The Prohibition on Extraterritorial Enforcement Jurisdiction in the Datasphere

Handbook on Extraterritoriality in International Law (Austen L. Parrish and Prof. Cedric Ryngaert eds., forthcoming, 2022)

Dr. Asaf Lubin[1]

Introduction

Criminal perpetrators are increasingly dependent on computers and media devices when planning and executing their illicit activities. This change has affected the way criminal investigations are conducted in the 21st century. Our modern-day law enforcement officers are now best described as "cyber constables," forced to master an ever-evolving ecosystem of digital forensic investigations. As the United States Department of Homeland Security (DHS) has noted, criminal and national security investigations now routinely involve information from a wide assortment of internet connected devices. From smart phones to email servers to fitness trackers, these devices "may contain vital evidence—such as user information, call logs, locations, text messages, emails, images or audio and video recordings—that could lead to the arrest of criminals."[2] It is for this reason that in the mid-2010s DHS launched the "Cyber Security Forensics Project" which joined investigators from local, state, and federal agencies with their international partners to develop new technological solutions for fighting crime and terrorism in the digital age.[3]

One obvious area in which innovation in digital investigations is most urgently needed is in the fight against cybercrime. The COVID-19 pandemic further exacerbated societies' reliance on remote communication tools and demonstrated just how vulnerable we have become to falling prey to malicious cyber activity.[4] The past year has seen yet another disturbing rise in cyber calamities including ransomware and supply chain attacks, data breaches, interreference in elections, and misinformation campaigns.[5] Against this backdrop our new cyber constables have proven mostly ineffective. Much has already been written about the "Cyber Enforcement Gap" which refers to the large difference between the number of malicious cyber incidents per year and

---

[1] Dr. Asaf Lubin is an Associate Professor of law at Indiana University Maurer School of Law and a Fellow at IU's Center for Applied Cybersecurity Research (CACR). He is additionally an affiliated fellow at Yale Law School's Information Society Project, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, and a visiting Scholar at the Hebrew University of Jerusalem Federmann Cyber Security Research Center. I wish to thank Dean Austen L. Parrish and Prof. Cedric Ryngaert for editing and putting together this handbook. I also wish to thank the participants of the three-day conference for their feedback on an earlier draft paper, and in particular to the moderator and participants of workshop #3, Hannah Bauxbaum, Dan Jerker B. Svantesson, Christopher Kuner, Timothy Holbrook, and Marek Martyniszyn. I also wish to thank Tim Cochrane for useful guidance and advice.

[2] DHS Science and Technology directorate, 'Cyber Security Division cyber Security Forensics Project' (DHS.gov, 12 October 2017) <https://www.dhs.gov/sites/default/files/publications/FactSheet_Cybersecurity%20Forensics%20One%20Pager%20FINAL_508.PDF> accessed 4 September 2021.

[3] *Id*.

[4] François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace' in T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.), *13th International Conference on Cyber Conflict: Going Viral*, 12 (NATO CCDCOE 2021) (noting that the pandemic has been particularly marked "by an important increase in the number of threats and operations in cyberspace.").

[5] *See e.g.* Bizclik Admin, '10 High Profile Cyber Attacks in 2021' (Cyber Magazine, 21 June 2021) <https://cybermagazine.com/top10/10-high-profile-cyber-attacks-2021> accessed 4 September 2021.

the number of investigations opened by law enforcement to bring the perpetrators of these attacks to justice.[6] In fact, one study found that "less than 1 percent of the cyber incidents that occur annually in the United States result in an actual arrest."[7]

As Peter Swire and Susan Brenner have both demonstrated, one of the root causes of cybercrime underenforcement is the transnational character of the offences and their method of execution. Not only are perpetrators "physically distant" from their victims,[8] but they also employ technologies that allow them to further conceal their identity and spoof[9] their way through multiple servers, networks, and devices. As a result, evidence relating to the crime is difficult to pin down, as it is both "everywhere and anywhere."[10] The ubiquitous features of internet communications—their "mobility, interconnectedness, and divisibility"[11]—introduce even further technical and legal complications on these investigations.

What prevents law enforcement from extending their long arm to the edges of the world wide web? According to the traditional view, the answer is the prohibition on extraterritorial enforcement jurisdiction, a doctrine that was born alongside the Westphalian legal order in 1648. As was articulated by the Permanent Court of International Justice (PCIJ) in the *Lotus* case: "the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not **exercise its power in any form in the territory of another State**."[12] The doctrine therefore prohibits law enforcement agents in State A from unilaterally entering State B and abducting a person or seizing documents as part of their criminal investigation.[13] Such use of coercive power across territorial lines, it is argued, will "shatter[] the sacrosanct principle of sovereign equality of nations."[14]

But the *Lotus* case is nearly a century old. Can a collision between two steamers on the high seas in 1926 really teach us something of value about internet governance in 2021? After all, the very notion of the "datasphere," where these cyber investigations take place, is bifurcated. On the one hand, we may conceptualize our datasphere in physical terms insomuch as it encompasses end-devices, cables, servers, routers, and networks through which we generate, process, and

---

[6] Allison Peters & Amy Jordan, 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime' [2020] 10 JNSLP 487, 492.

[7] *Id*. Note that the authors define cyber incidents as "malicious cyber incidents reported to the FBI each year"; presumably the gap is much larger if you also consider unreported cyber incidents, both those detected and undetected.

[8] Peter Swire, 'No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime' [2009] 7 J Telecom & High Tech. L. 107, 115; Susan W. Brenner, 'Law, Dissonance, and Remote Computer Searches,' [2012] 14 N.C. J.L. & Tech. 43, 45-46 (describing how cybercrime "effectively fractures the crime, which means relevant evidence" is scattered across multiple jurisdictions, further showing how that complicates law enforcement investigation).

[9] Spoofing is "a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity." In IP Spoofing "a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering." *See* 'What is IP Spoofing' (Kasparsky Lab, 2021) < https://www.kaspersky.com/resource-center/threats/ip-spoofing> accessed 4 September 2021.

[10] Jennifer Daskal, 'The Un-Territoriality of Data' [2015] 125 Yale L. J. 326, 397.

[11] *Id*., at 331.

[12] *See S.S. Lotus Case* (Fr v Turk) (Judgment) [1927] PCIJ Rep Series A No 10, 19 (emphasis added).

[13] Alvarez-Machain v. US [2003] 9th Cir, 331 F 3d 604 (lacking extraterritorial enforcement under the Controlled Substances Act to abduct the plaintiff from Mexico).

[14] Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, OUP 2015) 31.

transfer data. These physical elements that make up the datasphere's pipe system, can be regulated like any other pipe, using traditional territorial rules. But the datasphere is also a sphere of ideation, influence, commerce, and ingenuity that operates outside the realm of sovereign power. Data "generates a value that is intangible and independent from the physical resource itself. Once this data moves around in its own sphere, it generates a new relationship with the traditional institutional territories."[15] In so doing, it defies classic jurisdictional principles that are dependent on territorial line-drawing.[16] Not only that, but the datasphere is "ever-growing," for once data is "poured into the datasphere" it produces "further data in a never-ending process."[17] This is what sets the datasphere apart from the other spheres of the earth—the lithosphere, hydrosphere, and atmosphere;[18] "While humans are attempting to discover the universe, defying its infinity, at the same they are creating, on Earth, a potentially infinite digital environment made of data."[19]

This bifurcated nature of the datasphere complicates the work of our cyber constables. Our conventional understanding of a sovereign's right to exclude others may start to feel somewhat anachronistic in the face of new emerging technologies for remote searches and seizures.[20] Modern law enforcement agencies are further bolstered by a data ecosystem which centers around powerful corporate intermediaries who may, on occasion, be coopted or coerced to collaborate in incidents of extraterritorial enforcement overreach.[21] While the risk to international stability from this new

[15] Bergé, J-S., Grumbach, S. & Zeno-Zencovich, V., 'The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance' (2018) 5(2) Eur. J. Comp. L. & Gov 5(2), 144.

[16] There is a rich literature that has already demonstrated the challenges imposed by the concept of the datasphere on the application of existing public and private international law jurisdictional principles. A non-exhaustive list may include: Henry H. Perritt Jr., 'Jurisdiction in Cyberspace,' [1996] 41 VILL. L. REV. 1; Joel Trachtman, 'Cyberspace, Sovereignty, Jurisdiction, and Modernism,' [1998] 5(2) IND. J. GLOB. L. STUDIES 561; Jack L. Goldsmith, 'Against Cyberanarchy,' [1998] 65(2) UNI. CHI. L. REV. 1199; Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface,' [2008] 19(4) EUR. J. INT'L. L. 799; Kristin M. Finklea, 'The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement,' (CONG. RES. SERV., 17 Jan. 2013) <https://fas.org/sgp/crs/misc/R41927.pdf> accessed 5 September 2021; Kristen E. Eichensehr, 'Data Extraterritoriality,' [2017] 95 TEX. L. REV. ONLINE 145; Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017); Alexandra Perloff-Giles, 'Note: Transnational Cyber Offenses: Overcoming Jurisdictional Challenges,' [2018] 43 YALE J. INT'L. L. 191; Andrew Keane Woods, 'Litigating Data Sovereignty,' [2019] 128 YALE L.J. 328.

[17] Vincenzo Zeno-Zencovich, 'Legal Epistemology in the Times of Big Data,' in G. Peruginelli & S. Faro, (eds.), *Knowledge of the Law in the Big Data Age* 2018. Knowledge of the Law in the Big Data Age 3, 5 (IOS Press 2019).

[18] Jean-Sylvestre Bergé, 'The Datasphere as a New Paradigm for Relationship between Territories in Law' (2017) 7 Braz J Pub Pol'y III, V ("The earth sciences subdivide the environment into a collection of spheres, such as the lithosphere, atmosphere or biosphere. Each of these spheres has its own particular logic.").

[19] *See* Zeno-Zencovich, *supra* note 17, at 5.

[20] Dan Jerker B. Svantesson, 'Law Enforcement Cross-border Access to Data Preliminary Report' (SSRN, 23 November 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238> accessed 7 September 2021, 11 (noting that "the territoriality principle is a poor fit for the largely border-disregarding internet."); *See also* Opinion of Advocate General Wathelet delivered on 9 November 2016, Concurrence SARL v Samsung Electronics France SAS and Amazon Service Europe Sàrl, ECJ, Case C-618/15, ECLI: EU:C:2016:843, para 2 (noting that the "internet is a network which is by definition universal," and that as a result the territorial location of cybercrime, "be it the causal event or the loss sustained, is particularly difficult to determine.").

[21] See generally, Alan Z. Rozenshtein, 'Surveillance Intermediaries' [2018] 70 STAN. L. REV. 99, 104 (describing "handshake agreements" between government and tech giants as part of a "surveillance-industrial Internet complex").

reality is obvious,[22] so far political tensions have been kept at a minimum.[23] But should we continue to roll the dice?

Consider, for example, the following non-exhaustive list of cyber enforcement activities. Which of these techniques might you deem tolerable when employed against a target abroad without the consent or knowledge of the foreign state? Which of these might you consider to be crossing a threshold, and what factual and legal factors might influence your determination?

(1) Data scraping from social media platforms, other websites, and open-access databases located on servers abroad to import information.
(2) Subverting the command-and-control server of an anonymized botnet operating from one of the corners of the "dark web."
(3) Electronically tracing and restoring cryptocurrency payments that were paid to a foreign criminal cyber gang involved in a crippling ransomware attack.
(4) Compelling a domestically registered company to release certain data concerning a national involved in a domestic crime, where the data is stored abroad.

In this chapter I explore each of these four scenarios. Each scenario ties to a different aspect of the datasphere which frays at the edges of traditional doctrine.[24] These four aspects are: (1) consent, (2) anonymization, (3) piracy, and (4) extraterritoriality. For each of these aspects I try to demonstrate how jurisdictional rules may evolve, as a matter of *lex ferenda*, to better balance territorial integrity and cyber stability. My analysis thus attempts to provide a preliminary taxonomy of certain categories of cyber policing activity that could serve as a roadmap for future rule-prescribers and rule-appliers.

Part I: If Jean Bodin had a WhatsApp and Emer de Vattel was on TiktTok

If one wanted to, one could tell quite a coherent doctrinal story about the scope of application of the prohibition on extraterritorial enforcement jurisdiction in the datasphere. After

[22] Ahmed Ghappour, 'Searching Places Unknown,' [2017] 69 STAN. L. REV. 1075, 1108 (describing law enforcement use of cyber techniques on the dark web as operating "in obvious tension with international norms." Ghappour proceeds to cite five possible risks to foreign relations that may be derived from acts of extraterritorial enforcement. In particular he notes the concern that "rank-and-file" law enforcement officers will operate in a "regulatory vacuum" with insufficient attention to specific foreign affair policies or considerations); Robert J. Currie, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?,' [2016] 54 CAN. YB INT'L. L. 63, 78 (noting that "states are sensitive and conservative about any cross-border electronic traffic by foreign investigators and that they wish to maintain the ability to object publicly to actual events or even potential intrusion.").

[23] Orin S. Kerr & Sean D. Murphy, 'Government Hacking to Light the Dark Web Risks to International Relations and International Law?,' [2017] 70 STAN. L. REV. ONLINE 58, 65 (suggesting that as far as the use of extraterritorial network investigative techniques are concerned, they do not pose a significant threat to international relations, as the practice as so far demonstrated "a norm of cooperation instead of confrontation.").

[24] There is of course a fifth category, that of national security cyber espionage operations. As Jack Goldsmith wrote nearly two decades ago "[n]orms of "territorial sovereignty" have never precluded such offshore espionage. There is a simple reason for this: Nations are interested in what goes on inside other nations, and there is no across-the-board, cost- effective way to stop such spying." (see Jack Goldsmith, 'The Internet and the Legitimiacy of Remote Cross-Border Searches' (2001), 1(4) U. Chicago Leg. F. 103, 114). Within the limits of this book chapter I can't address this issue which I've devoted significant parts of my scholarship to. For further reading see Asaf Lubin, 'The Liberty to Spy', 61(1) Harv. Int'l L.J. 185 (2020).

all, it has been repeatedly argued that the "most solid view" of international law is that any non-consensual access to data that is "stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state."[25] This view of the *lex lata* has been endorsed by courts,[26] governments,[27] scholars,[28] and certain treaty regimes.[29] The logic behind this interpretation is quite clear. After all, as "a corollary of state sovereignty" officials operating in one state "may not exercise their functions in the territory of another state without the latter's consent."[30] Extending exclusive territoriality to data stored on computers and servers within one's borders reflects the thinking of Bodin, who believed that the "preservation of the state" mandates

[25] Bert-Jaap Koops & Morag Goodwin, 'Cyberspace, the Cloud and Cross-Border Criminal Investigation', [2014] Tilburg Law School Legal Studies Research Paper Series, No. 05/2016, at 61 (in fact the authors cite to a US attorneys manual to demonstrate that even more innocuous acts of remote evidence-gathering, like making a phone call or sending a letter, could be "considered a breach of sovereignty."); *Cf.* DOJ Justice Manual, Sec. 9-13.500, https://www.justice.gov/jm/jm-9-13000-obtaining-evidence#9-13.500 (describing a phone call or email to a witness abroad as one requiring prior approval from the Criminal Division's Office of International Affairs, but not one that is *ipso facto* a sovereignty violation).

[26] *See e.g.* X (Re), [2010] 1 FCR 460, 2009 FC 1058 (CaLII), para. 40; *Weber and Saravia v. Germany*, Decision, App. No. 54934/00, ECtHR, 29 June 2006, para. 88.

[27] A 2013 study by the UN Office of Drugs and Crime summarized the opinions of 47 responding states on a range of cybercrime issues. Two-thirds of the responders concluded that it would be "not permissible" for foreign law enforcement to "access computer systems or data" without relying on formal mechanisms for affirming consent, like an MLA process. Those countries explicitly cited "the principle of sovereignty" to justify their position *See* UNODC, Comprehensive Study on Cybercrime, (February 2013) <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 7 September 2021, 220 [hereinafter: UNODC Report].

[28] *See e.g.* Currie, *supra* note 22, at 97 (concluding that for the time being states are still committed to a "Westphalian-bound model" that prohibits extraterritorial enforcement jurisdiction in cyberspace); Joachim Zekoll, *Jurisdiction in Cyberspace*, *in* Beyond Territoriality: Transnational Legal Authority in the Age of Globalization (Gunther Handl, Jochim Zekoll, & Peer Zumbansen eds., 2012), 341, 369 (noting that disputes arising out of Internet activities are, for the most part, governed by traditional, state-based jurisdictional forces); Kevin Jon Heller, 'In Defense of Pure Sovereignty in Cyberspace' (2021) 97 Int'l L. Stud. 1432, 1464 (supporting a pure-sovereigntist model according to which "low-intensity law-enforcement operations violate sovereignty simply because they involve penetrating a computer system located on the territory of another state."); Stephen Allen, 'Enforcing Criminal Jurisdiction in the Clouds and International Law's Enduring Commitment to Territoriality,' in Stephen Allen, Daniel Costelloe, Malgosia Fitzmaurice, Paul Gragl, & Edward Guntrip (eds.) *The Oxford Handbook of Jurisdiction in International Law* (2019) 381, 409 (noting that "unilateral retrieval of data located within another state's territory" is in "contravention of international law," and further suggesting that any attempt to "bypass the territorial conception of enforcement jurisdiction by reference to exceptional grounds" is "unsustainable.").

[29] The leading cybercrime treaty, the Council of Europe Convention on Cybercrime (or Budapest Convention) prohibits non-consensual transborder access to computer data, except in very limited scenarios. *See* Council of Europe, Convention on Cybercrime, opened for signature 2001, E.T.S. No. 185, Art. 32 (entered into force 2004) [hereinafter: Budapest Convention] (note, however, that Article 39(3) confirms that the Convention does not affect other rights or restrictions, thereby opening the door for parallel evolution of customary practice around extraterritorial enforcement in cyberspace). Note further that in May 2021 the Protocol Drafting Plenary of the Cybercrime Convention Committee (T-CY) approved the (Draft) Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. The Additional Protocol, which will take effect in 2022, is meant to expedite the process by which parties to the protocol may access data from servers located abroad. *See* Debrae Kennedy-Mayo & Peter Swire, 'Update to Budapest Convention Expected to be Finalized in November' (*Cross-Border Data Forum*, 11 October 2021) < https://www.crossborderdataforum.org/update-to-budapest-convention-expected-to-be-finalized-this-november/ > accessed 8 November 2021.

[30] Restatement (Third) of Foreign Relations Law of the United States § 432 cmt. b (suggesting further that the offended state may be entitled to seek certain reparation).

that foreigners be denied any opportunity to usurp governmental functions.[31] It also reflects thinking by Vattel who promoted the notion of external sovereignty as a rule according to which "no state has the smallest right to interfere in the government of another."[32]

This essay could have ended right here, but the last two decades have shown time and again how states, as a matter of practice, engage in variedly complex unilateral cross border cyber activity.[33] In fact, it may be the case that at least some states are more interested in preserving *their* right to publicly condemn cyber intrusions into *their* sovereignty, than they are abiding by a general prohibition on foreign cyber intrusion.[34] As Robert Currie highlights: "While states generally take a territorial sovereignty point of view, there is a dissonance between what states say (opinio juris) and what they do (state practice)."[35] This strange duality creates a tension between the "myth system" and the "operational code";[36] between a fictional international law rule that is seemingly clear, well-defined, and uniformly applied and a far messier practice that is characterized by self-motivated, unilateral, extraterritorial, and non-consensual cyber enforcement activity.

Take the Netherlands as one case in point. In 2019 the country publicly defended the position that in cyberspace "the act of exercising investigative powers in a cross-border context is traditionally deemed a violation of a country's sovereignty unless the country in question has explicitly granted permission."[37] Despite this legal position, it was the Netherlands that conducted unilateral non-consensual cyber operations in both the *Bredolab* and *Descartes* cases in the early 2010s. Dutch law enforcement authorities took offensive cyber action against a foreign botnet[38] and a TOR server[39] storing child pornography in each of these cases respectively. In neither of

---

[31] Jean Bodin, *Les Six Livres de la République* [The Six Books of the Commonwealth), 49 (M.J. Tooley ed. & trans., 1955) (1576).

[32] Emer de Vattel, *The law of Nations; or, Principles of the Law of Nature, applied to the Conduct and Affairs of Nations and Sovereigns* (Joseph Chitty trans., 1863), 154.

[33] Indeed, even in the UNODC 2013 report discussed above a third of the responding states, not an insignificant number, found such activity permissible. Those states justified extraterritorial cyber enforcement activity by referring to notions of "reciprocity," "urgency in cases of serious crime," "impossibility to know in which country the data actually is," and "threats to national security." *See* UNODC Report, *supra* note 27, at 220.

[34] Currie, *supra* note 22, at 78 (tying states conservative interpretation of the prohibition on unilateral remote searches to their general desire "to maintain the ability to object publicly" to potential intrusions against them or their interests).

[35] *Id.*, at 93.

[36] W. Michael Reisman, *On the Causes of Uncertainty and Volatility in International Law*, *in* THE SHIFTING ALLOCATION OF AUTHORITY IN INTERNATIONAL LAW: CONSIDERING SOVEREIGNTY, SUPREMACY AND SUBSIDIARITY 33, 44-45 (Tomer Broude & Yuval Shany eds., 2008) (describing "myth systems" and "operational codes" as two "relevant normative systems.").

[37] The Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace — Appendix: International Law in Cyberspace [2019] <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> accessed 7 September 2021, 2. Note that the Dutch statement follows by clarifying that "Opinion is divided as to what qualifies as exercising investigative powers in a cross-border context and when it is permissible without a legal basis founded in a treaty."

[38] Botnet is a network of infected computers (e.g. internet-of-things connected devices) compromised and remotely controlled by a botmaster.

[39] TOR (The Onion Router) is an open-source software that allows users to browse the internet in an anonymous way, thereby protecting their privacy from certain traffic analysis.

these cases did they seek to cooperate with the countries where the servers were located, nor did they seek to employ mutual legal assistance (MLA) treaties.[40]

The Cloud Evidence Group is a working group that was established by the Budapest Cybercrime Convention Committee (T-CY) in 2014 to explore "solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions."[41] The Group concluded in 2016 that: "in the absence of international solutions, governments increasingly pursue unilateral solutions," and that these solutions are increasingly posing risks to "State to State relations and the rights of individuals."[42]

It is this dissonance between what states say and what they do that has led others to propose alternative theories about the law that governs extraterritorial enforcement in cyberspace. Mireille Hildebrandt, for example, has suggested that we reject "artificial demarcations that have run out of steam"[43] and instead embrace the ubiquity of cyberspace, the notion that it "does not stop where ordinary space begins."[44] As a result she argues that we should accept "universal extraterritorial jurisdiction to enforce."[45] As Hildebrandt writes: "as long as the official conducting a remote extraterritorial search is physically located in the territory of the investigating state, some will define her action as an *intraterritorial search* with indirect exterritorial effects."[46]

Taking an equally controversial position, Dan Svantesson has suggested we adopt a fourth category of jurisdiction, which he calls "investigative jurisdiction."[47] According to Svantesson, cross-border law enforcement access to data is different from "cross-border kidnapping, and … the fact that international law groups the two together reveals an inexcusable lack of sophistication."[48] A new fourth investigative jurisdiction can serve as an "in-between" category that will not rise to the level of full enforcement.

Within the limits of this book chapter, I don't contend to resolve the disputes between "the law in the books" and the "law in action," nor do I plan to take a definitive position in the debate between pure sovereigntists and contemporary cyber expansionists. Rather, I hope to practically highlight the limits of conventional territoriality in four specific categories of cyber enforcement

---

[40] *See* 'Transborder access and jurisdiction: What are the options?,' Report of the Transborder Group adopted by the Cybercrime Convention Committee (T-CY) [6 December 2012] <https://rm.coe.int/16802e79e8> accessed 7 September 2021, 35 [hereinafter: T-CY 2012 Report].

[41] Jan Kleijssen & Pierluigi Perri, *Cybercrime, Evidence and Territoriality: Issues and Options*, 47 NETHERLAND YB INT'L. L. 147, 150, fn. 13 (2016).

[42] T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group, 2 (17 Feb. 2016), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8.

[43] Mireille Hildebrandt, 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in cyberspace' (2013) 63 Uni. Toronto L.J. 196, 223.

[44] *Id.*, at 222.

[45] *Id*.

[46] *Id*. (emphasis added).

[47] Dan Jerker B. Svantesson, *Preliminary Report: Law Enforcement Cross-border Access to Data*, 7 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238; *See also*, D.J.B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP, 2017), 165-168.

[48] *Id*.

activity. For each of them, I try to show how they fray at the edges of existing doctrine and in what ways they could be utilized to shape the future evolution of jurisdiction theory.

Part II: Fraying at the Edges of Doctrine

Transnational cooperation in digital investigations is difficult. In the instances where an MLA regime is in place, the process is "abysmally slow" and conflicting rules between jurisdictions around access to data often result in full or partial denial of requests.[49] Where an MLA regime is not in place, there is even less certainty about the likelihood of mutual assistance. Even more troubling are instances where the host country is itself complicit in the crime being investigated, as is the case with certain state-sponsored cyber offences, there is no motivation to cooperate altogether.

It is therefore important to stress that denying states the authority to engage in unilateral remote cyber enforcement activity entails a tradeoff. Preserving the sanctity of sovereign equality comes at the expense of wreaking havoc on cyber stability. The international community inadvertently invites cybercriminals to continue their illicit activity with an increased degree of impunity, as it capitulates to doctrinal restrictions on the ability to conduct meaningful cross-border operations. As the Cloud Evidence Group noted: "If only a minuscule fraction of offences involving computer data and systems can be prosecuted […. it] raises questions regarding the rule of law in cyberspace."[50]

What would Vattel have to say about this? After all, Vattel promoted his theory of external sovereignty because he believed such a rule was necessary for the state to "discharge the duties she owes to herself and to her citizens."[51] But isn't one of those duties the responsibility protect the polity from transgressions and delinquency? And if so, in protecting the traditional view regarding extraterritorial enforcement are sovereigns not, in effect, abrogating from this core responsibility? Given the rise in cybercrime in recent years, it might be an opportune time to ask whether the tradeoff we collectively signed onto in Westphalia in the 17th century still reflects the core needs and values of our modern societies.

To the extent that an amendment is desired, we may wish to examine certain cyber exceptions to the traditional view as a matter of future law. Such reform need not necessarily embrace a full-blown expansionist theory like the one put forward by Hildebrandt. Rather, we may wish to explore, in the interim, specific nudges at the edges of doctrine. Within the limits of this chapter I consider the four specific scenarios and aspects discussed in the introduction, and examine the extent to which each of them may educate us about potential directions for doctrinal evolution.

a. Whose Consent is it anyway?

[49] Jonah Force Hill, Problematic Alternatives: MLAT Reform for the Digital Age, Harv. Nat'l. Sec. J. (Jan. 28, 2015), https://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/ (proposing further solutions on how to streamline and reform the MLAT process).

[50] T-CY Cloud Evidence Group, Criminal Justice Access to Data in the Cloud, 6 (26 May 2015), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59.

[51] *See* Vattel, *supra* note 32, at xiv.

If we are looking for areas in the doctrine where natural expansion may occur, it is perhaps wisest to begin with the notion of consent. After all, the prohibition on extraterritorial enforcement jurisdiction has a built-in caveat, it allows for such enforcement where there is valid consent. But who is authorized to give such consent, and under what circumstances may that consent be implied?

Consider a straightforward case: Irish Police officer Janet is investigating a cyberattack allegedly committed by a gang of Russian cybercriminals. As part of her investigation, she goes on the internet and reads a story in Russian media about the gang's origin story. To fetch the content of a particular URL, Janet's web browser had to locate a web server, connect to it, and send an HTTP request for the desired page. In essence Janet had to ping a server, and that server is likely remotely located, potentially even in Russia. Not only that, but the ping might have gone through servers located in four different other countries, on its way to and from Russia. Did Janet engage in an extraterritorial enforcement action? Few would argue this action is prohibited as a matter of international law, but why? If an absolute sovereignty view would construe even the merest phone call or email to a Russian witness as prohibited under existing doctrine,[52] why is pinging a server there acceptable?

One explanation could be that States have impliedly consented to certain types of internet traffic crossing through their servers. In a crowded internet, it is inevitable and must be accepted that certain kinds of communications will ultimately reach one's shores.[53] As such, the remote access to electronic data that is publicly accessible on the world wide web, may now be seen as territorial rather than extraterritorial. This was the position taken by the experts who drafted the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. But how far can we extend this line of reasoning? The experts believed that any data that is "meant to be accessible" from the state Janet is in, would be subject to the same legal rules.[54] So where Janet was "able to obtain, under false pretences, the log-on credentials to a closed online forum hosted on servers located abroad" her accessing the forum from her territory should be seen in the same manner as her accessing an open-access website.[55] This position raises many eyebrows, as it opens the door to an array of cyber enforcement activity. Kristen Eichnsehr criticized the manual's analysis of jurisdictional issues, claiming that the experts attempted "to settle too much, too fast, declaring over and done debates that States are still hashing out."[56]

Another possible explanation for the legality of law enforcement accessing open-access websites, is that the website publishers themselves consented. This is the position taken in the Budapest Convention. Article 32(b) creates an exception to the general prohibition on transborder access to stored computer data. It establishes that where Janet was able to secure the "lawful and voluntary consent of the person who has the lawful authority to disclose the data" her accessing

[52] *See supra* note 25 and accompanying text.

[53] Brian Egan, 'International Law and Stability in Cyberspace' (2017) 35 Berkeley J. Int'l. L. 169, 174 ("The very design of the Internet may lead to some encroachment on other sovereign jurisdictions.").

[54] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 69 (Michael Schmitt ed., 2d ed. 2017).

[55] *Id*., at 69-70.

[56] Eichensehr, *supra* note 16, at 160.

the data will not require the authorization of the affected state.[57] But Russia's opposition to the Budapest Convention is directly tied to this provision. Russian officials believe that by authorizing "one state to access computers in a second state with the permission of the computer owner, and without consulting governmental authorities in the second state," the treaty has overextended the reach of foreign nations at the expense of sovereignty.[58]

Russia has good reason to be concerned. By outsourcing consent from the State to the "computer owner," the door is opened for a number of individual players to increase their role in legitimizing cyber enforcement activity. "Internet service providers, cloud storage services, and other data holders" privately manage huge swaths of our internet infrastructure, and at times they have been "content to comply" with requests for assistance.[59] Consider practice in the United States surrounding botnet takedown. In many of those occasions the FBI and Microsoft sought and received restraining orders and injunctive relief from courts, which they used to compel U.S.-based companies to impose registry locks on internet domain names or disable the Botnet's IP addresses. They further used the orders to seek the voluntary cooperation of foreign-based internet service providers.[60]

The United States is not alone in this. In fact, many countries have laws in the books that would allow them to compel individuals within their territory to release data stored abroad.[61] An extension of the concept of consent that includes, not just the consent of the foreign sovereign, but also the consent of the data processor and the data subject, is therefore one area that pushes at the edges of existing doctrine.

b. Preserving Comity with Masked Sovereigns

Comity commands us to promote "friendly legal relations between sovereigns"[62] whenever possible and to adopt a degree of courtesy and "consideration of mutual respect"[63] which "should

[57] Budapest Convention, *supra* note 29, Article 32. This raises a complex question about the legality of the use of web-crawlers and other data scraping tools on publicly accessible websites. On the one hand the websites are publicly accessible and therefore under Article 32(a) of the Budapest Convention, accessing them without consent is lawful. On the other hand, the use of such tools would often violate particular end-user license agreements or terms of service, therefore coming into clash with Article 32(b) which refers back to the consent of the "computer owner."

[58] Mark Ballard, UN Rejects International Cybercrime Treaty, Computer Wkly. (Apr. 20, 2010), http://www.computerweekly.com/news/ 1280092617/UN-rejects-international-cybercrime-treaty.

[59] Currie, *supra* note 22, at 83.

[60] For further reading see Asaf Lubin & João Marinotti, *Why Current Botnet Takedown Jurisprudence Should Not Be Replicated*, Lawfare (July 21, 2021), https://www.lawfareblog.com/why-current-botnet-takedown-jurisprudence-should-not-be-replicated; Janine S. Hiller, Civil Cyberconflict: Microsoft, Cybercrime, and Botnets, 31 SANTA CLARA HIGH TECH. L.J. 163, 175 (discussing the way the FBI was able to stop the Coreflood virus using cross-border action).

[61] Currie, *supra* note 22, at 93 (including Australia, United Kingdom, France, Canada, Denmark, Ireland, Italy, Spain, Portugal, Romania, and Malaysia in the list of countries with such laws).

[62] F. A. Mann., Comity, in Oxford Scholarly Authorities on International Law (1986).

[63] James Paul George & Fred C. Pederson, *Conflict of Law*, 41 SW. L.J. 383, 409 (1987).

prevail between judicial institutions."[64] For data sovereignty disputes it entails the employment of doctrines of "recognition and deference, as well as doctrines of abstention and restraint."[65]

But how far should courtesy go? Is the obligation to keep friendly legal relations *in rem* or *in personam*? To the extent that it is *in rem*, a sovereign will be required to preserve comity wherever she may go, even with interacting with unidentified third parties. Such an expansion of the duty would seem to go outside the bounds of existing law. Certainly, the obligation to show deference is owed only to other sovereigns and as such is not extended *ad astra*. In a different chapter in this book, Austen Parrish describes the triple duties of cooperation, consultation, and negotiation in international law. He perfectly demonstrates how these obligations require that any exercise of unilateral prerogative be disfavored, at least until good faith efforts for finding collaborative solutions have been exhausted.[66]

But a sovereign has no good faith cooperation, consultation, or negotiation obligations towards a phantom. In a situation where the location of the data sought is unknown, especially where perpetrator has utilized tools of concealment to avoid geographical detection, why must a sovereign be required to show restraint? Anonymization in the datasphere introduces yet another layer of complication to existing doctrine since it circumvents all possibility for cooperation between law enforcement. This is precisely the nature of activities on the dark web, "a global network of computers that use a cryptographic protocol to communicate, enabling users to conduct transactions anonymously without revealing their location."[67] Is an operation on the dark web, say the use of network investigative technique to unmask the identity of a particular perpetrator, a violation of the prohibition on extraterritorial enforcement? Google seems to think so, suggesting that such an operation not only undermines the sovereignty of other nations, but it also "raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns."[68] While I'm sympathetic to an approach that seeks to promote international cooperation in the fight against cybercrime, I am also cognizant of the fact that reality can't be put on hold until that happens.

Simply put "it is not possible to apply the principle of territoriality if the location of the data is uncertain."[69] Stephen Allen writes that such an approach is "troubling" because it "reveals

---

[64] Arbitral Tribunal Constituted Pursuant to Article 287, and Article 1 of Annex VII, of the United Nations Convention on the Law of the Sea for the Dispute Concerning the MOX Plant, International Movements of Radioactive Materials, and the Protection of the Marine Environment of the Irish Sea (Ireland v. U.K.), the MOX Order Case, Order No. 3, ¶ 28 (Perm. Ct. Arb. 2003).

[65] *See* Woods, *supra* note 16, 406.

[66] Austen Parrish, *Sovereignty, Self-Determination, and the Duty to Cooperate: Public International Law's Limits on Unilateral Extraterritorial Regulation of Non-Citizens*, Current Draft (pages 10-12).

[67] *See* Ghappour, *supra* note 22, at 1077.

[68] Letter from Richard Salgado, Dir. of Law Enf't & Info. Sec., Google Inc., to the Advisory Comm. on Rules of Criminal Procedure 2-3 (Feb. 13, 2015), https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0029&attachment Number=1&contentType=pdf.

[69] *See* T-CY 2012 Report, *supra* note 40, at para. 134 (noting further that a "a 'paradigm shift' has therefore been called for."). For example, under the New Zealand Search and Surveillance Act of 2012 an exception to territoriality exists for "remote access search warrants" which are permissible where the search is "of a thing such as an Internet data storage facility that does not have a physical address that a person can enter and search." See therein, Sec. 12.117, https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf.

an eagerness to cast aside the primary principle of enforcement jurisdiction—territoriality—in favor of untried and untested alternatives."[70] He therefore argues that under international law as it currently stands, in the case of doubt as to the location of data, sovereigns should simply *do nothing*. But even he admits that "such a straightforward response prioritizes the principle of territoriality over a state's duty to maintain the integrity of its criminal justice system."[71] When faced with serious crime or exigent national security threats, I am not familiar with many constituencies who would be willing to accept such a dangerous trade, nor do I think such a skewed balance supports the fundamental ideals of peace and security grounding our international order.

Perhaps consent could be a hook on which we rest our hat. One may suggest as a compromise that countries that authorize the use of TOR and other cryptographic tools from within their territory, provide their implied consent, that when such technologies are abused to facilitate serious crime, foreign law enforcement may utilize unmasking techniques to identify the perpetrators. The scope of consent will be limited only to the passive act of identification. Once the individual or data is geographically located, obligations of cooperation and comity could kick back in.

c. <u>What do you do when the Hacker is a Pirate?</u>

Certain types of cybercrime may, in certain circumstances, be considered as falling within preexisting categories of internationalized crime, including transnational organized crime, hostage taking, terrorism, and even piracy.[72] What connect many of these categories of crime together is that the perpetrators may be seen as *hostis humani generis*—an enemy of mankind—and therefore may be subject to prosecution in whatever state they are found.[73]

The recent court case brought against Springhill Medical Center by Teiranni Kidd captures the mind. A foreign ransomware attack on the medical center disabled computers "on every floor" limiting the nurses' ability to locate medical staff, monitor fetal heartbeats, and access patient health record.[74] As a result, it is alleged in the suit, the staff provided inadequate care which resulted in a failure to notice the umbilical cord was wrapped around the baby's neck, which ultimately resulted in the baby's death shortly after birth.[75] "The filing is the first credible public claim that someone's death was caused at least in part by hackers who remotely shut down hospital computers in an extortion attempt."[76] The case further demonstrates the possibilities for severe and dramatic physical harms that can materialize from cybercrime.

---

[70] *See* Allen, *supra* note 28, at 393-394.

[71] *Id.*, at 394.

[72] I discuss this at greater length in Asaf Lubin, 'Law and Politics of Ransomware' (forthcoming, 2022).

[73] Alexandra Perloff-Giles, 'Note: Transnational Cyber Offenses: Overcoming Jurisdictional Challenges' (2018) 43 Yale J. Int'l. L. 191, 223.

[74] Kevin Poulsen, Robert McMillan and Melanie Evans, 'A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death' (Wall Street Journal, 30 September 2021) <https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116> accessed 8 November 2021.

[75] Kevin Collier, 'Baby died because of ransomware attack on hospital, suit says' (NBC News, 30 September 2021) <https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465> accessed 8 November 2021.

[76] *Id*.

Unlike Hildebrandt,[77] I do not posit that all of cyberspace should be subject to universal jurisdiction. Nonetheless, certain categories of heinous cybercrimes, chief amongst them is the crime of cyber extortion through ransomware, may trigger universal jurisdiction in certain extreme circumstances. Of course, as noted by Alexandra Perloff-Giles the challenge "in applying universal jurisdiction to the cyber context is defining the scope of threats for which universal jurisdiction is authorized. The scope must be defined narrowly enough to prevent countries like Russia and China from taking advantage of universal jurisdiction to shut down online dissent."[78] Within the limits of this chapter, I am unable to provide an exhaustive list of crimes or factors to be considered. Nonetheless, the mere possibility that certain acts of cyber piracy could trigger possible adjustments to the doctrinal view on jurisdiction is important to recognize.[79]

Such an extension of jurisdiction has a strong theoretical underpinning. Cedric Ryngaert has made the case for the application of a "positive sovereignty principle" in international alw, which he describes in the following way: "states are allowed to apply their laws to a foreign situation, to the extent that the State that has the stronger nexus to the situation fails to adequately deal with [it], in a manner that is, on aggregate, harmful to the regulatory interests of the international community."[80] The current situation surrounding the crime of ransomware offers a good manifestation of Ryngaert's proposed principle. Where Russian intelligence provides safe harbor to ransom gangs—sometimes even indirectly employing them[81]—it cannot rely on its own sovereignty to shield them from cyber enforcement action that is meant to protect the interests of the international community.

d. Between a "Center of Gravity" and Degrees of Gravity

All three elements discussed so far—consent, anonymity, and piracy—demonstrate the inherent limitations of applying to the datasphere a purely territorial conceptualization of the traditional prohibition on extraterritorial enforcement jurisdiction. In so doing, all three elements have implicitly demonstrated that while territory remains "the currency of analysis" it is also "the source of misunderstanding and disagreement."[82] So in this final section of the chapter, I wish to address the elephant in the room, the very concept of "extraterritoriality" itself. As a scenario of reference, we may consider the case of *Microsoft Ireland*, where a domestically registered

[77] *See* Hildebrandt, *supra* notes 43-46 and accompanying text.

[78] *See* Perloff-Giles, *supra* note 73, at 224-225.

[79] Consider in this regard Article 109 of the UN Convention on the Law of the Sea which, in the context of unauthorized broadcasting, extends prosecutorial jurisdiction to encompass "the state where the transmissions can be received, or any state where authorized radio communication is suffering interreference." As an example, in 1962 "Denmark seized the Lucky Star which was broadcasting just outside of Danish territorial waters. The crew was arrested and successfully prosecuted under Danish Law." (*see* Commander David G. Wilson, 'Interdiction on the High Seas: The Role and Authority of a Master in the Boarding and Searching of His Ship by Foreign Warships' (2008) LV Naval L. Rev. 157, 190-191, fn. 241).

[80] *See* Ryngaertt, *supra* note 14, at 190.

[81] *See* Frank Bajak, 'How the Kremlin provides a safe harbor for ransomware' (AP, 16 April 2021) <https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999> accessed 8 November 2021.

[82] Hannah Buxbaum, page. 670.

company is ordered to release certain data concerning a national involved in a domestic crime, where that data just happens to be stored abroad.[83]

In trying to resolve the question of whether the FBI's order to Microsoft is "extraterritorial" we must first acknowledge what Hannah Buxbaum has argued, that "territoriality" and "extraterritoriality" are merely "legal constructs." They are "claims of authority, or of resistance to authority, that are made by particular actors with particular substantive interests to promote." Indeed, it would be wrong to examine territoriality in "monolithic terms" thereby ignoring "the various localized practices and understandings that inform its content."

One solution could be to reconceptualize the doctrine of extraterritorial enforcement jurisdiction by rejecting a single factor test for determining what is extraterritorial enforcement in the datasphere. Describing what he called "the law of nowhere," Szigeti highlighted the "instability of territorial/extraterritorial divides" for intangibles like electronic data.[84] He therefore concluded that the "supremacy of territorial jurisdiction" is marred with "false assumptions," for not all things possess an "observable" and "verifiable" physical location.[85]

As Deputy Assistant Attorney General Richard W. Downing posited, we live in "a world of conflicting cross-currents—the simultaneous need to reach out for data stored abroad and concern about limiting the ability of others to reach in."[86] As a result, a multi-factor reasonableness standard is perhaps the only viable test that is capable of responding to the "constant push and pull"[87] of contemporary data sovereignty disputes. Such a test has its limits, of course, predominately in the discretion it leaves in the hands of judicial assessors.[88] As such, we should apply this standard only temporarily, until such time as greater consensus is achieved by courts and the international community as to the weight that different factors should be given in our assessment. This proposed analysis will have two parts, first asking what is "extraterritorial", and second asking what constitutes "enforcement". Let me briefly consider each part of the test.

(1) *Reconceptualizing extraterritoriality*. Developing a "center of gravity" test for data may offers the most promising answer for jurisdictional assessment, as opposed to a test that is linked solely to the randomness of a piece of data's momentary location. A "center of gravity" test would consider an array of factors including, among others: the nationality of the data owner, the location of the data owner, the location of data controller, the headquarters of the data controller, the

[83] For more on the *Microsoft Ireland* case, see e.g. Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 Stan. L. Rev. Online 9.

[84] Péter D. Szigeti, 'In the middle of nowhere: The Futile quest to distinguish territoriality from extraterritoriality,' in Daniel Margolies, Umut OZsu, Maia Pal, & Ntina Tzouvala (eds.) The Extraterritoriality of Law: History, Theory, Politics (2019), 30, 41-42.

[85] *Id*.

[86] Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the 5th German-American Data Protection Day on "What the U.S. Cloud Act Does and Does Not Do" (DOJ News, 16 May 2019) < https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-5th-german-american> accessed 8 November 2021.

[87] *Id*.

[88] *See e.g.* Donald Earl Childress III, 'Comity as Conflict: Resituating International Comity as Conflict of Laws' (2010) 44 U.C. Davis L. Rev. 11, 15 (noting that "[t]he primary concern is that the vague definition of comity itself "suggest[s] a [judicial] discretion unregulated by general principles" permitting courts to mask complex political decisions implicating sovereign interests and the international community in the nomenclature of law.").

headquarters of the cloud service provider that is contracting with the data controller, the territory where the data owner has subscribed to a service, the territory where the crime was perpetrated or where its effects were felt, the territory of the criminal justice authority, and yes also the location where the data is stored as but one factor to be considered within the mix.[89] A similar idea of a "balance-of-interest test" was introduced in the context of the Cloud Act following the *Microsoft Ireland* saga.[90]

(2) *Reconceptualizing enforcement* – It might be prudent to explore whether a *de minimis* line for sovereignty violations exist, according to which not all exercises of authority in the affected state will rise to the level of a reprehensible infringement. This echoes the views of Brian Egan, legal advisor to the US State Department, who had argued that not all non-consensual extraterritorial cyber operations constitute a prohibited enforcement action.[91] Finding out which activities rise above or below this *de minimis* line will depend on a follow-up "degree of gravity." Applying this test is of course a "challenging area" for the law to grapple with. Yes, there may be cases where consensus could be reached. Consider one example in this regard: suppose law enforcement in Germany apply for a warrant to hack the phone of a German national who is a member of a ring of money launderers. For two weeks the investigation goes according to plan and the police acquires significant troves of valuable information. One Friday, the target decides to get in his car and drive from Aachen to the nearby Dutch city of Maastricht, a mere 33-minute drive, to spend the weekend there. The police is unaware of the target's plans and continues to collect information from the phone while he is in the Netherlands. During the three days that the perpetrator spent in Maastricht, was an extraterritorial enforcement action carried out? If you answer yes to this question, what might be the logic? Is it simply because data happened to transfer through Dutch GSM networks during that time?

Applying the proposed tests of "center of gravity" and "degree of gravity" could help shed light about the Microsoft Ireland case. There, it would have seemed obvious that the operation is territorial and not extraterritorial (as all relevant jurisdictional links but the location of the data pointed to the United States) and that in any event the degree of intrusion onto Irish sovereignty was so limited that it could potentially be argued to not cross a *de minimis* threshold of intrusion to rise to the level of a sovereignty violation.

Conclusion

I recognize that advancing certain types of exceptions to the general prohibition on extraterritorial enforcement jurisdiction introduces many risks. The prohibition in its pure form does serve as a "check on empire building" and forces princes to develop "comprehensive responses" instead of pushing their agendas forward through polices that advance unilateralism,

[89] One example of where the focus on the location of the data storage seems completely arbitrary is in the context of data sharding, in which data is partitioned and broken up into different subsets to assist with processing, and where each shard may be stored in a different geographical location. In a multifactor test, the locations of all the various data shard could be considered within a broader "center of gravity" test.

[90] *See generally* Daskal, *supra* note 83.

[91] *See* Egan, *supra* note 53, at 174.

isolationism, and "piecemeal fragmentation."[92] I therefore agree wholeheartedly that we should continue to aspire for greater cooperation in the fight against cybercrime. We should also double our efforts to promote the development of collective norms and international regimes for responsible behavior in cyberspace, including in the context of transborder access to evidence for criminal investigations.

Nonetheless, we must also acknowledge that consensus is not likely to be achieved in the immediate future. We therefore find ourselves locked in the "tension between investigational needs and the protection of sovereignty," and this tension continues to contribute "to a sense of disarray that pervades the landscape."[93] Against this backdrop, making certain reasonable allowances towards unilateral prerogatives is not only inevitable, it is absolutely necessary as we try to keep the international order afloat amidst turbulent cyber waters.

[92] Austen L. Parrish, *The Interplay between extraterritoriality, sovereignty, and the foundations of international law*, *in* THE EXTRATERRITORIALITY OF LAW: HISTORY, THEORY, POLITICS, 169, 177-178 (Daniel Margolies, Umut OZsu, Maia Pal, & Ntina Tzouvala eds., 2019).

[93] Currie, *supra* note 22, at 82.