SciencesPo
CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

INTERNET FRAGMENTATION'S OUTWARD TURN

Mailyn FIDLER

Visiting Assistant Professor
Harvard Law School
J.D., Yale Law School

June 2025

Table of Contents

Abstract

Internet fragmentation has turned outward. Internet fragmentation is often explained as inward-looking, a way for countries to exert sovereignty and control over a global network within their own borders. But this framing is too simple. Internet fragmentation has shifted from being a tool of domestic politics to a tool of power projection. The means of Internet fragmentation have evolved from filtering, blocking, and banning, to semiconductor export controls, undersea cable sabotage, and contestation of international legal frameworks. Now, states, along with private actors, use Internet fragmentation to deny or degrade the experience of the Internet in other states rather than regulate the experience in their own. This new form of Internet fragmentation shades from protectionism into aggression, a shift that reflects increased global tensions and in turn raises the risks of global conflict.

Introduction

The critique of the "Splinternet"[1] typically goes something like this: the Internet is turning into walled gardens, architected by national governments in conjunction with private power.[2] This kind of fragmentation is fundamentally inward looking. Internet fragmentation is typically viewed as a tool deployed to shore up domestic power, to keep wanted things in and unwanted things out.[3] The classic example of Internet fragmentation is the pursuit of national Internets: a state allows networked communication within its borders, where it can control it, but seeks to stop that network at its borders.[4] More recently, scholars have included actions such as banning foreign software and passing laws that force Internet infrastructure to comport with local political demands as forms of Internet fragmentation, new stones in the walled garden.[5] Critics contend that this trend is detrimental and ought to be reversed.[6] Most notably, Internet fragmentation fosters ills of isolationism, including parochialism in politics and trade.[7]

[1] The Splinternet was first used to describe the possibility of technically separate, parallel Internet networks where different rules could apply to support different goals. *See* Clyde Wayne Crews, *On My Mind*, FORBES (Apr. 2, 2001), https://www.forbes.com/forbes/2001/0402/036.html. It has since primarily been used to describe networks for a variety of reasons, from political to commercial, typically as a pejorative. *See, e.g.*, Evgeny Morovoz, *Think Again: The Internet*, FOREIGN POL'Y (Apr. 26, 2010), https://foreignpolicy.com/2010/04/26/think-again-the-internet/.

[2] *See, e.g.*, Mark Lemley, *The Splinternet*, 70 DUKE L. J. 1397 (2021).

[3] Anupam Chander, *The National Security Internet*, 114 Geo. L. J. __, 1 (forthcoming 2025).

[4] MILTON MUELLER, WILL THE INTERNET FRAGMENT? SOVEREIGNTY, GLOBALIZATION, AND CYBERSPACE (2017); Jonah Force Hill, *Internet Fragmentation*, HARVARD BELFER CTR. at 5 (2012).

[5] Lemley, *supra* note 2, at 1400-01 (using examples of China and Russia banning U.S. companies and characterizing the European Union's policies as essentially "dividing the U.S. experience [of Internet products] from the European experience."); Chander, *supra* note 7, at 1 (arguing that the TikTok "saga" is of a piece with the Chinese "Delete America" policy).

[6] Lemley, *supra* note 2, at 1399 ("The balkanization of the Internet is a bad thing and we should stop it if we can."); Chander, *supra* note 5 (what Chander calls "national security firewalls" are "expensive, harm trade, intrusive, undermine competition, easy to evade, and, worst of all, increase the risk of authoritarian control."); Clement Perarnaud et al., *'Splinternets': Addressing the Renewed Debate on Internet Fragmentation*, EUR. PARL. RES. SVC. at 1 (2022) (hereinafter "Splinternets Report").

[7] Chander, *supra* note 7, at 10-11.

This Article argues that this trend is more multifaceted than this standard account presents.[8] Internet fragmentation is experiencing an outward turn. This tool is now used not only to tend to one's own walled garden but to make others' gardens worse. If the Internet fragmentation of yesterday threatened democracy and deepened autocracy, [9] impeded economic growth, and thwarted global cooperation, the Internet fragmentation of today projects power and threatens conflict.

Part I situates standard examples of Internet fragmentation as inward looking, deployed primarily to shore up a state's domestic sovereignty. Part II demonstrates Internet fragmentation's new outward turn. Using examples of semiconductor sanctions, undersea cable sabotage, selective infrastructural investment, and fragmentation of Internet-related laws, this Part offers an account of new, and more aggressive, forms of Internet fragmentation.

This new form of Internet fragmentation reads more like low-level conflict than pursuit of Internet autonomy—the border skirmishes of a balkanized network. Understanding this outward turn is important because it locates these seemingly disparate policy choices within a common framework and reveals their potentially damaging effects. And, placing Internet fragmentation on the ladder of conflict makes it clear that policymakers have a choice between pursuing escalation or de-escalation in response.

I – Standard Views of Internet Fragmentation

A. The Beginnings of Internet Fragmentation

Internet fragmentation is often held at odds with the founding vision of the Internet. The technical structure of the Internet enabled, in a new way, "open, interoperable

[8] *See also* Juan Ortiz Freuler, *Infrastructural Power: State Strategies for Internet Control*, 14 INTERNET L. & POL'Y REV. 1 (2025) (arguing for moving beyond old models of Internet fragmentation to one focusing on broader concepts of infrastructural control.)

[9] Florence G'Sell, *Digital Authoritarianism: From State Control to Algorithmic Despotism*, OXFORD HANDBOOK OF DIGITAL CONSTITUTIONALISM (forthcoming).

and unified"[10] communication and information-sharing across borders.[11] The Internet allowed "every device. . .to exchange data packets with any other device that was willing to receive them."[12] In this way, the Internet seemed to embody maximalist technical openness.[13] Many, particularly in the West, hooked this technological openness to political values. The U.S. State government, across multiple administrations, adopted the "free flow of information across borders" as a goal, heralding such openness as pro-democratic.[14]

Internet fragmentation, in contrast, involves technical "restrictions, blockages, and cleavages" in the network.[15] For proponents of openness, Internet fragmentation is a concern. Critics worried that Internet fragmentation was "chip[ping] away. . .at the Internet's enormous capacity to facilitate human progress."[16] Economically, critics worry that this kind of fragmentation disrupts the at-scale economic benefits of the web.[17] Politically, critics worried that fragmentation would "shrinking" the world and result in more parochial politics, with knock-on effects for global institutions and cooperation.[18] For example,

[10] Hill, *supra* note 4, at 5.
[11] TIM WU & JACK GOLDSMITH, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006) at 25, *citing* FRANCES CAIRNCROSS, THE DEATH OF DISTANCE (2001) (explaining early internationalist views of the internet).
[12] William Drake, Vincent Cerf, and Wolfgang Kleinwachter, *Internet Fragmentation: An Overview*, WORLD ECONOMIC FORUM (2016); Nathaniel Fick & Jami Miscik, *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, COUNCIL ON FOREIGN RELATIONS, INDEPENDENT TASK FORCE REPORT NO. 80 (2022).
[13] *Id*.
[14] *See, e.g., U.S. Dep't of State, Global Internet Freedom Task Force,* U.S. DEP'T OF STATE (2001-2009) https://2001-2009.state.gov/g/drl/lbr/c26696.htm; *U.S. Dep't of State, Internet Freedom and Technology and Human Rights*, U.S. DEP'T STATE (last accessed Jul. 10, 2024), https://www.state.gov/internet-freedom-and-technology-and-human-rights/.
[15] *See* MUELLER, *supra* note 4 at 28.
[16] Drake, Cerf, & Kleinwachter, supra note 12, at 3.
[17] *See, e.g.*, Sarah Box, *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*, 36 GLOB. COM. INTERNET GOV. PAPER SERIES (2016), at 2.
[18] *See, e.g.*, Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 367-8 (2018) (describing the "cosmopolitan view" of the internet); Anupam Chander, *Trump v. Tiktok*, 55 VAND. J. TRANSNAT'L L. 1145, 1165 (2022), *citing Editorial Board, Opinion, India isn't just fracturing the Internet with its ban on Chinese app. It's shrinking it., WASH. POST (July 4, 2020), https://www.washingtonpost.com/opinions/global-opinions/india-isnt-just-fracturing-the-internet-with-its-ban-onchinese-apps-its-shrinking-it/2020/07/03/e5d0cad8-bbcb-11ea-8cf5-9c1b8d7f84c6_story.html.*

fragmentation has been criticised for undermining the applicability of international law—particularly human rights law—to the governance of the Internet.[19]

The canonical example of this kind of Internet fragmentation was the development, or attempted development, of "national" Internets. These "national" internets are separated to a degree or entirely from the rest of the network. For example, Iran, as early as 2006, publicly indicated plans to build such an Internet[20] and may have begun testing it.[21] Similarly, in 2019, Russia passed a law about developing a "sovereign RuNet." This law mandated that Internet traffic had to pass through government-approved internet exchange points.[22] In 2021, Cambodia passed a law requiring all incoming Internet traffic to enter through a single-entry gate.[23] These efforts were not successful to the degree their champions had proclaimed they would be.[24] But all of these efforts demonstrate a political desire to prioritize domestic political objectives over full openness.

B. The Sovereignty Splinternet

The standard worries about Internet fragmentation reflect its use as a tool of retrenchment and isolationism. Internet fragmentation, as described, is inward-looking, reflecting a core set of political goals: intentional efforts by national governments to subordinate the Internet to domestic sovereign control.[25] This

[19] Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393 (2013); Michael Karanicolas, *Understanding the Internet as a Human Right*, 10 CAN. J. L. & TECH. 2 (2012).
[20] *See* MUELLER, *supra* note *supra* note 4, at 50.
[21] Saeed Kamali Dehghan, *Iran Clamps Down on Internet Use*, GUARDIAN (Jan. 5, 2012), https://www.theguardian.com/world/2012/jan/05/iran-clamps-down-internet-use.
[22] *Splinternets Report*, *supra* note 6, at 26; this echoed earlier calls for development of a sovereign internet in 2014, *see* MUELLER, *supra* note *supra* note 4, at 51.
[23] *A Proposal in Cambodia Would Turn the Country's Internet into a National Internet*, INTERNET SOC'Y (Dec. 1, 2023), https://www.internetsociety.org/resources/internet-fragmentation/cambodias-national-internet-gateway/.
[24] *See* MUELLER, *supra* note 4, at 52 (describing limited evidence of success of both the Iranian and Russian efforts); *Splinternets Report*, *supra* note 6, at 2.
[25] I draw inspiration for this term from Mueller's term "alignment" fragmentation and the work of Polatin-Reuben and Wright, which Mueller cites, describing fragmentation as "subjugation of the cyber domain to local jurisdictions." See MUELLER, *supra* note 4, at 33; D. Polatin-Reuben & J. Wright, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet*, 4th Usenix Conference on Free and

Article will use the term "subordination fragmentation" to describe this type of Internet fragmentation.[26] In other words, this type of fragmentation refers to governments intentionally implementing policies or laws resulting in technical "restrictions, blockages, and cleavages" on the Internet in ways that allow them to assert sovereign control over this domain, much as they aim to assert control over their territorial air and sea space.[27]

This assertion of control reflects the pursuit of a type of sovereignty—domestic sovereignty. The Internet, an outside, global force, brings with it a degree of threat to a decidedly national entity, the state. In international law, sovereignty is typically defined as "supreme authority within a territory."[28] Building on this concept, international relations scholar Stephen Krasner defines domestic sovereignty as the "the ability of public authorities to exercise effective control within the borders of their own polity."[29] This control can extend to any number of dimensions, from economics to speech of citizens to assertion of physical control over resources. The Internet can hinder a sovereign's ability to exercise effective control of these dimensions within their state.

Rather than embrace a global network, many states have sought to assert control over the portion of that global network running through their borders.[30] Milton Mueller uses the term "alignment" to describe this process of "forc[ing] the round peg of global communications into the square hole of territorial states."[31]

Open Communication on the Internet, https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf.

[26] I draw inspiration for this term from Mueller's term "alignment" fragmentation and the work of Polatin-Reuben and Wright describing fragmentation as "subjugation of the cyber domain to local jurisdictions." See MUELLER, *supra* note 4, at 33; D. Polatin-Reuben & J. Wright, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet*, 4th Usenix Conference on Free and Open Communication on the Internet, https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf.

[27] *See* MUELLER, *supra* note 4, at 28.

[28] Samantha Besson, *Sovereignty*, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (Anne Peters and Rudiger Wolfrum, eds.) (2011).

[29] STEPHEN KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY (1999) AT 4.

[30] *See* MUELLER, *supra* note 4, at 28 (Internet fragmentation is really about "the attempt by governments to align the Internet with their jurisdictional boundaries.")

[31] Milton Mueller, *Internet Fragmentation Exists, But Not in the Way That You Think*, NET POLITICS, COUNCIL ON FOREIGN RELATIONS (June 12, 2017), https://www.cfr.org/blog/internet-fragmentation-exists-not-way-you-think.

States have not found it as hard as that metaphor might suggest, using a combination of technical and legal tools to subordinate the Internet. As Professor Jack Goldsmith writes, this vision of openness was in many ways experienced as uniquely American, and "other nations have rejected the attempted export of American values and are increasingly effective at imposing their own values on the internet."[32] This might take the form of reasserting "control [over] their own people."[33] As discussed further below, blunt Internet shutdowns and more complicated filtering mechanisms chill speech. Other restrictions and blockages are motivated by protecting economic interests.[34] And other states seek to enforce their territorial identity socially or physically, perhaps explaining the desire to censor speech or route Internet traffic through easily physically controllable exchange points.[35] Subordination fragmentation is, essentially, the exercising of control over the Internet within one's own country in ways that create "restrictions, blockages, and cleavages" of the Internet.

One particularly notable example of subordination fragmentation is China's Golden Shield Project—also known as the Great Firewall—which exemplifies this subordination fragmentation. China has massively invested in legal frameworks allowing and in technical capabilities enabling monitoring, filtering, and blocking of online content.[36] The project is concerned with controlling politically sensitive

[32] *See, e.g.*, Jack Goldsmith, *The Failure of Internet Freedom*, in THE PERILOUS PUBLIC SQUARE: STRUCTURAL THREATS TO FREE EXPRESSION TODAY at 241 (David Pozen ed., 2020). One example of U.S. exporting values was its introduction of a resolution at the UN Human Rights Council affirming that the human rights "that people have offline must also be protected online. The resolution passed. *See* U*N Human Rights Council: First Resolution on Internet Free Speech*, LIBRARY OF CONGRESS (July 12, 2012), https://www.loc.gov/item/global-legal-monitor/2012-07-12/u-n-human-rights-council-first-resolution-on-internet-free-speech/; see also Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393 (2013).
[33] DENNIS BROEDERS, THE PUBLIC CORE OF THE INTERNET (2015), AT 17.
[34] *Id*.
[35] *Id;* Beth Simmons & Rachel Hulvey, *Cyberborders: Exercising State Sovereignty Online*, 95 TEMPLE L. REV. 617, 617 (2023).
[36] Jamie P. Horsely, *Behind the Façade of China's Super-Regulator*, DIGICHINA (Aug. 8, 2022), https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/; Yaqiu Wang, *In China, the 'Great Firewall' Is Changing a Generation*, POLITICO (Sept. 1, 2020), https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385;

information and combating outside influence, among other aims.[37] Although this project does not bluntly cut off the network at the borders in the same way a national Internet might, it similarly extends domestic control over the network within a country, creating restrictions and blockages that make the experience of the Internet manifestly different within than without.

Internet shutoffs also reflect subordination fragmentation. With Internet shutoffs, governments simply shut off the Internet, not just censor certain websites, within their borders when the Internet's use does not suit their interests.[38] For example, in 2025, about a third of Russia's Internet users were unable to access most websites.[39] This shutdown appeared to be a "dry run" for a complete shutdown of the web, if the government deemed it necessary.[40] This "kill-switch" method of fragmentation has been increasingly implemented around the world during times of political turmoil.[41] This form of fragmentation is important to include because it requires less investment than a Great Shield or national Internet and can be deployed rapidly and selectively in response to changing situations. This tactic is not limited to Russia; rather, it is used widely, with countries ranging from India to Gabon deploying this tactic during protests, conflicts, and around elections as a means of control.[42]

---

[37] Sonali Chandel et al., *The Golden Shield Project of China: A Decade Later—An In-Depth Study of the Great Firewall*, 2019 INT'L CONF. ON CYBER-ENABLED DISTRIBUTED COMPUTING AND KNOWLEDGE DISCOVERY (2019).

[38] *An Overview of Global Internet Shutdowns,* ACCESS NOW (2023), https://www.accessnow.org/campaign/keepiton/#global-tracker.

[39] Daria Dergacheva, *Shutting Down the Net: The Growing Threat of Russian Internet Censorship*, GLOBAL VOICES (Jan. 22, 2025), https://globalvoices.org/2025/01/22/shutting-down-the-net-the-growing-threat-of-russian-internet-censorship/.

[40] Id.

[41] Zach Rosson, Felicia Anthonio, & Carolyn Tackett, *The Most Violent Year: Internet Shutdowns in 2023*, ACCESSNOW (May 15, 2024), https://www.accessnow.org/internet-shutdowns-2023/ (describing Internet shutdowns as the "go-to tool for both democratic and authoritarian regimes to suppress fundamental rights and conflicts as the "leading driver for internet shutdowns."); Ihueze Nwobilor, *Navigating Internet Fragmentation in the African Context: Challenges and Opportunities*, PARADIGM INITIATIVE (May 25, 2024), https://paradigmhq.org/navigating-internet-fragmentation-in-the-african-context-challenges-and-opportunities/ (noting that a third of internet shutdowns in 2021 happened in Africa).

[42] *Unabashed and Unabated: India Leads the World Shutdown Count for Sixth Year*, ACCESS NOW (May 15, 2024), https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/; *#KeepItOn: Authorities in Gabon Must*

More controversially, scholars have also positioned data localization as a form of Internet fragmentation.[43] Data localization refers to laws that require certain data to be stored within the territorial borders of a state.[44] Professor Anupam Chander and Uyên P. Lê systematically catalogued reasons states offer for data localization—and each of these reasons are textbook aspects of domestic sovereignty.[45] Chander and Lê offer: some countries pursue data localization because it guards against incursions of foreign intelligence agencies.[46] Taking steps to mitigate foreign intelligence incursions is a classic pursuit of the domestic sovereign: Surveillance can interfere with the internal affairs of a state, because a foreign government's detection of communications relating to the state's affairs could affect the state's ability to take actions in its own interest. [47] Bolstering against foreign surveillance thus bolsters domestic autonomy.

In Chander and Lê's account, some states pursue data localization because it bolsters domestic law enforcement capabilities.[48] Police are intimately related to a sovereign's monopoly on legitimate use of force, a key aspect of sovereignty.[49] Russia's data localization efforts seem particularly motivated by this aspect of

Safeguard Open and Secure Internet Access During Elections, ACCESS NOW (Apr. 8, 2025), https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/; Shrinking Democracy, Growing Violence: Internet Shutdowns in 2023, Access Now

[43] Lemley, *supra* note 2, at 1420; *Internet Way of Networking Use Case: Data Localization*, INTERNET SOC'Y (2020) ("data localization…[will result in a] more constricted and less resilient network with suboptimal performance, retrofitted to comply with national borders."); *see also* Christopher Kuner, *Data Nationalism and its Discontents*, 64 EMORY L. J. ONLINE 2089 (2015); Jennifer Daskal & Paul Ohm, *Debate: We Need to Protect Strong National Borders on the Internet*, 17 COLO. TECH L.J. 13 (2018); Felicity Deane, *Trade in the Digital Age: Agreements to Mitigate Fragmentation*, 14 ASIAN J. INT'L L. 154 (2024).

[44] Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1696 (2018).

[45] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677, 679 (2015).

[46] Chander and Le, *supra* note 45 at 713.

[47] *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 304 (2015), *citing* Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, in ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, at 1,12 (Roland Stanger, ed., 1962).

[48] Chander and Le, *supra* note 45 at 700, 713.

[49] MALCOM ANDERSON, POLICING THE WORLD: INTERPOL AND THE POLITICS OF INTERNATIONAL POLICE CO-OPERATION (1989) AT 17.

sovereignty, for instance.[50] Still other states pursue data localization in pursuit of domestic economic growth. Growing a country's economy in ways that are resilient to outside influence is another major domestic concern of the sovereign.[51] Chander and Lê offer Nigeria as one example whose data localization seems primarily motivated by economics.[52] Nigeria issued regulations in 2013 requiring that information and communications technology companies "host all subscriber and consumer data locally in Nigeria."[53] All of these motivations for a specific form of subordination fragmentation—namely, data localization—can be understood as expressions of a domestic political imperative to safeguard national sovereignty.

In many ways, the European Union's General Data Protection Regulation functions as a form of data localization, even though its stated intentions are unrelated to data localization.[54] The EU's data protection regulations allow transfer out of the Union only if appropriate safeguards are in place, adding friction and sometimes "breaks" in the network.[55] Other forms of digital protectionism function as data localizing forces, too.[56]

---

[50] Chander and Le, *supra* note 45 at 701, 713 (quoting Russian parliament member urging passage of data localization laws that would enable "e-mail and social networking companies. . .[to] be subject to domestic law enforcement search warrants.")

[51] The debates around odious sovereign debt encapsulates this notion well. Arguably, demands that a new, legitimate government repay the debt of its former, illegitimate government would themselves be illegitimate. *See, e.g.*, ODETTE LIENAU, RETHINKING SOVEREIGN DEBT (2014), AT 43.

[52] *Id.*, at 700, 713. *See id*. at 708-713 for a table of data localization laws categorized by rationale cited.

[53] Lukman Abdulruf & Oyeniyi Abe, *The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations*, UNIVERSITY OF WITWATERSRAND SCHOOL OF LAW, at 2 (2021).

[54] Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 1 ("This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.")

[55] *Splinternets Report*, *supra* note 6, at 30, 36, 37, 38-42, 46.

[56] *See, e.g.*, Susan Aaronson, *What are We Talking About When We Talk About Digital Protectionism?*, 18 WORLD TRADE REV. 541 (2019) (examining protectionist implications of practices like filtering, censorship, localization, and more).

Another example of legal Internet fragmentation is content fragmentation, which occurs when different kinds of content are not equally available across an otherwise interoperable network.[57] Consider the French government's efforts to require Yahoo to prevent French users from accessing images of Nazi memorabilia up for auction on the site,[58] or Germany's hate speech law.[59] The Internet a user experiences is different, based on their location. Although different in implementation from the Golden Shield Project, content fragmentation similarly reflects political judgements about what content is allowable for its citizens, subordinating openness to that decision.

All of these examples represent governments, in conjunction with private parties, making decisions to "cleave" the Internet, or the experience of the Internet, within their borders in ways that either keep desired data in and undesired data out. States use a range of technical and legal levers to accomplish shaping their own walled gardens as they like. What started as primarily a practice of repressive governments has gradually expanded, with states of all political persuasions subordinating the Internet for inward-looking, sovereignty-related aims.

II – Internet Fragmentation as Power Projection

A. The Outward Turn

Yet, Internet fragmentation has started to turn outward. It is no longer just used as a tool to align the Internet with the demands of domestic sovereignty. Internet fragmentation has become both an aim of and byproduct of power projection. Instead of reading primarily like a tool of protectionism, this tool has started to shade into aggression.

[57] *Splinternets Report*, *supra* note *supra* note 6, at 5.
[58] Joel Reidenberg, *Yahoo & Democracy on the Internet*, 42 JURIMETRICS 261 (2002) (describing the French efforts in detail).
[59] Joris van Hoboken & Ronan O Fathaig, *Regulating Disinformation in Europe: Implications for Speech and Privacy*, 6 U.C. IRVINE J. OF INT'L, TRANS. & COMP. L. 9 (2021) (describing 2017 Germany's Network Enforcement Act).

This shift is significant because of its implications for global order. Worries about subordination fragmentation were primarily about bolstering anti-democratic practices and eroding the existing global economic and international legal order. But Internet fragmentation's outward turn threatens increased conflict. Internet fragmentation becomes something done to a state rather than something a state chooses for itself. The below sections explore semiconductor export controls, sabotage of submarine cables, selective investment in Internet infrastructure, and contestation over developing, international legal frameworks for the Internet as instances of outward-directed Internet fragmentation. Understood as instances of power projection, states can better calibrate their responses to these Internet fragmentation moves.

Understanding this new, outward turn in Internet fragmentation first requires defining power and its projection. The examples that follow illustrate examples of power projection and are not instances of fragmentation; the subsequent sections then turn to instances of power projection as fragmentation. Like sovereignty, power is a multilayered concept. Traditionally conceived of in military terms, international relations has come to embrace a broader conception of power. States can project power in traditional means but also in "structur[ing] a situation so that other countries develop preferences or define their interests in ways consistent with its own."[60] Such soft power can come from "cultural and ideological attraction as well as rules and institutions of international regimes."[61] Importantly, most policy choices are neither solely oriented towards domestic sovereignty or of power projection. But recent Internet fragmentation has reflected an increasing concern with outward-facing effects.

The "Brussels Effect" is a primary example of this projection of power through rules.[62] The European Union has developed regulations that have, in turn, "become entrenched in the legal frameworks of developed and developing markets alike, positioning the region as a regulatory power even where it lags in

[60] Joseph Nye, *Soft Power*, 80 FOREIGN POL'Y 153, 168 (1990).
[61] *Id*.
[62] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).

technological innovation or measures of hard power.[63] As Anu Bradford argues, this externalization of rules benefits the domestic sovereignty of the European Union by creating a bigger market for European companies already compliant with these rules.[64] But, other scholars position this tactic as Europe's primary means of projecting power.[65]

Infrastructure and investment can also be forms of soft power. China's Belt and Road Initiative is a significant contemporary example. This project aims to create transportation, energy, and informational interconnectedness between China and partner countries.[66] China has "both geopolitical and economic motivations" for the initiative.[67] The initiative seeks greater trade between China and affected countries—which certainly benefits China and affects its ability to project domestic sovereignty. But it also is a way of projecting power. The debt agreements that fund these infrastructural investments tend to give China leverage over the receiving countries, and China has been known to introduce surveillance mechanisms into telecommunications infrastructure deployed as part of the Initiative.[68] Each new project exercises and further boosts China's ability to extend influence.

In the following case studies, law, infrastructure, and material power intersect in recent instances of Internet fragmentation. These examples are intentionally

[63] *Id*. at 1; see also Mailyn Fidler, *African Data Protection Laws: Politics, but as Usual, in*
AFRICAN DATA PROTECTION LAWS (Raymond Atuguba Akongburo et al. eds, 2024) (describing the staying power of European data protection regulations in African laws).
[64] Bradford, *supra* note 62, at 35.
[65] NORMATIVE POWER EUROPE, RICHARD WHITMAN, ED. (2011); Jan Zielonka, *Europe as a Global Actor: Empire by Example?*, 84 INT'L AFF. 471 (2008); Ian Manners, *The Normative Ethics of the European Union*, 84 INT'L AFF. 45 (2008).
[66] James McBride, Noah Berman, and Andrew Chatzky, *China's Massive Belt and Road Initiative*, COUNCIL ON FOREIGN RELATIONS (Feb. 2, 2023), https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative#chapter-title-0-4.
[67] *Id.*
[68] Anna Gelpern et al., *How China Lends*, AID DATA (2021); Mailyn Fidler, *African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts*, NET POLITICS, COUNCIL ON FOREIGN RELATIONS (Mar. 7, 2018), https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

selected to depart from the conventional patterns of fragmentation observed in previous decades. Nevertheless, each case involves "restrictions, blockages, and cleavages" within the network, either deliberately deployed as instruments of power or as consequences arising from the projection of power.[69]

B. The Sanctions Splinternet

Mark Lemley and Anupam Chander position the recent popularity of export controls over certain types of hardware as a form of Internet fragmentation.[70] For example, the U.S. has implemented export controls to prevent American semiconductor chips and other key components of artificial intelligence products from being used in certain foreign technology.[71] Other Western countries have acted similarly. China has implemented export regulations on certain kinds of data with national security implications as of 2022—with national security implications defined broadly.[72]

These actions constitute Internet fragmentation. They result in cleavages in the network because access to the same technology aids standardization, and standardization aids interoperability. As Lemley puts it, these kinds of moves risk "moving back to a world where what you can see and who you can talk to is a function of what software and hardware you use. And that, in turn, increasingly will depend on where you live."[73]

Lemley and Chander characterize these export controls as continuous with subordination fragmentation—among which they include actions like banning

[69] *See* MUELLER, *supra* note 4, at 28.
[70] Lemley, *supra* note 2, at 1412; Chander, *supra* note 3, at 40.
[71] *Framework for Artificial Intelligence Diffusion*, DEP'T OF COMMERCE (Jan. 15, 2025), https://public-inspection.federalregister.gov/2025-00636.pdf; *Ana Swanson, U.S. Delivers Another Blow to Huawei, N.Y. TIMES (Oct. 22, 2020, 11:33 AM), https://nyti.ms/3cC57QX.*
[72] Chander, *supra* note 3, at 22, *citing* Outbound Data Transfer Security Assessment Measures, Art. 4 (translation by DigiChina), https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/.
[73] Lemley, *supra* note 2, at 1414.

Huawei technology from portions of the U.S. market or the TikTok ban.[74] Lemley points to nationalism and concerns about control over hardware to implement domestic surveillance as the explanation.[75] Chander positions export controls as part of the "national security" internet, motivated in part by a need to keep domestic networks free of foreign surveillance—another form of "keep out."[76]

But these explanations, while not incorrect, are incomplete. These sanctions splinter the Internet not just with the aim of protecting the enacting country but of affecting other countries. Export controls deny affected countries the ability to be fully integrated into the international internet. Indeed, export controls as a means of denial or deprivation is well-established in sanctions literature.[77] Much like weapons sanctions seek to prevent the development of weapons programs in Iran, for instance, Internet-related sanctions seek to slow or separate development of technology.[78]

Export bans like this are different in kind, not just degree, from import bans, like U.S. restrictions on Huawei technology. Import bans are structured more like other subordination fragmentation moves. Just like content fragmentation seeks to control the experience of the Internet within a sovereign territory, import bans seek to control the hardware of the Internet within a sovereign territory. Import bans clearly affect the partner country. But the balance shifts with export controls: Export controls do not intrinsically affect the technological landscape of the issuing country. Instead, its initial effects are primarily directed outward. For instance, the U.S. Huawei restrictions, aimed to protect American networks from Chinese surveillance and reduced Chinese economic opportunities.[79] The U.S. AI-related export controls aim to prevent Chinese technological development.

[74] Id at 1410; Chander, *supra* note 3, at 7.
[75] Lemley, *supra* note 2, at 1414.
[76] Chander, *supra* note 3, at 57.
[77] See, e.g., Homer E. Moyer, Jr., and Linda A. Mabry, *Export Controls as Instruments of Foreign Policy: The History, Legal Issues, and Policy Lessons of Three Recent Cases*, 15 LAW & POL'Y INT'L BUS. 1 (1983).
[78] Daniel Drezner, *How Not to Sanction*, 98 INT'L AFF. 1533, 1540 (2022).
[79] Chander, *supra* note 3.

A shift into export controls brings Internet fragmentation into a more aggressive foreign policy space. No longer is a state only seeking to exert control over its own networks, but now states are also seeking measure of control over the experience of networks in other countries, as well. Although used for a range of foreign policy goals, export controls and trade sanctions have long been deeply interconnected with conflict. Historically, sanctions have been used to try to deter or retaliate against aggression.[80] Sanctions contributed to the tensions leading to the outbreak of World War II.[81] Indeed, sanctions are increasingly considered a "tool of modern warfare" – a tool as "deadly" as use of force.[82]

The shift into sanctions that splinter the Internet is more geopolitically aggressive than seeking to extend deeper control over one's own territory. Perhaps nationalizing Internets can be seen as a rejection of the Western global order. But it holds few concrete security risks. But splinternet sanctions shade into aggression, which magnifies the risks associated with Internet fragmentation. Even if considered purely defensive—the implementing country sees its security boosted by preventing the sanctioned country from accessing a technology—the security spiral means that such a move will affect the sanctioned country's own perception of security.[83] Countries may in turn respond with fragmenting moves, just as we have seen China and the U.S. trade related restrictions back and forth.[84] Internet fragmentation's outward turn likely begets more fragmentation.

C. The Sabotage Splinternet

A form of Internet fragmentation that is almost laughably blunt has emerged: the deliberate cutting of undersea fiber optic cables. Multiple times in 2024 and 2025, undersea cables in the Baltic Sea were likely sabotaged, possibly by Russia or

[80] Moyer and Mabry, *supra* note 77.
[81] NICHOLAS MULDER, THE ECONOMIC WEAPON: THE RISE OF SANCTIONS AS A TOOL OF MODERN WARFARE (2022).
[82] *Id*. (quoting President Woodrow Wilson).
[83] ROBERT JERVIS, PERCEPTION AND MISPERCEPTION IN INTERNATIONAL POLITICS (1976).
[84] In May 2025, the U.S. implemented restrictions that mirror Chinese restrictions on sensitive data. *See* Daniel Sutherland and Jim Dempsey, *Cybersecurity Risk from Kaspersky to TikTok*, LAWFARE (May 28, 2025), https://www.lawfaremedia.org/article/cybersecurity-risk-from-kaspersky-to-tiktok.

China.[85] Also in 2024, multiple cables in the Red Sea were cut, attributed to Houthi rebel attacks.[86] And, in 2025, news broke of China's new, deep-sea cable cutting ship, heralded as an escalatory development in international security.[87]

Cable cutting is Internet fragmentation at its most basic: the literal infrastructure of the Internet is fragmented when cables are cut. That Internet relies on a worldwide network of undersea fiber optic cables to deliver connectivity.[88] These cables carry data from one part of the Earth to another at very high speeds and have substantial strategic importance to both private and military actors.[89] Indeed, firms value undersea fiber optic Internet speeds so much that some have invested in new cable projects seeking gains of as little as five milliseconds over competitors.[90]

Cutting another country's cables—often far from the sabotaging country's territorial boundaries—makes little sense as a strategy primarily to shore up domestic sovereignty. Rather, it seems more a tactic to deny desired levels of interconnectedness to *other* countries. Saboteurs are projecting their power by cutting cables in other countries' own nautical backyards. This act fundamentally projects power: we can do this to you. We have the technological and material

[85] Johan Ahlander, Essi Lehto, and Andrius Sytas, *Two Undersea Cables in Baltic Sea Cut, Germany and Finland Fear Sabotage*, REUTERS (Nov. 18, 2024), https://www.reuters.com/business/media-telecom/telecoms-cable-linking-finland-germany-likely-severed-owner-says-2024-11-18/; Christina Anderson and Amelia Nierenberg, *Sweden Suspects 'Gross Sabotage' After Damage to Cable Under Baltic Sea*, N.Y. TIMES (Jan. 27, 2025), https://www.nytimes.com/2025/01/27/world/europe/cable-baltic-sea-sweden-damage.html.

[86] Jon Gambrell, *3 Red Sea Data Cables Cut as Houthis Launch More Attacks on the Vital Waterway*, AP NEWS (Mar. 4, 2024), https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a.

[87] Erin L. Murphy and Matt Pearl, *China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts*, CSIS (Apr. 4, 2025), https://www.csis.org/analysis/chinas-underwater-power-play-prcs-new-subsea-cable-cutting-ship-spooks-international.

[88] *See generally* NICOLE STAROSIELSKI, THE UNDERSEA NETWORK (2015).

[89] *Strategic Importance of, and Dependence On, Undersea Cables*, NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE (2019).

[90] *See, e.g.,* Joe Pappalardo, *New Transatlantic Cable Built to Shave 5 Milliseconds off Stock Trades*, POPULAR MECHANICS (Oct. 27, 2011), https://www.popularmechanics.com/technology/infrastructure/a7274/a-transatlantic-cable-to-shave-5-milliseconds-off-stock-trades/.

capability to deny you connectivity if and when we want. And, unlike export controls, we can (often) do so covertly.

Such tactics have a long history of conflict-adjacency. Both nation states and rebels have used this tactic to project (differing) levels of power. This tactic has a long history, although in the past it has been used during or on the eve of war, heightening its aggressiveness as a tactic. The Germans cut telegraph cables during World War I, and the United States did so in the Philippines and the Caribbean during the 1898 Spanish-American War.[91] Like the Houthis, other less powerful groups have also historically turned to planned or actual sabotage of telegraph wires.[92]

These historical examples indicate that cable cutting should spark worries about Internet fragmentation moving beyond handing autocrats a tool for repression or allowing continued domination of tech markets by certain actors. This form of Internet fragmentation may function as the telecommunications equivalent of border skirmishes: low intensity conflict that belies or will beget deeper friction. Internet fragmentation seems to have joined a collection of tactics, including state-sponsored cyber attacks, that contribute to low-intensity conflict.[93] If export controls deny adversaries access, cable cutting and similar tactics disrupt, degrade, and destroy access.[94] While these actions still might not reach the level

[91] Jonathan Reed Winkler, *Silencing the Enemy: Cable-Cutting in the Spanish-American War*, WAR ON THE ROCKS (Nov. 6, 2015), https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; JONATHAN REED WINKLER, NEXUS: STRATEGIC COMMUNICATIONS AND AMERICAN SECURITY IN WORLD WAR I (2008) AT 106.

[92] *Starosielski* at 34, *citing* Ariane Knuesel, *British Diplomacy and the Telegraph in Nineteenth-Century China*, 18 DIPLOMACY & STATECRAFT 517 (2007), (discussing indigenous Australian sabotage of telegraph wires and Chinese government potential plans to disrupt cable-laying).

[93] *See, e.g.*, Lennart Maschmeyer, *A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict*, 46 J. STRAT. STUDS. 570 (2023); JAI GALLIOT, FORCE SHORT OF WAR IN MODERN CONFLICT: JUS AD VIM (2019); Avi Kober, *Low-Intensity Conflicts: Why the Gap Between Theory and Practise*, 18 DEFENSE & SEC. ANALYSIS 15 (2002) (noting the increase in low-intensity conflict post-Cold War); Matthew C. Waxman, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, 87 INT'L L. STUD. 43 (2011); TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2017).

[94] This tactic is perhaps heading to the skies: Elon Musk has threatened to down his Starlink satellite communications network turned off during the Russian conflict with Ukraine. As Starlink expands to areas already underserved by Internet connections,

of aggression according to international law, they round out the saboteur's toolkit.[95]

D. The Inverse Splinternet: Selective Infrastructure Investment

All of the above examples of Internet fragmentation, both inward and outward-looking, involve breaks or cleavages in existing networks in ways that make the experience of the Internet different in different regions. Consider a different kind of fragmentation: blockages that prevent an area from developing full connectivity. That cut-off area, a connectivity desert, experiences many of the same effects as a walled garden that was created post hoc by fragmentation.

Such a connectivity desert does not have access to the full benefits of an open, interoperable, global Internet. In many ways, such a desert will experience many of the same difficulties as walled gardens. For instance, economic growth tends to be slower.[96] Certain democratizing influences will be absent.[97]

But the kind of fragmentation that connectivity deserts experience is different from subordination fragmentation in one crucial way. Subordination fragmentation is typically an active choice by governments, in conjunction with the private sector, to structure networks within a territory a certain way. The inverse fragmentation experienced by connectivity deserts is not typically primarily the choice of that territory. Rather, that lack of connectivity is deeply influenced by outside

---

this dependence on one private entity makes fragmentation easier, if not more likely. *See, e.g.*, Andrea Shalal and Joey Roulette, *US Could Cut Ukraine's Access to Starlink Internet Services Over Minerals, Say Sources*, REUTERS (Feb. 22, 2025), https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

[95] See, e.g., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2017); Convention for the Protection of Submarine Telegraph Cables (1884).

[96] *See, e.g.*, Georges V. Houngbonon, Justice Tei Mensah, and Nouhoum Traore, *The Impact of Internet Access on Innovation and Entrepreneurship in Africa*, WORLD BANK POLICY WORKING PAPER 9945 (2022).

[97] *See generally* PETER M. SHANE, DEMOCRACY ONLINE: THE PROSPECTS FOR POLITICAL RENEWAL THROUGH THE INTERNET (2004); *The Role of Technical Assistance and Capacity-Building in Fostering Mutually Beneficial Cooperation in Promoting and Protecting Human Rights*, UNITED NATIONS HUMAN RIGHTS COUNCIL, https://documents.un.org/doc/undoc/gen/g20/012/07/pdf/g2001207.pdf.

constraints, such as decisions by other countries to invest in telecommunications infrastructure.

This difference matters because it has substantial consequences for the "fragmented" country. Where subordination fragmentation bolsters domestic sovereignty, inverse fragmentation reflects the exercise of outside power over a territory, a sign of weak domestic sovereignty. States subject to inverse fragmentation are vulnerable to outside influence, rather than exercising forces against outside influence. While subordination fragmentation seemingly reduces vulnerability, inverse fragmentation deepens vulnerability. That sense of vulnerability, coupled with the consequences of fragmentation, has knock-on effects discussed below.

To illustrate this type of fragmentation and its stakes, consider the African continent and the relatively slow growth in access to fiber optic submarine cables. Robust undersea cable infrastructure provides a more reliable ticket to the global Internet. Yet access to these cables has geographically been uneven, with these differences especially pronounced in the African context. The African continent was among the last regions to connect to undersea fiber optic infrastructure, which carries substantially faster and more reliable Internet speeds.[98] For instance, in 2001, sub-Saharan Africa had one undersea fiber optic cable with one landing point, compared to five cables in Latin America with at least 50 landing points.[99]

This divergence can largely be explained by strategic investment decisions made by Western states in global telecommunications infrastructure through around

[98] *See, e.g.*, Barney Warf, *International Competition Between Satellite and Fiber Optic Carriers: A Geographic Perspective*, 58 PROF. GEO. 1, 10 (2006) ("satellites … can compete with transoceanic submarine cables only with great and mounting difficulty.")
[99] The Brazilian Festoon (1996), with 14 landing points; the Columbian Festoon (1997), with 5 South American landing points; the Venezuelan festoon (1998) with 12 landing points; Americas-II (2000), with 4 landing points; GlobeNet (2000), with 4 landing points; South American Crossing (2000), with 10 landing points. See Submarine Cable Map, Telegeography (last accessed May 28, 2025), https://www.submarinecablemap.com/.

2010[100] Up to that point, American companies primarily directed their investments toward Latin America, focusing on regions geographically and economically closer to the United States.[101] In contrast, European companies invested in undersea cable infrastructure around the African continent. However, the location and scale of these investments were driven less by African connectivity needs and more by broader strategic objectives, such as enhancing links with Asian markets. Because these objectives were broadly shared among European countries, investments tended to converge along specific routes, leading to repeated use of similar cable paths and landing points. This convergence produced significant redundancy in certain regions—where connectivity was substantially enhanced—while leaving other areas under-connected or entirely excluded.[102] As Professor Nicole Starosielski puts it, these investor dynamics generated, in the undersea cable network, one of the "most static [network] in the history of communications."[103]

As a result, some African countries are now better integrated into the "modern" global network infrastructure, while others remain disconnected and effectively excluded from the new information superhighway, relying instead on slower and less reliable satellite connections. For example, consider Senegal and Guinea—

[100] *See, e.g.*, Jonas Hjort and Jonas Poulsen, *The Arrival of Fast Internet and Employment in Africa*, 109 AM. ECON. REV. 1032, 1033 (2019) (noting the early 2010s as a turning point in European-based arrival of submarine cables); Ewan Sutherland, *Undersea Cables and Landing Stations Around Africa: Policy and Regulatory Issues*, 25th EUR. REG. CONF. ON INT'L TELECOM. SOC'Y (2014) (detailing shift in investors around 2010); Dwayne Winseck, *Internet Infrastructure and the Persistent Myth of U.S. Hegemony*, in INFORMATION, TECHNOLOGY AND CONTROL IN A CHANGING WORLD (2019) (indicating a recent shift away from Western dominance in global communications infrastructure investment); Joel Cariolle, Telecommunication Submarine-Cable Deployment and the Digital Divide in Sub-Saharan Africa, Fondation Pour Les Études et Recherches Sur Le Développement International, Working Paper 241 (2018); *but see* Russell Southwood, *The Ugly Underbelly of the Communications Revolution: Corruption, Cronyism, Regulation and Government* (1999-2000), AFRICA 2.0 (2022) (detailing domestic influences on telecoms fragmentation).

[101] *See, e.g.*, JOSE ANTONIO OCAMPO AND JUAN MARTIN, A DECADE OF LIGHT AND SHADOW: LATIN AMERICA AND THE CARIBBEAN IN THE 1990S (2003) AT 176 (citing the U.S. as one of the two most active foreign investors in Latin American telecommunications companies after privatization).

[102] Landing sites are usually considered the most vulnerable parts of cables, adding both increased expense and risk with every additional "surfacing." *See* Starosielski, *supra* note 88, at 38-39.

[103] *Id.*

two countries situated in broadly comparable locations along the west coast of the African continent. As of 2025, Senegal hosts six submarine cables at its landing points, whereas Guinea has only one.[104] Senegal's first cable arrived in 2002, with Guinea's connection only coming in 2012.

This altered landscape of connectivity represents "restrictions, blockages, and cleavages" in the network. Certainly, these cleavages are not the same as, for example, a country requiring all traffic to enter its borders through a single government-controlled exchange.[105] However, the network remains fragmented, and this fragmentation continues to produce significant consequences.

A primary consequence is what may be termed inverse fragmentation, in which fragmentation reflects the projection of power—typically by dominant Western states—into less powerful regions. Effort nominally bringing connectivity ended up with inadvertent fragmenting effects. This is a novel form of fragmentation that should be considered alongside subordination fragmentation. It is an inherently outward-facing form of fragmentation and reflects the exercise of economic and infrastructural power over other states.

Domestically, those fragmenting effects have consequences for the affected countries, from the economic to the political. Affected countries are also more vulnerable to interruptions in their non-redundant networks—vulnerability is embedded within connectivity.[106] And political vulnerability is embedded as well: the form of the network reminds African countries of the limits of their self-determination. This sense of vulnerability gave rise to more fragmentation—the subject of the next section.

As the landscape of investment in infrastructure shifts, inverse fragmentation will likely shift or increase. As discussed above, China's massive investments in infrastructure come with certain pressures.[107] The United States has similarly

[104] Submarine Cable Map, supra note 99.
[105] Id.
[106] Solomon Moore, *Ship Accidents Sever Data Cables Off East Africa*, WALL ST. J. (Feb. 28, 2012); Brid-Aine Parnell, *Epic Net Outage as Four Undersea Cables Chopped*, THE REGISTER (Feb. 28, 2012), https://perma.cc/C93J-SMLJ.
[107] Rachel Savage and Duncan Miriri, *Post-COVID, China Is Back in Africa and Doubling Down on Minerals*, REUTERS (May 28, 2024),

exerted pressure on African nations to accept connectivity from Elon Musk's satellite company Starlink.[108] The terms of these deals as well as their geographic patterns will create new areas of inverse fragmentation and vulnerability. Deserts and walled gardens are certainly different—but they share similarities worth considering.

E. The Legal Splinternet

The law and the Internet are deeply intertwined. The law is often used to implement subordination fragmentation. Consider, for example, content fragmentation as implemented in several European jurisdictions: legislation imposes obligations on private entities to ensure that their content complies with specific legal standards. As a result, both the experience of using the Internet and the applicable legal regime governing it differ markedly in those jurisdictions compared to others.

The laws aspiring to govern the internet internationally, or at least multilaterally, have been subject to significant contestation and fragmentation. Although some of this legal fragmentation, like the content example, serve subordination fragmentation aims, other legal fragmentation acts as a means of projecting power. Recognizing this legal fragmentation is important for two reasons. First, it reflects another dimension of fragmentation: the Internet fragmentation problem looks worse when you consider both the technical and legal dimensions. Second, legal fragmentation is a tool available to less powerful states who might not have the ability to project power in other ways. Pushing back through Internet law, when pushing back materially is not possible, offers an alternate form of political contestation for these countries. Failing to see this within the lens of Internet fragmentation pursued by more powerful countries discounts its potential effects.

https://www.reuters.com/markets/commodities/post-covid-china-is-back-africa-doubling-down-minerals-2024-05-28/.

[108] Joshua Kaplan, Brett Murphy, Justin Elliott, and Alex Mierjeski, *The Trump Administration Leaned on African Countries. The Goal: Get Business for Elon Musk*, PROPUBLICA (May 15, 2025), https://www.propublica.org/article/trump-musk-starlink-state-department-gambia-africa-pressure.

Fragmentation of international law is the "proliferation of international regulatory institutions," "with overlapping jurisdictions and ambiguous boundaries." [109] Fragmentation of *Internet* law involves fragmentation of international legal mechanisms for governing various aspects of the Internet, including data protection, cybercrime, cybersecurity and more across borders. Like Internet fragmentation, fragmentation of international law has been highly critiqued.[110] Scholars and policymakers argue that fragmentation can dilute the ability of international institutions to present common solutions to common problems[111], reducing conflict in the process, and increase the likelihood of disputes about which rules govern.[112]

This proliferation of multilateral cybercrime conventions demonstrates legal Internet fragmentation in full force. As of 2025, five regional cybercrime conventions exist: The Budapest Convention (2001), developed by the Council of Europe[113]; the Minsk Convention (2001), developed by the Commonwealth of Independent states[114]; the Yekaterinburg Convention (2009), developed by the

[109] Eyal Benvenisti & George Downs, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STAN. L. REV. 595, 596. (2007); *but see* Tamar Megiddot, *Beyond Fragmentation: On International Law's Integrationist Forces*, 44 YALE J. INT'L L. 115, 119-120 (2019) (exploring multiple definitions).
[110] *See, e.g.*, *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, International Law Commission*, UNITED NATIONS (2006) (fragmentation creates "the danger of conflicting and incompatible rules, principles, rule-systems and institutional practices"); *but see* Tamar Megiddot, *Beyond Fragmentation: On International Law's Integrationist Forces*, 44 YALE J. INT'L L. 115, 119-120 (2019) (exploring positive consequences); Martti Koskenniemi & *Päivi Leino, Fragmentation of International Law? Postmodern Anxieties,* 15 LEIDEN J. INT'L L. 553, 575 (2002) (fragmentation can be a "positive demonstration of the responsiveness of legal imagination to social change"); Kal Raustiala, *The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law*, 43 VA. J. INT'L L. 1 (2002) (fragmentation can reflect the increased strength of and role for international law).
[111] Robert O. Keohane, *The Demand for International Regimes*, 36 INT'L ORG. 325, 334 (1982) ("Regimes are developed in part because …[they might enable] mutually beneficial agreements that would otherwise be difficult or impossible to attain.");
[112] *See, e.g.,* Sara McLaughlin Mitchell & Paul Hensel, *International institutions and Compliance with Agreements*, 51 AM. J. POL. SCI. 721 (2007) (arguing that legal institutions reduce likelihood of conflict, using data from territory and river disputes).
[113] Budapest Convention on Cybercrime, 23. Nov. 2001, TIAS 13174 (hereinafter Budapest Convention).
[114] Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offenses Relating to Computer Information, 1 June 2001, CIS Legislation (hereinafter Minsk Convention).

Shanghai Cooperation Organization[115]; the Cairo Convention (2010), developed by the League of Arab States[116]; and the Malabo Convention (2014), developed by the African Union. [117]

The Budapest Convention's drafters explicitly positioned this instrument as universal,[118] providing mechanisms for non-member states to accede.[119] Indeed, the Council has opposed the drafting of other, competing conventions.[120] The Budapest's identity as aspirationally universal, then, sets up the other regional responses as fragmentation vis-à-vis the Budapest Convention. designed to stand as alternatives, not complements, to the Budapest Convention, furthering fragmentation.[121]

[115] Yekaterinburg Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization in the Field of Information Security, 16 June, 2009, Carnegie Endowment for International Peace, https://perma.cc/WK5K-R7FE (hereinafter Yekaterinburg Convention).
[116] Arab Convention on Combating Information Technology Offenses, 21 December, 2010, Asian School of Cyber Laws (hereinafter Cairo Convention).
[117] African Union Convention on Cybersecurity and Personal Data Protection, June 27, 2014, African Union (hereinafter Malabo Convention).
[118] *See* Mailyn Fidler, *Fragmentation of International Cybercrime Law, 2025 Utah L. Rev. 737, n. 29 (2025)*, *citing* Danielle Flonk, Markus Jachtenfuchs, Anke Obendiek, *Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?, 9* GLOB. CONSTITUTIONALISM 364, 377-78 (2020) ("The Budapest Convention has explicitly been designed to have a global reach."); *Council of Europe Highlights 2015*, COUNCIL OF EUROPE (2015), at 40 (the "Budapest Convention remained the most influential treaty on cybercrime."); *Council of Europe Highlights*, COUNCIL OF EUROPE (2017), at 47 (the "global impact of the Convention…further increased,"); *Council of Europe Highlights 2019*, COUNCIL OF EUROPE (2019) (convention "remains the most relevant international agreement on cybercrime,"); *Council of Europe Highlights 2020*, COUNCIL OF EUROPE (2020) (Budapest Convention "remains the most relevant international agreement in this field").
[119] Budapest Convention art. 37(1).
[120] *See* Michael Vatis, *The Council of Europe Convention on Cybercrime,* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POL'Y 207 (2010) at 219, *citing* Jeremy Kirk, *Council of Europe Pushes for Only One Cybercrime Treaty,* COMPUTERWORLD (Mar. 23, 2010), *https://www.computerworld.com/article/1528103/council-of-europe-pushes-for-only-one-cybercrime-treaty.html*, (quoting the Deputy Secretary General of the Council of Europe: "we will have the best chance to succeed if we unite around one international instrument that already exists."); *see also* Fidler, *supra* note 118at 5 (discussing the Council of Europe and European Union's joint investment of over 50 million in efforts to get countries to join the Budapest Convention).
[121] Minsk Convention art. 17; Yekaterinburg Convention art. 12(3).

The African Union Convention is perhaps the most surprising instance of fragmentation, here. African states tend to join international efforts rather than develop their own, with a few key exceptions.[122] One explanation for this tendency is that less powerful states can use their strength in numbers in international institutions to advance their agendas.[123] Developing independent international agreements for governing inherently international problems may not always hold similar benefits. Yet, the cybercrime case, is among the exceptions from this general pattern.

Subordination fragmentation helps to explain some of the trajectory of the Convention's development. The Malabo Convention contains provisions that extend the sovereign's domestic powers with respect to online activity, prohibiting, for example, insulting a person based on their political opinion.[124] This provision, and others, expand the reach of criminal law and give signatory governments the ability to punish certain harmful acts or speech as cybercrime.[125] Doing so expands the reach of domestic control over internet-related phenomenon, a hallmark of subordination fragmentation.

But the patterns of support for the Convention tell a more complicated story. The Malabo Convention currently commands only fifteen ratifications out of fifty-five member states.[126] Examining the Malabo Convention in more detail, states that have elsewhere pursued other key Internet fragmentation strategies in pursuit of

[122] African Charter on Human and Peoples' Rights, 1981, Organization of African Unity; Bamako Convention on the Ban of the Import into Africa and the Control of Transboundary Movement and Management of Hazardous Wastes Within Africa, 1991, Organization of African Unity.
[123] *See, e.g.*, Christina Schneider, *Weak States and Institutionalized Bargaining Power in International Organizations*, INT'L STUDS. Q. 55 (2011); Julia Morse & Robert Keohane, *Contested Multilateralism*, 9 REV. INT'L ORG. 385, 389-390 (2014) ("A dissatisfied coalition composed primarily of weak states. . . may only be able to mount a symbolic challenge, critiquing an existing institutional practice but being unable to force immediate change" and "A group of dissatisfied actors that includes states with significant resources and institutional leverage will have an easier time identifying credible outside options than a coalition of weaker actors".)
[124] Malabo Convention art. 29(3)(1)(g).
[125] For more on this logic generally, *see* Mailyn Fidler, *Cybersecurity Mission Creep*, ____ U. Ill. L. Rev. ___ (forthcoming 2026).
[126] List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, African Union (Oct. 19, 2023).

domestic sovereignty tend not to be the Malabo Convention's supporters. For instance, states that have engaged in Internet shutdowns tend not to support the Convention.[127] Similarly, subordination fragmentation is often, although not always associated with more authoritarian governance practices.[128] Yet no substantial difference between signatories and non-signatories on such measures exists.[129]

Instead, countries with the fewest undersea cable connections and landing points tend to support the Convention. Table 1 demonstrates that Malabo Convention signatories tend to have fewer cable connections, fewer landing sites, and slower cable growth during the study period.[130]

Table 1: Coastal Signatory Status by Cable Status

	Cables	Landing Points	Cable Growth 2017-2021
Signatories	2.17	1.08	0.58
Non-signatories	3.27	1.53	0.87

[127] On average, from 2016-2023, states that have, as of 2024, ratified the Malabo Convention experienced 1.8 shutdowns per year. Countries that had neither signed nor ratified the Malabo Convention experienced an average of 3.7 per year. *See Documenting Shutdowns Globally*, ACCESSNOW (2016-2023).
[128] China's score is 9, Russia 13, and Iran 11. *Global Freedom Scores*, FREEDOM HOUSE (2024).
[129] *Global Freedom Scores*, FREEDOM HOUSE (2024).
[130] The data in this article reflects a snapshot from 2017-2021, a span of five years. I selected the starting point, three years after the convention's adoption, to include more than just a few ratifying states. I selected five years as a decently-sized window into the dynamics of the convention, a period unaltered by major events that might disrupt signatory patterns. For instance, the document entered into force in 2023. Political calculations around which country would be the ratification to make the document enter into force would likely distort overall patterns, so data from around this time would similarly contain different patterns. The data about undersea cables and support for the convention necessarily only includes coastal African states. It also excludes island nations and states bordering the Mediterranean, because the geography of each of those types of state skews the incentives for infrastructure investment in their favor; they stand apart from the rest of the continent. A version of this table appeared in Fidler, *supra* note 63. I have updated it to reflect newly available data and regional classifications. The changes have not affected the inferences drawn. For cable data, the data reflects data at time of signature for signatories, and in 2021 for non-signatories.

In other words, those states the most affected by inverse fragmentation—the connectivity deserts created by outside investment in undersea connectivity—have, in turn, tended to support the African continent's legal Internet fragmentation. When states have little recourse to the other—and perhaps more powerful—types of Internet fragmentation that can directly target other states, legal fragmentation is still available. In a global environment where the Internet fragmentation of more powerful actors is taking an outward turn, less powerful state recourse to legal fragmentation should not be underestimated.

This form of legal fragmentation by less powerful states is strategic; it is not solely aimed at obstructing the preferences of more powerful states. It may also have actively facilitated the development of a more integrated legal framework on cybercrime—one that more accurately reflects the priorities and interests of non-Western actors. In December 2024, the UN adopted its Cybercrime Convention.[131] This treaty has been heralded[132] as a key step towards finally managing the fragmented patchwork of multilateral laws governing cybercrime and has received substantially more global support than the Budapest Convention. I propose a hypothesis to be explored in future work: the fragmentation that preceded the adoption of the UN Convention played a crucial role in shaping its development and eventual acceptance.[133] If that hypothesis holds true, this adds additional evidence to the use of legal fragmentation as a projection of power.

Internet legal fragmentation offers even less powerful states, with less access to the tools and tradecraft of other outward-facing Internet fragmentation, a way to project power and contest central aspects of the global order. The law is part of

[131] See Adopted draft text of the convention, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, United Nations (2024); Summer Walker, *Still Poles Apart: UN Cybercrime Treaty Negotiations*, GLOB. INIT. AGAINST TRANSNAT'L ORG. Crime (2023).
[132] James A. Lewis, Fragmentation or Open-Mindedness: Rethinking Responsible Behavior in an Age of Multilateralism, CSIS (Oct. 16, 2024), https://www.csis.org/analysis/fragmentation-or-mindedness-rethinking-responsible-behavior-age-multilateralism.
[133] *See* Mailyn Fidler, *Cybercrime Convergence* (draft on file with the author).

the architecture of the Internet, now, and legal fragmentation affects that architecture. Pushing back through fragmentation of law, when pushing back materially is not possible, offers an alternate form of political contestation for these countries.

Conclusion

Internet fragmentation has become another tool in states' toolkits for challenging the global order. No longer primarily about cultivating the experience of the Internet within borders, it comes in many forms and is now part of the toolkit for contesting international systems of power. Just as conversations about trade and the environment can be used and abused for considerations of power and primacy, Internet fragmentation can too. This use can help explain state choices and inform responses to fragmentation in ways that respond to the actual underlying political motivations. It also raises the possibility that Internet fragmentation is experiencing a more aggressive turn, from "not in my backyard" to "not in your backyard." In turn, this form of Internet fragmentation risks escalation of conflict between states in ways that old forms did not. The Internet is a transformative tool; so too is Internet fragmentation. States, both powerful and less so, have discovered the transformative power of Internet fragmentation not only for their own affairs but for moving the needle on global affairs, for better or for worse.

Bibliography

A

Susan Aaronson, *What are We Talking About When We Talk About Digital Protectionism?*, 18 WORLD TRADE REV. 541 (2019).

Lukman Abdulruf & Oyeniyi Abe, *The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations*, UNIVERSITY OF WITWATERSRAND SCHOOL OF LAW (2021).

Adopted draft text of the convention, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, United Nations (2024).

African Charter on Human and People's Rights, 1981, Organization of African Unity.

African Union Convention on Cybersecurity and Personal Data Protection, June 27, 2014, African Union.

Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offenses Relating to Computer Information, 1 June 2001, CIS Legislation.

Johan Ahlander, Essi Lehto, and Andrius Sytas, *Two Undersea Cables in Baltic Sea Cut, Germany and Finland Fear Sabotage*, REUTERS (Nov. 18, 2024), https://www.reuters.com/business/media-telecom/telecoms-cable-linking-finland-germany-likely-severed-owner-says-2024-11-18/

Christina Anderson and Amelia Nierenberg, *Sweden Suspects 'Gross Sabotage' After Damage to Cable Under Baltic Sea*, N.Y. TIMES (Jan. 27, 2025), https://www.nytimes.com/2025/01/27/world/europe/cable-baltic-sea-sweden-damage.html.

MALCOM ANDERSON, POLICING THE WORLD: INTERPOL AND THE POLITICS OF INTERNATIONAL POLICE CO-OPERATION (1989).

Arab Convention on Combating Information Technology Offenses, 21 December, 2010, Asian School of Cyber Laws.

B

Bamako Convention on the Ban of the Import into Africa and the Control of Transboundary Movement and Management of Hazardous Wastes Within Africa, 1991, Organization of African Unity.

Eyal Benvenisti & George Downs, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STAN. L. REV. 595 (2007).

Samantha Besson, *Sovereignty*, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (Anne Peters and Rudiger Wolfrum, eds.) (2011).

Sarah Box, *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*, 36 GLOB. COM. INTERNET GOV. PAPER SERIES (2016).

Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).

DENNIS BROEDERS, THE PUBLIC CORE OF THE INTERNET (2015).

Budapest Convention on Cybercrime, 23. Nov. 2001, TIAS 13174.

C

FRANCES CAIRNCROSS, THE DEATH OF DISTANCE (2001).

Joel Cariolle, Telecommunication Submarine-Cable Deployment and the Digital Divide in Sub-Saharan Africa, Fondation Pour Les Études et Recherches Sur Le Développement International, Working Paper 241 (2018).

Sonali Chandel et al., *The Golden Shield Project of China: A Decade Later—An In-Depth Study of the Great Firewall*, 2019 INT'L CONF. ON CYBER-ENABLED DISTRIBUTED COMPUTING AND KNOWLEDGE DISCOVERY (2019).

Anupam Chander, *The National Security Internet*, 114 Geo. L. J. __ (forthcoming 2025).

Anupam Chander, *Trump v. Tiktok*, 55 VAND. J. TRANSNAT'L L. 1145 (2022).

Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015).

Convention for the Protection of Submarine Telegraph Cables (1884).

Council of Europe Highlights 2015, COUNCIL OF EUROPE (2015).

Council of Europe Highlights, COUNCIL OF EUROPE (2017).

Council of Europe Highlights 2019, COUNCIL OF EUROPE (2019).

Council of Europe Highlights 2020, COUNCIL OF EUROPE (2020).

Clyde Wayne Crews, *On My Mind*, FORBES (Apr. 2, 2001), https://www.forbes.com/forbes/2001/0402/036.html

D

Jennifer Daskal & Paul Ohm, *Debate: We Need to Protect Strong National Borders on the Internet*, 17 COLO. TECH L.J. 13 (2018).

Felicity Deane, *Trade in the Digital Age: Agreements to Mitigate Fragmentation*, 14 ASIAN J. INT'L L. 154 (2024).

Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291 (2015).

Saeed Kamali Dehghan, *Iran Clamps Down on Internet Use*, GUARDIAN (Jan. 5, 2012), https://www.theguardian.com/world/2012/jan/05/iran-clamps-down-internet-use.

Daria Dergacheva, *Shutting Down the Net: The Growing Threat of Russian Internet Censorship*, GLOBAL VOICES (Jan. 22, 2025), https://globalvoices.org/2025/01/22/shutting-down-the-net-the-growing-threat-of-russian-internet-censorship/.

Documenting Shutdowns Globally, ACCESSNOW (2016-2023).

William Drake, Vincent Cerf, and Wolfgang Kleinwachter, *Internet Fragmentation: An Overview*, WORLD ECONOMIC FORUM (2016).

E

Editorial Board, Opinion, India isn't just fracturing the Internet with its ban on Chinese app. It's shrinking it., WASH. POST (July 4, 2020), https://www.washingtonpost.com/opinions/global-opinions/india-isnt-just-fracturing-the-internet-with-its-ban-onchinese-apps-its-shrinking-it/2020/07/03/e5d0cad8-bbcb-11ea-8cf5-9c1b8d7f84c6_story.html.

F

Nathaniel Fick & Jami Miscik, *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, COUNCIL ON FOREIGN RELATIONS, INDEPENDENT TASK FORCE REPORT NO. 80 (2022).

Mailyn Fidler, *African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts*, NET POLITICS, COUNCIL ON FOREIGN RELATIONS (Mar. 7, 2018), https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

Mailyn Fidler, *Fragmentation of International Cybercrime Law*, 2025 UTAH L. REV. 737 (2025).

Mailyn Fidler, *African Data Protection Laws: Politics, But as Usual*, in in AFRICAN DATA PROTECTION (Raymond Atuguba, et al., eds.) (2024).

Mailyn Fidler, Cybercrime Convergence (manuscript on file with author).

Mailyn Fidler, *Cybersecurity Mission Creep*, ___ U. Ill. L. Rev. ___ (forthcoming 2026).

Danielle Flonk, Markus Jachtenfuchs, Anke Obendiek, *Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?, 9* GLOB. CONSTITUTIONALISM 364 (2020).

Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, International Law Commission, UNITED NATIONS (2006).

Framework for Artificial Intelligence Diffusion, Dep't. of Commerce (Jan. 15, 2025), https://public-inspection.federalregister.gov/2025-00636.pdf.

Juan Ortiz Freuler, *Infrastructural Power: State Strategies for Internet Control*, 14 INTERNET L. & POL'Y REV. 1 (2025).

G

JAI GALLIOT, FORCE SHORT OF WAR IN MODERN CONFLICT: JUS AD VIM (2019)

Jon Gambrell, *3 Red Sea Data Cables Cut as Houthis Launch More Attacks in the Vital Waterway*, AP NEWS (Mar. 4, 2024), https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a.

Anna Gelpern et al., *How China Lends*, AID DATA (2021);

Global Freedom Scores, FREEDOM HOUSE (2024).

Global Internet Freedom Task Force, U.S. DEP'T OF STATE (2001-2009) *https://2001-2009.state.gov/g/drl/lbr/c26696.htm;*

Jack Goldsmith, *The Failure of Internet Freedom*, in THE PERILOUS PUBLIC SQUARE: STRUCTURAL THREATS TO FREE EXPRESSION TODAY 241 (David Pozen ed., 2020).

Florence G'Sell, *Digital Authoritarianism: From State Control to Algorithmic Despotism*, OXFORD HANDBOOK OF DIGITAL CONSTITUTIONALISM (forthcoming).

H

Jonah Force Hill, *Internet Fragmentation*, HARVARD BELFER CTR. (2012).

Jonas Hjort and Jonas Poulsen, *The Arrival of Fast Internet and Employment in Africa*, 109 AM. ECON. REV. 1032, 1033 (2019).

Joris van Hoboken & Ronan O Fathaig, *Regulating Disinformation in Europe: Implications for Speech and Privacy*, 6 U.C. IRVINE J. OF INT'L, TRANS. & COMP. L. 9 (2021).

Georges V. Houngbonon, Justice Tei Mensah, and Nouhoum Traore, *The Impact of Internet Access on Innovation and Entrepreneurship in Africa*, WORLD BANK POLICY WORKING PAPER 9945 (2022).

Jamie P. Horsely, *Behind the Façade of China's Super-Regulator*, DIGICHINA (Aug. 8, 2022), https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/.

I

Internet Freedom and Technology and Human Rights, U.S. DEP'T STATE (last accessed Jul. 10, 2024), https://www.state.gov/internet-freedom-and-technology-and-human-rights/.

Internet Way of Networking Use Case: Data Localization, INTERNET SOC'Y (2020).

J

ROBERT JERVIS, PERCEPTION AND MISPERCEPTION IN INTERNATIONAL POLITICS (1976).

K

Joshua Kaplan, Brett Murphy, Justin Elliott, and Alex Mierjeski, *The Trump Administration Leaned on African Countries. The Goal: Get Business for Elon Musk*, PROPUBLICA (May 15, 2025), https://www.propublica.org/article/trump-musk-starlink-state-department-gambia-africa-pressure.

#KeepItOn: Authorities in Gabon Must Safeguard Open and Secure Internet Access During Elections, ACCESS NOW (Apr. 8, 2025), https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/.

Robert O. Keohane, *The Demand for International Regimes*, 36 INT'L ORG. 325 (1982)

Jeremy Kirk, *Council of Europe Pushes for Only One Cybercrime Treaty,* COMPUTERWORLD (Mar. 23, 2010), *https://www.computerworld.com/article/1528103/council-of-europe-pushes-for-only-one-cybercrime-treaty.html*

Ariane Knuesel, *British Diplomacy and the Telegraph in Nineteenth-Century China*, 18 DIPLOMACY & STATECRAFT 517 (2007).

Avi Kober, *Low-Intensity Conflicts: Why the Gap Between Theory and Practise*, 18 DEFENSE & SEC. ANALYSIS 15 (2002).

Martti Koskenniemi, *What is International Law For?*, in INTERNATIONAL LAW (Malcolm Evans, ed., 5th ed.) (2018).

Martti Koskenniemi & *Päivi Leino, Fragmentation of International Law? Postmodern Anxieties,* 15 LEIDEN J. INT'L L. 553 (2002).

STEPHEN KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY (1999)

Christopher Kuner, *Data Nationalism and its Discontents*, 64 EMORY L. J. ONLINE 2089 (2015).

L

Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393 (2013).

Mark Lemley, *The Splinternet*, 70 DUKE L. J. 1397 (2021).

James A. Lewis, Fragmentation or Open-Mindedness: Rethinking Responsible Behavior in an Age of Multilateralism, CSIS (Oct. 16, 2024), https://www.csis.org/analysis/fragmentation-or-mindedness-rethinking-responsible-behavior-age-multilateralism.

ODETTE LIENAU, RETHINKING SOVEREIGN DEBT (2014).

List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, African Union (Oct. 19, 2023).

M

Ian Manners, *The Normative Ethics of the European Union*, 84 INT'L AFF. 45 (2008).

Lennart Maschmeyer, *A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict*, 46 J. STRAT. STUDS. 570 (2023).

James McBride, Noah Berman, and Andrew Chatzky, *China's Massive Belt and Road Initiative*, COUNCIL ON FOREIGN RELATIONS (Feb. 2, 2023), https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative#chapter-title-0-4.

Tamar Megiddot, *Beyond Fragmentation: On International Law's Integrationist Forces*, 44 YALE J. INT'L L. 115 (2019).

Sara McLaughlin Mitchell & Paul Hensel, *International institutions and Compliance with Agreements*, 51 AM. J. POL. SCI. 721 (2007).

Evgeny Morovoz, *Think Again: The Internet*, FOREIGN POL'Y (Apr. 26, 2010), https://foreignpolicy.com/2010/04/26/think-again-the-internet/.

Julia Morse & Robert Keohane, *Contested Multilateralism*, 9 REV. INT'L ORG. 385 (2014).

Solomon Moore, *Ship Accidents Sever Data Cables Off East Africa*, WALL ST. J. (Feb. 28, 2012).

Homer E. Moyer, Jr., and Linda A. Mabry, *Export Controls as Instruments of Foreign Policy: The History, Legal Issues, and Policy Lessons of Three Recent Cases*, 15 LAW & POL'Y INT'L BUS. 1, (1983).

Milton Mueller, *Internet Fragmentation Exists, But Not in the Way That You Think*, NET POLITICS, COUNCIL ON FOREIGN RELATIONS (June 12, 2017), https://www.cfr.org/blog/internet-fragmentation-exists-not-way-you-think.

MILTON MUELLER, WILL THE INTERNET FRAGMENT? SOVEREIGNTY, GLOBALIZATION, AND CYBERSPACE (2017).

NICHOLAS MULDER, THE ECONOMIC WEAPON: THE RISE OF SANCTIONS AS A TOOL OF MODERN WARFARE (2022).

Erin L. Murphy and Matt Pearl, *China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts*, CSIS (Apr. 4, 2025), https://www.csis.org/analysis/chinas-underwater-power-play-prcs-new-subsea-cable-cutting-ship-spooks-international.

N

NORMATIVE POWER EUROPE, RICHARD WHITMAN, ED. (2011).

Ihueze Nwobilor, *Navigating Internet Fragmentation in the African Context: Challenges and Opportunities*, PARADIGM INITIATIVE (May 25, 2024), https://paradigmhq.org/navigating-internet-fragmentation-in-the-african-context-challenges-and-opportunities/.

Joseph Nye, *Soft Power*, 80 FOREIGN POL'Y 153, 168 (1990).

O

JOSE ANTONIO OCAMPO AND JUAN MARTIN, A DECADE OF LIGHT AND SHADOW: LATIN AMERICA AND THE CARIBBEAN IN THE 1990S (2003)

An Overview of Global Internet Shutdowns, ACCESS NOW (2023), https://www.accessnow.org/campaign/keepiton/#global-tracker.

P

Joe Pappalardo, *New Transatlantic Cable Built to Shave 5 Milliseconds off Stock Trades*, POPULAR MECHANICS (Oct. 27, 2011), https://www.popularmechanics.com/technology/infrastructure/a7274/a-transatlantic-cable-to-shave-5-milliseconds-off-stock-trades/.

Brid-Aine Parnell, *Epic Net Outage as Four Undersea Cables Chopped*, THE REGISTER (Feb. 28, 2012), https://perma.cc/C93J-SMLJ.

Clement Perarnaud et al., *'Splinternets': Addressing the Renewed Debate on Internet Fragmentation*, EUR. PARL. RES. SVC. (2022).

D. Polatin-Reuben & J. Wright, An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet, 4th Usenix Conference on Free and Open Communication on the Internet, https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf.

A Proposal in Cambodia Would Turn the Country's Internet into a National Internet, INTERNET SOC'Y (Dec. 1, 2023), https://www.internetsociety.org/resources/internet-fragmentation/cambodias-national-internet-gateway/.

Q

R

Kal Raustiala, *The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law*, 43 VA. J. INT'L L. 1 (2002).

Joel Reidenberg, *Yahoo & Democracy on the Internet*, 42 JURIMETRICS 261 (2002).

The Role of Technical Assistance and Capacity-Building in Fostering Mutually Beneficial Cooperation in Promoting and Protecting Human Rights, UNITED NATIONS HUMAN RIGHTS COUNCIL, https://documents.un.org/doc/undoc/gen/g20/012/07/pdf/g2001207.pdf.

Zach Rosson, Felicia Anthonio, & Carolyn Tackett, *The Most Violent Year: Internet Shutdowns in 202*3, ACCESSNOW (May 15, 2024), https://www.accessnow.org/internet-shutdowns-2023/.

S

Rachel Savage and Duncan Miriri, *Post-COVID, China Is Back in Africa and Doubling Down on Minerals*, REUTERS (May 28, 2024), https://www.reuters.com/markets/commodities/post-covid-china-is-back-africa-doubling-down-minerals-2024-05-28/.

Christina Schneider, *Weak States and Institutionalized Bargaining Power in International Organizations*, INT'L STUDS. Q. 55 (2011).

Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681 (2018).

Andrea Shalal and Joey Roulette, *US Could Cut Ukraine's Access to Starlink Internet Services Over Minerals, Say Sources*, REUTERS (Feb. 22, 2025), https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

PETER M. SHANE, DEMOCRACY ONLINE: THE PROSPECTS FOR POLITICAL RENEWAL THROUGH THE INTERNET (2004).

Beth Simmons & Rachel Hulvey, *Cyberborders: Exercising State Sovereignty Online*, 95 TEMPLE L. REV. 617 (2023).

Russell Southwood, *The Ugly Underbelly of the Communications Revolution: Corruption, Cronyism, Regulation and Government* (1999-2000), AFRICA 2.0 (2022).

NICOLE STAROSIELSKI, THE UNDERSEA NETWORK (2015).

Strategic Importance of, and Dependence On, Undersea Cables, NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE (2019).

Submarine Cable Map, Telegeography (last accessed May 28, 2025), https://www.submarinecablemap.com/.

See Daniel Sutherland and Jim Dempsey, *Cybersecurity Risk from Kaspersky to TikTok*, LAWFARE (May 28, 2025), https://www.lawfaremedia.org/article/cybersecurity-risk-from-kaspersky-to-tiktok.

Ewan Sutherland, *Undersea Cables and Landing Stations Around Africa: Policy and Regulatory Issues*, 25th EUR. REG. CONF. ON INT'L TELECOM. SOC'Y (2014).

T

TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2017).

U

Unabashed and Unabated: India Leads the World Shutdown Count for Sixth Year, ACCESS NOW (May 15, 2024), https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/.

UN Human Rights Council: First Resolution on Internet Free Speech, LIBRARY OF CONGRESS (July 12, 2012), https://www.loc.gov/item/global-legal-monitor/2012-07-12/u-n-human-rights-council-first-resolution-on-internet-free-speech/.

V

Joris van Hoboken & Ronan O Fathaig, *Regulating Disinformation in Europe: Implications for Speech and Privacy*, 6 U.C. IRVINE J. OF INT'L, TRANS. & COMP. L. 9 (2021).

Michael Vatis, *The Council of Europe Convention on Cybercrime,* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POL'Y 207 (2010).

W

Summer Walker, *Still Poles Apart: UN Cybercrime Treaty Negotiations*, GLOB. INIT. AGAINST TRANSNAT'L ORG. Crime (2023).

Yaqiu Wang, *In China, the 'Great Firewall' Is Changing a Generation*, POLITICO (Sept. 1, 2020), https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385.

Barney Warf, *International Competition Between Satellite and Fiber Optic Carriers: A Geographic Perspective*, 58 PROF. GEO. 1 (2006).

Matthew C. Waxman, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, 87 INT'L L. STUD. 43 (2011).

JONATHAN REED WINKLER, NEXUS: STRATEGIC COMMUNICATIONS AND AMERICAN SECURITY IN WORLD WAR I (2008).

Jonathan Reed Winkler, *Silencing the Enemy: Cable-Cutting in the Spanish-American War*, WAR ON THE ROCKS (Nov. 6, 2015), https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/.

Dwayne Winseck, *Internet Infrastructure and the Persistent Myth of U.S. Hegemony*, in INFORMATION, TECHNOLOGY AND CONTROL IN A CHANGING WORLD (2019).

Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328 (2018).

Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, in ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, at 1,12 (Roland Stanger, ed., 1962).

TIM WU & JACK GOLDSMITH, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

X

Y

Yekaterinburg Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization in the Field of Information Security, 16 June, 2009, Carnegie Endowment for International Peace, https://perma.cc/WK5K-R7FE.

Z

Jan Zielonka, *Europe as a Global Actor: Empire by Example?*, 84 INT'L AFF. 471 (2008).

About the author:

Professor Mailyn Fidler is an internationally recognized scholar of power, technology, and the law. Fidler teaches and writes in the areas of criminal law, criminal procedure, cybersecurity, cybercrime, and national security law. She has authored several cutting-edge law review articles, including “Fragmentation of International Cybercrime Law” in the *Utah Law Review* and “Cybersecurity Mission Creep” in the *University of Illinois Law Review*.

Fidler has presented at influential and invitation-only forums on legal scholarship, including the University of Michigan Law School’s Junior Scholars’ Conference. Fidler’s work has also drawn attention from policymakers. Last fall the governments of the United Kingdom and France invited her to participate in the Pall Mall multilateral process on regulating spyware held in Paris.

Fidler is currently a Visiting Assistant Professor at Harvard Law School, a faculty affiliate at Yale Law School’s Information Society Project, and a faculty associate at Harvard Law School’s Berkman Klein Center for Internet & Society, where she was previously an affiliate and resident fellow. She is on the faculty of the University of New Hampshire Franklin Pierce School of Law and holds degrees Yale Law School, Oxford University and Stanford University.

About the Digital, Governance and Sovereignty Chair:

Sciences Po’s Digital, Governance and Sovereignty Chair’s mission is to foster a unique forum bringing together technical companies, academia, policymakers, civil societies stakeholders, public policy incubators as well as digital regulation experts.

Hosted by the **School of Public Affairs**, the Chair adopts a multidisciplinary and holistic approach to research and analyze the economic, legal, social and institutional transformations brought by digital innovation. The Digital, Governance and Sovereignty Chair is chaired by **Florence G’sell**, Professor of Law at the Université de Lorraine, lecturer at the Sciences Po School of Public Affairs, and visiting professor at the Cyber Policy Center of Stanford University.

The Chair’s activities are supported by:

sopra steria next

Caisse des Dépôts GROUPE