2, 2022), https://www.hhs.gov/sites/default/files/the-return-of-emotet.pdf [https://perma.cc/VWE5-CXCJ].

ered an exploit in Microsoft Exchange email servers.[122] It installed a similar webshell to EMOTET, known as "China Chopper," on devices that were connected to Microsoft Exchange, and then used those webshells to steal the data of thousands of individuals and organizations and conduct ransomware attacks.[123]

The HAFNIUM attack illustrates two common themes among cyberattacks and responses. First, attacks often are either directly executed or at least supported by States and State actors.[124] In the absence of any effective legal framework, this seriously complicates effective enforcement, as takedowns of command-and-control servers may potentially double as counterattacks on hostile governments. Certain States use this ambiguity to their advantage in the international system, simultaneously decrying extraterritorial enforcement efforts while supporting this type of attack.[125]

Second, like the EMOTET operation, the HAFNIUM disruption shows American law enforcement's willingness to go beyond the traditional criminal punishment authorized under

---

122. *UK and Allies Hold Chinese State Responsible for Pervasive Pattern of Hacking*, UNITED KINGDOM NATIONAL CYBER SECURITY CENTRE (July 19, 2021), https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking [https://perma.cc/CE2H-73Q8].

123. *See* Joshua Deacon, *HAFNIUM, China Chopper and ASP.NET Runtime*, SPIDERLABS BLOG (Mar. 15, 2021), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hafnium-china-chopper-and-aspnet-runtime/ [https://perma.cc/WWH8-D25A] (describing how "China Chopper" operates); *see also* Alex Hern, *What is the Hafnium Microsoft Hack and Why Has the UK Linked it to China?*, The Guardian (July 19, 2021) ("[i]n March, tens of thousands of organisations around the world discovered their private internal discussions had been cracked open and lain bare by a group of Chinese hackers.").

124. *See* Michael McGuire, *Nation States, Cyberconflict and the Web of Profit*, HP WOLF SECURITY 8 (Apr. 8, 2021), https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf [https://perma.cc/XB8D-FLTW] ("Nation States now use digital networks to aggressively compete for influence in ways which often stand outside the usual norms of conduct. . . .").

125. *See, e.g.*, David Ignatius, Opinion, *Russia and China's Hypocritical Attempt to Control Cyberspace*, WASH. POST (July 20, 2021, 5:50 PM), https://www.washingtonpost.com/opinions/2021/07/20/russia-china-are-trying-control-internet-even-they-censor-it/ [https://perma.cc/ABG4-9BEP] (highlighting the simultaneous rise in cyberattacks originating from Russian and Chinese territory with their efforts to spearhead new internet governance frameworks).

Section 1030.[126] While the FBI was unable to access the command-and-control server, given its likely location in the Chinese mainland, in April 2021 the FBI did get court authorization to secretly access thousands of American devices, deleting data and files HAFNIUM had installed.[127] The FBI relied on a combination of Section 1030 and Federal Rule of Criminal Procedure 41 in the HAFNIUM disruption to surreptitiously remove malware from infected devices in the United States, taking an even further step than in the EMOTET disruption.[128] The procedural rule under which the search warrant was filed allows for the "search and seizure" of evidence, and permits a judge in a Section 1030 case to authorize law enforcement to "use remote access to search electronic storage media and to seize or copy electronically stored information."[129]

Construing this provision as a grant to *delete* information, even if that information is malware, from unsuspecting individuals' devices stretches the logical interpretation of the Rule to its limits.[130] And yet, in both the HAFNIUM and EMOTET cases, the FBI did just that. In EMOTET, on behalf of a "trusted foreign law enforcement partner,"[131] and in HAFNIUM on its own. While both search warrants cite "damage" to the devices as the motivation for the botnet disruption, they are sparse on exact details of how each individual computer was damaged.[132]

---

126. *See* Joel Schwartz, *The FBI's New Malware Eradication Service Is on Thin Legal Ice*, BLOOMBERG L. (May 13, 2021, 4:00 AM), https://news.bloomberglaw.com/us-law-week/the-fbis-new-malware-eradication-service-is-on-thin-legal-ice [https://perma.cc/SNA4-XNL9] (describing how an FBI operation to remove malicious software from private servers would ordinarily be criminal under Section 1030).

127. Affidavit in Support of an Application Under Rule 41(b)(6)(B) For a Search Warrant ¶ 20, *in re* The Search of Certain Microsoft Exchange Servers Infected with Web Shells, No. 4:21mj755 (S.D. Tex. Apr. 9, 2021).

128. *Id.* ¶¶ 18, 20.

129. FED. R. CRIM. P. 41(b)(6).

130. Lubin & Marinotti, *supra* note 9 (noting that expanding Rule 41 to cover "remote and nonconsensual mass cleanup . . . is quite a dramatically expansive interpretation"); *see also* Schwartz, *supra* note 126 (noting the premise of the 2016 amendment to Rule 41 was "not to clean and secure victim computers").

131. EMOTET Affidavit, *supra* note 91, ¶ 20.

132. *Id.* ¶ 15 ("The infected computers have been 'damaged' within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the Emotet

What is clear is that the latitude of these enforcements extended far beyond past enforcement operations against botnets.[133] Prior operations were expressly limited to seizing the command-and-control server and notifying affected individuals of the presence of malware on their devices.[134] These new operations not only potentially fall afoul of the Budapest Convention,[135] they also raise serious questions about what the limitations of enforcement are in cyberspace.

Malware-as-a-Service crimes like the HAFNIUM and EMOTET attacks are primarily done outside of the public eye, with perpetrators' identities and intent easily masked.[136] With the absence of an effective international legal framework, State responses increasingly follow the same model, enforcing without public discourse or oversight. This creates three salient problems. First, while the EMOTET and HAFNIUM disruptions hampered the operation of dangerous botnets, they created precedent that is easily abused, as States could con-

---

malware has impaired the integrity and availability of data, programs, systems, and information on the infected computers.").

133. *See* Office of Sen. Sheldon Whitehouse, *International Cybercrime Prevention Act of 2021: Section by Section Analysis* (2021), https://www.whitehouse.senate.gov/imo/media/doc/International%20Cybercrime%20Prevention%20Act%20of%202021%20Section-by-Section.pdf [https://perma.cc/VAZ2-PMXR] (noting that "[u]nder current law, DOJ's authority to obtain injunctive relief to shut down botnets is limited to those botnets engaged in fraud or illegal wiretapping" and not denial of service, destruction of data, or other crimes); *see also* Miriam H. Wugmeister et al., *DOJ Takes Novel Action to Remove State-Sponsored Hacking Group's Malicious Code from U.S. Victim Computers*, Morrison Foerster Client Alert (Apr. 15, 2021), https://www.mofo.com/resources/insights/210415-doj-takes-novel-action.html [https://perma.cc/6JX4-BPKG] (highlighting the unprecedented nature of the HAFNIUM enforcement).

134. *See* Alex Iftimie, *No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims*, Lawfare Blog (Apr. 19, 2021, 4:07 PM), https://www.lawfareblog.com/no-server-left-behind-justice-departments-novel-law-enforcement-operation-protect-victims [https://perma.cc/55H5-VY29] (discussing how disruptions prior to the HAFNIUM operation had been much more limited in scope).

135. Budapest Convention, *supra* note 25, art. 19(5) (noting that all search and seizure operations are subject to Article 15's human rights provisions).

136. François Delerue, Cyber Operations and International Law 145–48 (2020) (using a 2007 denial-of-service attack in Estonia as an illustration of the impediments to accurately identifying the perpetrators of an international cyberattack).

duct such "cleaning operations" against dissidents or other disfavored denizens of the internet.[137] Second, the wholesale accessing of infected devices, including surreptitiously loading and deleting data, potentially constitutes infringement of the right to privacy and the freedom from arbitrary interference with the home.[138] Finally, while there is no evidence of the EMOTET or HAFNIUM disruptions damaging any of the infected devices, more frequent use of such tactics may result in damage to personal devices "due to some unforeseeable circumstances, such as unique or unusual configuration of the compromised machine."[139]

The need for international law in this space is evident. States are constantly under threat from unforeseen places and actors; simultaneously, individuals' rights are in a more precarious position than ever as States exert more control in this new global commons. If the recent resurgence of EMOTET's activities indicates anything, it is that to be effective, enforcement operations may require a more heavy-handed approach. This means more risk to individuals and States, and the potential for greater fallout from covert cyberoperations. As awareness of the problem grows, public and private actors are calling for revising the framework for cyber enforcement,[140] and the system is ripe for the implementation of an updated regime.

IV. Updating the Framework for Cyber Operations

The current rules governing cyberspace, as demonstrated by both the rise in cyberattacks and the increasing scope of

---

137. Scott Ikeda, *Emotet Malware Taken Down by Global Law Enforcement Effort, Cleanup Patch Pushed to 1.6 Million Infected Devices,* CPO Mag. (Apr. 30, 2021), https://www.cpomagazine.com/cyber-security/emotet-malware-taken-down-by-global-law-enforcement-effort-cleanup-patch-pushed-to-1-6-million-infected-devices/ [https://perma.cc/D2WQ-RKWB].

138. ICCPR, *supra* note 38, art. 17; *see also* ACLU Proposal, *supra* note 41, at 16 (discussing the potential for privacy violations due to "modern technology [. . .] that were not foreseeable during the drafting of General Comment 16.").

139. Ikeda, *supra* note 137.

140. *See e.g.*, Paris Call for Trust and Security in Cyberspace (Nov. 12, 2018), https://pariscall.international/en/call [https://perma.cc/9PDX-KKEU] (demonstrating the international support for revising the cyber enforcement framework).

State action in response to those attacks, are deficient in three ways. First, they fail to provide States with guidelines on when and how to enforce against cyberattacks. Second, they do not adequately protect individual or States' rights in cyberspace. And third, they do not provide any effective recourse in response to violations of rights. In May and June 2022, 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) convened to discuss a potential new framework to address the evolution of cybercrime since the passage of the Budapest Convention.[141] For this new treaty to be effective, however, it must address these three issues.

Several potential additions to the cybercrime regime would help ensure both States' rights to enforce and individuals' rights to privacy and noninterference with their information. First, States should enshrine the "substantial effects" jurisdiction proposed by the Tallinn Manual as the new limit for extraterritorial enforcement in cyberspace. Second, States should incorporate a "least intrusive means" test as a measure of proportionality both for jurisdiction and the safeguarding of individuals' rights when enforcing against cyberattacks. Third, States should adopt a new protocol setting up a review committee to hear complaints regarding violations occurring out of cyber operations.

The potential for updating the cyber enforcement framework could follow two tracks. First, the intentionally neutral language of the Budapest Convention may allow for updating the standards of territoriality and human rights without negotiating an entirely new instrument.[142] An entirely new treaty on cybercrime is also a possibility, and the Ad Hoc Committee composed of experts and State representatives has met three times in 2022 to begin negotiating a new multilateral instrument.[143] Engagement in these deliberations has thus far been

---

141. *See* G.A. Res. 74/247, ¶ 2 (20 January 2020) (establishing the Ad Hoc Committee); *see also* AHC, Annotated Provisional Agenda ¶ 1, U.N. Doc. A/AC.291/8 (detailing dates and agenda of the meeting).

142. *See* Explanatory Report, *supra* note 37, ¶ 36 ("[T]he Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.").

143. The Ad Hoc Committee held its first session from 28 February 2022 to 11 March 2022, its second session from 30 May 2022 to 10 June 2022, and

successful; even Russia and China, despite their recent aversion to new multilateral treaties, have participated in the early negotiations, though some experts have questioned whether their proposals would undermine the rules-based order, rather than bolster it.[144] Regardless, the changes to the system proposed below are feasible through either process and could be incorporated into the Budapest Convention or into any new agreement negotiated on point.

A. *Substantial Effects as a Grant of Jurisdiction*

One crucial update to the cyber enforcement framework is the recognition of the impossibility of using a traditional territoriality framework in a world of botnet attacks. A narrow view of territoriality, limiting States to enforcing against botnets which originate in their territory, would hamstring the ability to prevent such attacks, and would be inapposite to States' policies of defending their national interests.[145] A *de minimis* test, however, would essentially allow States with high traffic in data, like the United States, China, the members of the European Union, and others to enforce against every infraction, given the likelihood of a cloud-based cyberattack at least "passing through" those jurisdictions at some point in its lifecycle.

Instead, States should incorporate the Tallinn Manual's "substantial effects" jurisdictional test into any new cyberspace framework. This approach would reflect the majority of State practice in this area, and would ensure that States are able to

---

its third session from 29 August 2022 to 9 September 2022. Three additional meetings will be held in 2023. G.A. Dec. 76/552, U.N. Doc. A/76/49 (Vol. III), at 222 (Jan. 20, 2022).

144. Allison Peters, *Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime*, FOREIGN POLICY (Sept. 19, 2019), https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/ [https://perma.cc/9K9L-FSBR]; *see also* Deborah Brown, *Cybercrime is Dangerous, but a New UN Treaty Could Be Worse for Rights*, JUST SECURITY (Aug. 13, 2021), https://www.justsecurity.org/77756/cybercrime-is-dangerous-but-a-new-un-treaty-could-be-worse-for-rights/ [https://perma.cc/FB9J-BXAR] (discussing how Russia's proposed cybercrime treaty "could criminalize free expression and undermine privacy").

145. Schmitt, *Defense of Sovereignty*, *supra* note 22 (noting that that applying a more relaxed sovereignty principle in cyberspace "affords states a greater margin of appreciation within which to conduct operations they deem crucial.").

respond to cyberthreats without unduly burdensome restrictions regarding consent, or recourse to the U.N. Security Council.[146] The aforementioned problems with attribution, and State-sponsored cyber intrusions masquerading as rogue attacks, means that maintaining absolute sovereignty in cyberspace is untenable,[147] but the use of a "substantial effects" standard rather than a *de minimis* test would provide some protection against overenforcement. One potential guideline is that proposed to the Ad Hoc Committee by India, referred to as "data-oriented jurisdiction."[148] This proposal would allow for extraterritorial enforcement by a State if an offense is: "committed outside its territory with a view to the commission of an offence established in accordance with this Convention within its territory;" "[t]he offence is committed targeting computer resources located within its territory;" or "[t]he offence involves the digital/electronic data of their nationals, irrespective of the place of its physical storage/processing/screening/federation."[149] This effects-based jurisdiction reflects a more realistic understanding of the modern cloud-based system and the growing necessity of fighting botnet crimes originating from outside a State's national territory. Still, most participating States have maintained the primacy of sovereignty as an element of their proposals on a new cybercrime convention and reconciling expanded jurisdiction with territorial sovereignty is a stumbling block the Ad Hoc Committee will have to overcome.

China, at first glance, would appear to be reticent to agree to such a proposal. Despite the interminable development of interwoven connections between China and other States in the digital sphere, the Chinese government maintains that "the principle of sovereignty enshrined in the UN Charter covers

146. *See* Corn & Taylor, *supra* note 20, at 211 (hypothesizing that the U.S. does not need the host state's consent before taking actions against ISIS cyber facilities within the host state).

147. *See id.* at 210 (arguing that a universal rule of sovereignty has no clear application to the domain of cyberspace).

148. AHC, Compilation of Proposals and Contributions Submitted by Member States on the Provisions on Criminalization, the General Provisions and the Provisions on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes, Submission of India ¶ 14, U.N. Doc. A/AC.291/9/Add.3 (May 16, 2022).

149. *Id.*

all aspects of state-to-state relations, which also includes cyberspace," and maintains that there is no room for extraterritorial action in cyberspace.[150] However, in the most recent round of negotiations on a new cybercrime instrument, Russia, on behalf of China and several other nations, proposed a provision allowing States to exercise jurisdiction over cybercrime if "[t]he offence 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."[151]

The obvious worry is the potential abuse of such jurisdiction. Russia's proposal contains no mention of the principle of proportionality, and while it obliquely mentions the safeguards of the ICCPR, it also includes the *caveat* that "*[t]o the extent that it is consistent with the public interest*, in particular as regards the administration of justice, the State Party shall consider the impact of the powers and procedures provided for in this section on the rights, responsibility and legitimate interests of third parties."[152] Especially following the invasion of Ukraine, this clause should be viewed critically, and the deficiencies in Russia's proposal highlight the importance of balancing any jurisdictional expansion with substantive and actionable human rights protections.

B. *A "Least Intrusive Means" Test to Protect States' and Individuals' Rights*

To balance this new affirmative grant of jurisdiction, the new conceptualization of cyber enforcement should also adopt a "least intrusive means" test for States to assess whether acces-

---

150. *International Strategy on Cooperation in Cyberspace*, MINISTRY OF FOREIGN AFFS. OF THE PEOPLE'S REPUBLIC OF CHINA (Mar. 1, 2017), https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html [https://perma.cc/SG6K-QC28].

151. AHC, Compilation of Proposals and Contributions Submitted by Member States on the Provisions on Criminalization, the General Provisions and the Provisions on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Submission of the Russian Federation Art. 39, ¶ 2, U.N. Doc. A/AC.291/9/Add.2 (Apr. 21, 2022) [hereinafter Second Session State Submissions].

152. *Id.* art. 32 ¶ 3 (emphasis added).

sing individuals' devices without consent is an appropriate response to a botnet attack.[153] This can even be accomplished using the existing framework of the Budapest Convention, through its use of "proportionality" as a component of Article 15.[154]

The test would entail a fact-specific analysis of the goals and implementation of any pertinent measure adopted by a State, and would require the State to show that "of all the instruments that could be chosen to achieve the aims pursued, that instrument . . . selected . . . is least problematic from the perspective of the individual rights at stake."[155] Such a test is commonly applied in situations where rights are limited in response to some social need, and the United States Supreme Court,[156] the German Constitutional Court,[157] and the Court of Justice for the European Union (the CJEU)[158] all use it as a measure of necessity, proportionality, and legality when reviewing State action. The CJEU has instituted a high bar of proportionality for access to individuals' data and devices, permitting it only when the data access "taken as a whole[ ] allows

153. The least intrusive means test is used as an assessment of proportionality for protecting several other rights and freedoms. *See, e.g.*, U.N. Human Rights Committee, General Comment No. 34, ¶ 34, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011) (discussing the test's application with regard to the right to the freedom of expression).

154. Budapest Convention, *supra* note 25, art. 22.

155. Janneke Gerards, *How to Improve the Necessity Test of the European Court of Human Rights*, 11 INT'L J. CONST. L. 466, 482 (2013).

156. *See, e.g.*, Shelton v. Tucker, 364 U.S. 479, 488 (1960) (noting that "[t]he breadth of legislative abridgment must be viewed in the light of less drastic means for achieving the same basic purpose.").

157. Dieter Grimm, *Proportionality in Canadian and German Constitutional Jurisprudence*, 383 UNIV. TORONTO L. J. 383, 387 (2007) (noting that when reviewing fundamental rights limitations, "the German Court asks whether the law is necessary to reach its end or whether a less intrusive means exists that will likewise reach the end.").

158. *See, e.g.*, Case C-58/08, Vodafone Ltd. v. Sec'y of State for Bus., Enter., & Regul. Reform, 2010, E.C.R., I-5026, ¶ 51 ("the principle of proportionality is one of the general principles of Community law and requires that measures implemented through Community law provisions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and must not go beyond what is necessary to achieve them.").

very precise conclusions to be drawn concerning the private lives of the persons concerned."[159]

While the Ad Hoc Committee has yet to directly field a proposal for the inclusion of a "least intrusive means" test into the new potential cybercrime convention, several States' proposals reference incorporating into the treaty any "rights arising pursuant to obligations it has undertaken under the International Covenant on Civil and Political Rights, and other applicable international human rights instruments, [including] the principle of proportionality."[160] A similar test is promulgated as part of the International Covenant on Civil and Political Rights' requirements for State limitations on freedom of speech, religion, and other fundamental rights, and therefore its inclusion into the cybercrime regime is feasible.[161]

This test would be utilized in two ways. First, in assessing the extension of jurisdiction into another State's territory, State action would be examined on the basis of whether other enforcement mechanisms without such an extraterritorial incursion present a reasonably effective alternative option.[162] States would also have to demonstrate the value of the goals underlying the enforcement operation.[163] A takedown of a botnet virulently spreading malware around the world, including in a State's territory? Likely acceptable. An attempt to take down opposition media operating in another State's territory? Not acceptable, even if the distributed media does have a substantial effect in the acting State's sovereign territory.

---

159. *See* Case C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:788, ¶ 54 (Oct. 2, 2018) (indicating that only the objective of serious crime fighting justifies the need to access personal data).

160. Second Session State Submissions, *supra* note 151, at 6, 19, 23, 45, 48 (included in the submissions of Brazil, European Union, Ghana, the United Kingdom, and Switzerland).

161. *See, e.g.*, ICCPR, *supra* note 38, art. 18(3) (requiring limitations of the right to freedom of religion to be "necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others."). This clause is interpreted by the Human Rights Committee to require limitations to be proportional. *See, e.g.*, U.N. Hum. Rts. Comm. [UNHRC], General Comment No. 22, ¶ 8, CCPR/C/21/Rev.1/Add.4 (July 30, 1993) ("[l]imitations may be applied only for those purposes for which they were prescribed and must be directly related and proportionate to the specific need on which they are predicated.").

162. Grimm, *supra* note 157, at 387–8.

163. *See* Gerards, *supra* note 155, at 486–87.

Second, the same test should be applied to the rights of individuals, especially in situations like the HAFNIUM and EMOTET attacks. It may be that a covert intrusion into individual devices to destroy the nodes of a malicious botnet *was* the least intrusive effective means toward achieving the legitimate aim of stopping these botnets. If, however, simply notifying the affected IP addresses of the infection on their system or requiring notice and consent by the individuals before deletion would have been equally effective methods of combatting these botnet attacks, as they had been in several previous enforcement operations,[164] then the HAFNIUM and EMOTET operations would fall afoul of this requirement. Therefore, applying this definition of proportionality requires State actors to consider whether they have "duly respected the obligation to make a reasoned and well-informed choice for a certain means."[165] For individuals, the inclusion of such a test as a protection of rights would also provide a defined mechanism for legal probing of whether an operation has violated human rights standards, whether at a regional human rights court or a potential review committee hearing.[166]

Part of the value of a least intrusive means test is forcing State actors to inspect their own processes: when the law requires a review of feasible alternatives as a necessary component of legality, it facilitates more comprehensive review by governments.[167] As an added benefit, whether or not negotiations for a new instrument are successful, this test is incorporable into the existing Budapest Convention framework, through Guidance Notes or other agreement of the Parties. Proportionality as noted in Article 15, though currently undefined, could include application of a "least intrusive means" test.[168] The Budapest Convention's provisions on the search

---

164. *See* Iftimie, *supra* note 134 (describing past enforcement operations such as the 2011 Coreflood disruption).

165. Gerards, *supra* note 155, at 487.

166. *See infra*, Part IV-C.

167. Ireland v. The United Kingdom, App. No. 5310/71, ¶ 154 (Jan. 18, 1978), https://hudoc.echr.coe.int/eng?i=001-57506 [https://perma.cc/GS7P-5AP3] (holding that the benefit of this formulation of proportionality is to "elucidate, safeguard and develop the rules . . . thereby contributing to the observance by the States of the engagements undertaken by them as Contracting Parties.").

168. Budapest Convention, *supra* note 25, art. 15.

and seizure of data also affirmatively incorporates Article 15's proportionality requirement, meaning this formulation would apply in botnet disruption operations.[169] Regional human rights courts, the WTO Appellate Body, and the Human Rights Committee apply proportionality using this type of test (in addition to the aforementioned national and E.U. courts),[170] and the U.N. Group of Governmental Experts recognized the application of proportionality with regards to international security in cyberspace.[171] Incorporating a "least intrusive means" test as a codified element of proportionality in cyberspace would therefore be an effective counterweight to a "substantial effects" jurisdiction grant and would limit States' cyber operations accordingly.

C. *An Optional Protocol for the Review of Complaints*

Finally, to operationalize the "least intrusive means" test, the Parties to the Budapest Convention should adopt a third additional protocol[172] to the treaty which allows the Cybercrime Convention Committee to hear individual complaints regarding violations of human rights in cyberspace. In the alternative, the Ad Hoc Committee should introduce such a protocol contemporaneously to the conclusion of a new treaty, to ensure the effective enforcement of its substantive provisions. States are already, under the terms of the Budapest Convention, permitted to submit disputes between each other to the

---

169. *Id.* art. 19(5).

170. *See, e.g.* Hatton v. United Kingdom, App. No. 36022/97, ¶ 86 (July 8, 2003), https://hudoc.echr.coe.int/Eng?i=001-61188 [https://perma.cc/L3VW-A9RC] ("The Chamber considered that States were required to minimise, as far as possible, interference with Article 8 rights, by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous way as regards human rights."); Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (Apr. 7, 2005), ¶¶ 309–11 (discussing how States must treat alternative measures under the WTO's General Agreement on Trade in Services); General Comment No. 27, *supra* note 35, ¶ 14.

171. GGE Report, *supra* note 21, ¶ 28(d).

172. The first two additional protocols to the Budapest Convention concern the criminalization of acts of a racist and xenophobic nature and enhanced cooperation and disclosure provisions. Additional Protocol to the Convention on Cybercrime, Jan. 28, 2003, E.T.S No. 189; Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, May. 12, 2022, E.T.S. No. 224.

European Committee on Crime Problems, the International Court of Justice, or an arbitral tribunal.[173] Providing a forum for individuals to bring complaints would harden the human rights obligations under the Convention and would provide "interpretative guidance to the national authorities in order to help them carry out their primary task of safeguarding fundamental rights."[174] While this mechanism has yet to be proposed in the initial negotiations of the new cybercrime regime, its inclusion is essential to counterbalance expanding grants of jurisdiction to States purporting to combat cybercrime.

The structure of this protocol would be similar to that of the first Optional Protocol to the ICCPR, which allows the Human Rights Committee "to receive and consider . . . communications from individuals claiming to be victims of violations of any of the rights set forth in the Covenant."[175] Both the Convention on the Elimination of Discrimination Against Women and International Covenant on Economic, Social and Cultural Rights have adopted similar protocols for the review of individuals' complaints of rights violations.[176]

Generally, under such protocols, once an individual has exhausted domestic recourse for remedy for a violation, they may bring a complaint to the Committee, which then reviews the submission, brings it to the attention of the accused State, and provides its recommendations on the issues involved.[177] The process is particularly useful for emerging bodies of law like that of cyberspace, as it both encourages States to review their actions more diligently, and also "enable[s] the adjudicating body to study concrete cases and thus enable[s] it to

---

173. Budapest Convention, *supra* note 25, art. 44.

174. Gerards, *supra* note 155, at 468.

175. First Optional Protocol to the International Covenant on Civil and Political Rights, art. 1, *opened for signature,* Dec. 16, 1966, 999 U.N.T.S. 302 (entered into force Mar. 23, 1976).

176. Optional Protocol to the Convention on the Elimination of All Forms of Discrimination Against Women, *opened for signature* Dec. 10, 1999, 2131 U.N.T.S. 83 (entered into force Dec. 22, 2000); Optional Protocol to the International Covenant on Economic, Social and Cultural Rights, *opened for signature* Sept. 24, 2009, 2922 U.N.T.S. 29 (entered into force May 5, 2013).

177. *What is an Optional Protocol?,* U.N. WOMEN, https://www.un.org/womenwatch/daw/cedaw/protocol/whatis.htm [https://perma.cc/AUP3-ZA98] (last visited Oct. 22, 2022).

create a more concise jurisprudence."[178] This procedure would allow for complementarity between international adjudicatory bodies, as its members would be better equipped than the Human Rights Committee to handle the technologically complicated subject matter of infringements in cyberspace.[179]

A slightly different hypothetical to the EMOTET disruption shows the utility of this procedure. If the enforcing States had made a miscalculation in determining that a cyber operation would not have adverse effects on peoples' devices,[180] the submission of individual complaints to a Cybercrime Convention Committee would ensure some outlet of recourse for individuals. Even if national agencies disclaimed responsibility for the operation in their own courts, as the FBI did in the EMOTET disruption, there would still be an accessible forum for some type of reparation.

Like the expansion of jurisdiction, however, the main obstacle for establishing this complaint resolution protocol would be resistance by States Parties. The optional protocols to the ICESCR, ICCPR, and CEDAW have all struggled to gain the support of powerful States, including the United States (which is not a party to either ICESCR or CEDAW, nor the first Optional Protocol to the ICCPR).[181] However, the goal of this protocol would be to start with an initially small but influential community and bolster the rules-based order over time. Many countries, including the European States, Turkey, the Philippines, Canada, Chile, Argentina, and others are all parties to

---

178. Rep. of the Open-Ended Working Grp. to Consider Options Regarding the Elaboration of an Optional Protocol to the Int'l Covenant on Econ., Social and Cultural Rights on its First Session, ¶ 23, U.N. Doc. E/CN.4/2004/44 (Mar. 15, 2004).

179. John Tobin, *Seeking Clarity in Relation to the Principle of Complementarity: Reflections on the Recent Contributions of Some International Bodies*, 8 MELBOURNE J. INT'L L. 356, 370 (2007) (discussing the benefits of "the capacity for individuals to make use of the individual complaint mechanisms that exist under several treaties and regional human rights systems.").

180. *See* Ikeda, *supra* note 137 (noting the possibility of a miscalculation damaging individuals' devices).

181. *See, e.g.,* Marie Wilken, *U.S. Aversion to International Human Rights Treaties*, GLOB. JUST CTR. (June 22, 2017), https://globaljusticecenter.net/blog/773-u-s-aversion-to-international-human-rights-treaties [https://perma.cc/JSG8-X46A] (illustrating that U.S.'s failure to ratify the first Optional Protocol to the ICCPR has undermined the aggrieved citizens' ability to rely on international protections).

both the Budapest Convention and the First Optional Protocol to the ICCPR,[182] suggesting there might be a wide enough base at the outset to make this complaint procedure effective.

This is one area where the interconnectedness of data and enforcement bolster the procedure. Given the need for cooperation among States to enforce against botnet attacks, as shown by the EMOTET disruption, even operations undertaken by potential non-signatories like the United States would likely be subject to at least partial review because of cooperation contributions by other States.[183] Allowing for individual complaint review is not a panacea to the ills of cyber operations, but it would make human rights in cyberspace a more enforceable regime and would force States to scrutinize their actions more thoroughly before enforcing against cybercrimes.

V. Conclusion

The proliferation of botnet attacks has brought about a destabilization of the international law of cyberspace, combining an increased threat of attack to individuals, corporations, and State actors, with bold new assertions of enforcement jurisdiction in response. While international law is often slow to develop, this is the very type of problem it was meant to address: ensuring States can effectively protect their nationals and interests through collective action, while safeguarding the fundamental protections enjoyed by both other States and individuals.[184] EMOTET and HAFNIUM reveal the problem in a

182. Budapest Convention Parties, *supra* note 24; *Status of Ratification of the First Optional Protocol to the ICCPR*, U.N. Off. of the High Comm'r for Hum. Rts., https://indicators.ohchr.org [https://perma.cc/4SP5-KT3S] (last updated Mar. 9, 2022).

183. An analogous situation is that of CIA extraordinary rendition cases litigated before the European Court of Human Rights. Though the United States is not a signatory to the European Convention on Human Rights, and itself did not grant any remedy to individuals who had been extraordinarily rendered to CIA black sites for interrogation, the involvement of European partners and their legal obligations resulted in at least some legal recourse for affected individuals. *See, e.g.*, Nasr v. Italy, App. No. 44883/09 (Feb. 23, 2016), https://hudoc.echr.coe.int/eng?i=001-113123 [https://perma.cc/PL7W-DGMB] (ruling in favor of the applicants and awarding EUR 70,000 to one and EUR 15,000 to the other plus any amount due as tax).

184. *See* Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, International Law in Cyberspace (Sept. 18, 2012) *in* 54 Harv. Int. L.J. Online 1, 10

nutshell. While States act to protect their interests from attack, the solution threatens to swallow the problem, and presents a threat to the rules-based order.

The Budapest Convention and Tallinn Manual are not perfect, but they do represent a foundation on which this paper's proposals aim to build. Codifying jurisdiction principles in cyberspace provides needed guidance to States on when they may undertake cyber operations, and the introduction of "least intrusive means" as an element of proportionality, as well as an individual complaint mechanism, would serve to safeguard rights in the face of expanding jurisdiction. As negotiations continue for the next several years on a new cybercrime framework, balancing any new jurisdictional grant with safeguarding human rights should be an essential component of the Ad Hoc Committee's mandate.

These solutions will not fix everything. The Human Rights Committee's role in this realm should not be understated, and the need for clarification on the applicability of civil and political rights in cyberspace looms over the entire regime. And while changes to the regime may make some parties more interested in acceding, the failure of the Budapest Convention to gain widespread acceptance in Africa and Asia underscores the work left to be done.[185] In this respect, the ongoing negotiations of the Ad Hoc Committee reflects progress, as dozens of African and Asian States are participating in the ongoing negotiation process.[186] The changes proposed in this paper present a plausible evolution of the cyberspace enforcement regime, incorporable into a new treaty on cybercrime, and would serve to buttress the international order in the increasingly tumultuous frontier of cyberspace.

(Dec. 2012), https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf [https://perma.cc/48G7-UJAF] (arguing that "[c]ompliance with international law . . . can only free us to do more, and to do more legitimately, in the emerging frontiers of cyberspace").

185. In Africa, just Mauritius, Senegal, Ghana and Cabo Verde have ratified the Budapest Convention, while in Asia, the only ratified Parties are Azerbaijan, Georgia, Japan, the Philippines, Sri Lanka, and Turkey. *See* Budapest Convention Parties, *supra* note 24.

186. *See generally* AHC, Second Session List of Participants, U.N. Doc. A/AC.291/INF/4 (June 8, 2022) (listing several Asian and African State participants at the second session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes).