

UCLA

UCLA Public Law & Legal Theory Series

Title

The Global Governance of the Internet

Permalink

<https://escholarship.org/uc/item/7w517168>

Journal

UCLA School of Law Public Law & Legal Theory Series

Authors

Raustiala, Kal

Hollis, Duncan B.

Publication Date

2022-08-26

Temple University Beasley School of Law
LEGAL STUDIES RESEARCH PAPER NO. 2022-17

The Global Governance of the Internet

Duncan B. Hollis
Temple University Beasley School of Law

Kal Raustiala
University of California, Los Angeles School of Law

Cite: in THE OXFORD HANDBOOK OF INTERNATIONAL INSTITUTIONS (Duncan Snidal & Michael N. Barnett eds., forthcoming 2023)

This paper can be downloaded without charge from the
Social Science Research Network Electronic paper Collection:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4197418

The Global Governance of the Internet

Duncan B. Hollis & Kal Raustiala

Cyberspace needs governance. But who should govern it and how? In 1996, John Perry Barlow responded to early efforts to regulate the Internet by issuing his famous *Declaration of the Independence of Cyberspace*:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace . . . On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. . . . Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.¹

More than twenty-five years on, Barlow's paean to governance by individuals and non-state actors retains significant descriptive and normative value. A number of current "multistakeholder" cyber governance processes (e.g., the Internet Engineering Task Force (IETF)) trace their origins to the small, trusted, and largely academic community that Barlow claimed to speak for, and who first constructed and operated the Internet.²

Barlow's attempt to exile states from the digital domain, however, proved remarkably ineffective. Shortly after his essay was written the United States demonstrated that it possessed substantial control over the Internet, and myriad states now participate actively in Internet governance. As the Internet's relevance to international relations has grown even more clear, states increasingly have sought to extend other institutional frameworks – especially multilateral ones – to it.³ Meanwhile, the libertarian ideal of cyber governance based on functionality and minimal

¹ John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, Feb. 8, 1996, <https://www.eff.org/cyberspace-independence>.

² We discuss multistakeholder governance further below: See, e.g., Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *INT'L THEORY* 7, (2015): pp. 572, 574-84, doi:10.1017/S1752971915000081; Milton Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace*, (MIT Press, 2004).

³ See, e.g., U.N.G.A., "Developments in the field of information and telecommunications in the context of international security," Resolution 75/240, Jan. 21, 2021; Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?," *EU Institute for Security Studies*, (July 2017), <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf>; David P. Fidler, "Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations," *ASIL Insights* 17, no. 6 (February 2013).

regulation—famously defined, in Barlowesque fashion, as an Internet ordered by “rough consensus and running code”⁴—has come under increasing pressure from those who would substitute sovereignty as the dominant ordering principle. The result is a heterogenous, dynamic, and multi-layered regime complex comprising a diverse set of principles, agreements, and institutions in a domain that is increasingly indispensable to international relations and modern life.⁵

The trajectory of this evolution in digital governance merits notice. Unlike some traditional commons such as the sea or space, cyberspace did not preexist in a natural state. The digital domain was literally constructed (as Barlow noted), and that construction occurred via the joint and sometimes uncoordinated efforts of the US government, academic institutions, and various private actors. Moreover, all this construction began within the United States, and only extended outward globally over time. These unusual origins, and the continued centrality of U.S. entities in driving digital transformations, have given the U.S. a unique role in digital governance.

Today, both the concept and the contours of the digital domain remain deeply contested.⁶ Cyberspace is of relatively recent vintage. Its institutions, rules and organizing principles remain nascent and not well embedded. As a result, digital governance is relatively underexplored in the literature on international institutions.⁸

This chapter aims to remedy such inattention. We survey the dynamics by which institutions provide order in the digital domain, the incremental changes that have occurred over time, and the looming prospect of more fundamental transformations. In particular, we highlight three important aspects of digital governance. First, digital governance reflects cyberspace as a *socio-technical* system.⁷ Order, adaptation, and transformation in cyberspace always involve a “technical” aspect that operates across the micro, meso, and macro institutional frameworks used to organize analyses in this volume. This flows directly from the point made above:

⁴ David D. Clark, “A Cloudy Crystal Ball Visions of the Future,” IETF, Jul. 16, 1992, http://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf.

⁵ Joseph S. Nye, “The Regime Complex for Managing Global Cyber Activities,” *Global Commission on Internet Governance*, Vol. 1, (May 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf. A “regime complex” refers to an overlapping set of individual regimes governing a particular international issue area. Kal Raustiala and David G. Victor, “The Regime Complex for Plant Genetic Resources,” *INT’L ORG.* 58, no. 2 (April 2004): pp. 277, doi:10.1017/S0020818304582036.

⁶ On cyberspace as a concept see, e.g., Jack L. Goldsmith and Timothy Wu, *Who Controls the Internet? Illusions of a Borderless World*, (Oxford University Press, 2008); Julie E. Cohen, “Cyberspace As/And Space,” *COLUMBIA L. REV.* 107, (2007): p. 210, [https://heinonline.org/HOL/LandingPage?handle=hein.journals/clr107&div=14&id=&page=](https://heinonline.org/HOL/LandingPage?handle=hein.journals/clr107&div=14&id=&page=;); Mark A. Lemley, “Place and Cyberspace,” *CALIF. L. REV.* 91, no. 2 (March 2003): p. 521, doi:10.2307.3481337.

⁸ See, e.g., Tim Maurer, “A Dose of Realism: The Contestation and Politics of Cyber Norms,” *HAGUE J. RULE LAW* 12 (2020): p. 283, doi:10.1007/s40803-019-00129-8; Tim Stevens, *Cyber Security and the Politics of Time*, (Cambridge University Press, 2016); Nazli Choucri, *Cyberpolitics in International Relations*, (MIT Press, 2012).

⁷ Chris C. Demchak and Peter J. Dombrowski, “Rise of a Cybered Westphalian Age,” *STRATEGIC STUDIES QUARTERLY* 5, no. 1. (Spring 2011): pp. 32, 56-58, https://www.jstor.org/stable/26270509#metadata_info_tab_contents.

the digital domain is man-made, and its architecture reflects particular technological choices. Second, the extensive creation, distribution, and control of technical level resources by *private actors* means they continue to claim an unusually high degree of regulatory authority and power. The cyber regime complex correspondingly reflects a diverse range of institutional frameworks, including multistakeholder models. Third, the dynamics of change in cyber governance have followed an *inverse path* from that generally witnessed elsewhere in the postwar era. The path for many, if not most, domains of global governance in the postwar era was one of state centrality giving way to a greater accommodation of a wider array of stakeholders over time. Instead, from its multistakeholder origins, digital governance continues to move toward greater multilateralism. The struggle underway between multilateralism and multistakeholderism is not unique, but its origins and directionality are distinctive in comparison to its contemporaries. The outcome of this struggle could shift not only the organizing principles and institutions of cyberspace, but also fundamentally transform the technical level itself from the existing, universal internet to a “splinternet” reflecting national or regional boundaries.⁸

To illustrate these arguments our chapter elaborates an example at each level – micro, meso, and macro – of institutional analysis. We begin in Part I by elaborating on the overarching socio-technical aspects of the digital context, exploring how technology orders cyberspace. Part II explores the evolution of the critical domain name system’s governance into an autonomous, multistakeholder model under the auspices of the International Corporation for Assigned Names and Numbers (ICANN), a *sui generis* organization that wields considerably regulatory authority. Part III moves to the meso-level to elaborate the scale and scope of the multistakeholder cyber regime complex, the diverse actors who populate it, and the pressures to transform it via more multilateralism. Part IV steps back to examine the macro-competition over (re)ordering cyberspace according to multilateral principles that includes ongoing debates over (i) how to conceptualize cyberspace (as a technical communications modality, as an economic platform, or as a military domain), (ii) the appropriate form for its regulation (existing rules or a new treaty), (iii) and the purpose in doing so (to preserve an “open Internet” or guarantee “digital sovereignty”). We conclude by highlighting how international relations scholarship may benefit from greater attention to the order, adaptations and transformations socio-technical institutions offer just as those concerned with more effective governance in the digital domain may benefit from the lessons offered by studying other international institutions in differing issue-areas.

I. Cyberspace as a Socio-Technical Institution: Code as Law

Cyberspace is a multi-layered assemblage of hardware, software, and networks that store and exchange data. The bottommost “link” layer includes the physical hardware used to access the Internet. Next, are three layers defined by computer code – (i) the “network” and (ii) “transport” layers, which break data into packets and route them between networks through the use of a naming system, and

⁸ The triumph of states is by no means assured, however. See Ian Bremmer, “The Technopopular Moment: How Digital Powers will Reshape the Global Order,” *FOREIGN AFFAIRS* (Nov./Dec. 2021): p. 100, <https://heinonline.org/HOL/LandingPage?handle=hein.journals/fora100&div=153&id=&page=>.

(iii) the “applications” layer that converts data into useful things like files, videos, and web sites.⁹ Each of these layers functions independently; at the application layer, for example, Google Chrome works regardless of whether the link layer employs DSL or WiFi.

Thus, any consideration of digital governance must begin with the technical aspect of its constitution. The way the technology is constructed shapes governance in cyberspace; that is, what states, firms, and individuals are capable of doing in this environment. This is a central way in which cyberspace is distinct from many areas of global governance. Institutions concerned with climate change cannot re-write the laws of nature any more than those concerned with international humanitarian law can revise the laws of gravity to blunt a weapon’s impacts. In cyberspace, however, as Larry Lessig famously highlighted, “code is law.”¹⁰ Software and hardware empowers users to do certain things at the same time as they foreclose other things. For example, technological choices dictate whether user identities can be authenticated and tracked on-line.¹¹ Yet altering these choices can be very difficult. To be sure, aspects of the Internet’s technical level have evolved over time, including some fairly major evolutions such as the partial closing off of the Internet in China, the shift from individualized data storage to a “cloud-based” infrastructure, and the Internet-enabling of tens of billions of small devices. (What is sometimes known as the “Internet of Things.”) Still, these changes are built upon the same basic technologies and protocols initially designed decades ago when the Internet effectively consisted of a handful of nodes, all within the territorial borders of the U.S.

In theory, an entirely new Internet or set of Internets could be stood up. Yet, in practice, network effects, path-dependence, and large sunk costs mean that such wholesale change remains highly unlikely. But it is not impossible. As we discuss at the end of this essay, many fear that we may be headed toward a balkanized version of this outcome, involving multiple, regional Internets governed in distinct ways and only loosely connected, if at all.

In highlighting the technical level’s importance to digital governance, however, we do not mean to disassociate it from other governance institutions nor ignore the “social” aspects of cyberspace as an institution. Technical hardware is still largely built, and software still coded by individuals, who are themselves embedded in institutions that encompass an (often dense) collection of norms. Changing those norms may thus

⁹ On top of these layers of “code” lies a non-technical content layer that comprises information exchanged through the Internet and related digital technologies.

¹⁰ See, e.g., Lawrence Lessig, *Code and Other Laws of Cyberspace*, (Basic Books, 1999): p. 190; Jonathan Zittrain, *The Future of the Internet and How to Stop It*, (Yale University Press, 2008); Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*, (Basic Books, 2006); Tim Wu, “When Code Isn’t Law,” *Va L. Rev.* 89, no. 4 (2003): p. 679, <https://heinonline.org/HOL/LandingPage?handle=hein.journals/valr89&div=26&id=&page=>.

¹¹ Anonymity was an original feature of the Internet, one that has eroded as commercial firms track user preferences and additional security measures were added. See, e.g., Jeffrey Kosseff, *The United States of Anonymous*, (Cornell University Press, 2022); Zittrain, *The Future of the Internet*, p. 32.

generate changes at the technical level. As such, “if code is a governing mechanism unto itself, it is one that rests on social norms deeply held by its authors.”¹²

II. Ordering Cyberspace at the Micro Level: The Domain Name System (DNS) as an Institution

The Internet began during the Cold War as an effort by the U.S. to link together a few mainframe computers. Initiated by the [Defense] Advanced Research Projects Agency (ARPA or DARPA), a then-newly created arm of the Department of Defense, this was the genesis of the original “Arpanet.” The first Arpanet communication was sent to Stanford from UCLA on October 29, 1969.¹³ That history is significant, because as a result virtually every major aspect of the Internet is linked to the U.S. Indeed ICANN, and many of the top technology firms, are headquartered in California because of this history.

The early Internet was tiny and dominated by a small tribe of computer scientists and engineers, many based at universities. As computing technology expanded rapidly, however, so too did the reach of the Arpa/Internet. In 1972 email was first developed, and the Internet’s utility as a communications platform came into sharper focus.¹⁴ At this stage several networks existed but not all were compatible, nor intended to be. The Defense Department had the Arpanet but also, later, the MILNET. In short, the practice for much of the 1970s and 1980s was not a single comprehensive network but instead a series of distinct, purposive networks that comprised like-minded users. This early approach is markedly different from the single, all-encompassing Internet we know today.

In 1985, the US National Science Foundation’s NSFNET program was the first to explicitly endeavor to build a single multifaceted, all-purpose network.¹⁵ NSF invested some \$200 million into the Internet from 1986-1995. At the same time, DARPA and NSF worked to ensure that their respective networks were interoperable.¹⁶ The Internet as we now know it was beginning to form, and the complexities of governance were growing.¹⁷ The U.S. government was the prime mover behind these developments, but the actual activities took place outside the federal government,

¹² See generally Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity,” *AM. J. INT’L L.* 110, no. 3 (2016): pp. 425, 461, doi:10.1017/S0002930000016894; Steven Weber, *The Success of Open Source*, (Harvard University Press, 2009).

¹³ Zittrain, *The Future of the Internet*, p. 27.

¹⁴ Barry Leiner, Vinton Cerf, David Clark, Robert Kahn, Leonard Kleinrock, Daniel Lynch, Jon Postel, Larry Roberts, and Stephen Wolff, “Brief History of the Internet,” *Internet Society*, (1997): p. 4, <https://www.internetsociety.org/internet/history-internet/brief-history-internet/>.

¹⁵ NSF funding for internet connections, which dramatically expanded the network, required universities to be in an open network.

¹⁶ Leiner et al., *Brief History of the Internet*, p. 4; Matthew Lyon and Katie Hafner, *Where Wizards Stay Up: The Origins of the Internet*, (Simon & Schuster, 1996), pp. 242–56.

¹⁷ The ARPANET was decommissioned in 1990. Robert Kahn and Vinton Cerf, “What is the Internet (And What Makes It Work)” (Corporation for National Research Initiatives, 1999), <http://www.policyscience.net/cerf.pdf>.

mostly at academic institutions, and much of the infrastructure was built by and owned by private actors.

Up until this point, politics, property rights, and commercialization were not high priorities. Governance of the Internet was informal and, until it became apparent that website names (i.e., “cars.com”) had real value, relatively uncontested. Early Internet governance was primarily focused on addressing coordination problems – developing interoperable technical standards and choosing among competing visions for solutions to technical problems. In the early 1990s the Federal Networking Council was created to better coordinate Internet activities. In the same period the non-governmental Internet Engineering Task Force (1986), and the Internet Society (1992) emerged. Composed of technical people, they largely treated Internet governance as a technical problem.

Governance remained quite limited even into the 1990s. Indeed, until 1998, the work of awarding domain names and IP addresses was largely handled by a researcher at UCLA (and later USC) named Jon Postel.¹⁸ This naming and numbering function is critical because it is what ensures that the Internet actually works as intended; that when you type in www.oup.com your browser actually goes to Oxford’s site. It is also what allows us type in “oxford university press” rather than a string of numbers.

Internet growth exploded during the 1990s. In 1994, *Today Show* host Bryant Gumbel could ask on live television, “what is the Internet, anyway?”¹⁹ By 2000, the first big dot com crash had occurred and nearly every American had heard of the Internet. This reflected a critical change in the politics of the Internet—one reflective of US policy preferences. As two key players recount:

For a long time, the federal government did not allow organizations to connect to the Internet to carry out commercial activities....[but eventually] Congress passed legislation allowing NSF to open the NSFNET to commercial usage...in April 1995, NSF ceased its support for the NSFNET. By that time, many commercial networks were in operation and provided alternatives to NSFNET for national level network services.²⁰

The Internet’s character in the late 1990s thus began to transform from science to commerce and from specialists to the general public. The Clinton administration, noting this shift, began to view the Internet largely as an economic resource. As more commercial actors moved online, it became clear that websites could be a very valuable form of property. Myriad ownership disputes ensued. These “included not only questions of who owned a given domain name, but also—and most importantly—who controlled the right to award names.”²¹ Yet because the Internet had evolved

¹⁸ U.S. Gov’t Accountability Office, “Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers,” OGC-00-33R, July 7, 2000, <http://www.gao.gov/assets/90/89949.pdf>.

¹⁹ NBC, “What is the Internet, Anyway?,” 1994, https://www.youtube.com/watch?v=UIJku_CSyNg at 1:26.

²⁰ Kahn and Cerf, “What is the Internet.”

²¹ Kal Raustiala, “Governing the Internet,” *AM. J. INT’L L.* 110, no. 3 (July 2016): pp. 491, 494, doi:10.1017/S0002930000016912.

organically, with little thought that it could raise fundamental questions of property rights, let alone geopolitical issues, basic questions of ownership and authority were unclear. Indeed, in response to a 1995 Internet Society proposal to revamp the domain name process, a U.S. official asked “Is [the Internet Society] claiming that it has jurisdiction and overall responsibility for the top-level address and name space? If yes, how did [it] obtain this responsibility; if no, then who does own it?”²²

That these basic questions remained unresolved underscored how unusual a resource the Internet was. In 1995, NSF called a conference to try to clarify authority over the Internet. The assembled stakeholders had divergent views. The Pentagon argued that it had funded the creation of the Arpanet and still funded the work of Jon Postel; therefore, the Defense Department owned the crucial naming and numbering function. Indeed, U.S. officials in this period warned that any attempt to manipulate the naming system “would be prosecuted as a criminal offense.”²³ Underlying all these claims was the belief that the U.S. “possessed ultimate authority over the Internet’s deep structure, including naming and numbering authority.”²⁴

Even as the U.S. asserted for itself a significant governing role, it was not entirely clear on what basis it did so. Though plainly a funder and progenitor of the early Internet, much of the infrastructure was private—and increasingly global.²⁵ This uncertain foundation became even more significant later, as the Internet became a central focus of many other governments.

Whatever doubts accompanied U.S. claims of control, however, the Internet’s naming and numbering continued to be administered from California; key firms were nearly all American; and many of the root servers were physically based in the U.S. The U.S. “position at the center of the global Internet brought it major economic, military, and intelligence benefits.”²⁶ By the end of the 1990s the contemporary Internet—mass use, largely for personal and commercial purposes, that spanned internationally—had supplanted the early domestic, research-based networks of the past. The Internet’s increasingly private orientation and “ultimate commercial triumph” was “a product of the specific political economy context” of the U.S.²⁷ The Internet grew rapidly in this new guise. Indeed, by 1999 there were roughly 200 million users—a huge change from a decade earlier, but a number soon to be an order of magnitude higher. In this new world, a novel governance approach—and one that was far more global—was required.

²² Mueller, *Ruling the Root*, p.136.

²³ *Id.*, p. 162.

²⁴ Goldsmith and Wu, *Who Controls the Internet*, p. 41.

²⁵ Zittrain, *The Future of the Internet*, p. 27.

²⁶ Adam Segal, “When China Rules the Web: Technology in Service of the State,” *FOREIGN AFF.* 97, no. 5 (September/October 2018): pp. 10, 18. <https://omnilogos.com/when-china-rules-web-technology-in-service-of-state/>.

²⁷ Peter Cowhey and Jonathan Aronson, *Transforming Global Information and Communication Markets*, (MIT Press, 2009): p. 209.

III. Fragmentation or Specialization – A Meso-level image of cyberspace as a regime complex

The enormous expansion of the Internet by 2000 led to several efforts to create a more sound footing for digital governance in the 21st century. A variety of institutions were either created to regulate, or gravitated toward regulating, the newly-significant digital domain. By the early 2000s a regime complex—an array of overlapping and non-hierarchical governance institutions—for digital governance had arisen.

For instance, rather than have one person in California run the crucial naming and numbering process, in 1998 the U.S. Government—tellingly deploying the Commerce Department—solicited proposals for a new approach. The winning concept was a non-profit entity based in Los Angeles known as the Internet Corporation for Assigned Names and Numbers (ICANN). In contracting with ICANN to manage the domain name system, Commerce expressed an eventual goal of privatizing Internet governance.²⁸ Doing so would, however, take the better part of two decades. Eventually, in 2016, Commerce relinquished contractual control over ICANN's functions and the U.S. become one among many governments working in a “Government Advisory Committee” that provides input to ICANN's governing board alongside many other actors. Today, ICANN remains a non-profit company incorporated under California law, albeit one that operates globally, with “individuals, non-commercial stakeholder groups, industry, and governments play[ing] important roles in its community-based, consensus-driven, policy-making.”²⁹

ICANN, however, only governs a discrete—albeit critically important—part of the digital domain via multistakeholder means. Different institutions have emerged to govern other aspects of the digital domain such as Internet protocols (IETF), web standards (World Wide Web Consortium) and network interconnections (Internet exchange point operators). Other, more recent, multistakeholder governance examples include *The Paris Call for Trust and Security in Cyberspace*, which has garnered over 1000 signatories (including national and sub-national governments, firms, and civil society actors) from whom certain “communities” have coalesced to clarify its nine principles’ operation and build capacity to follow them.³⁰

In contrast to these multistakeholder efforts, many states, seeking greater sovereign control over digital flows, have advocated for a more multilateral approach to digital governance. As the communications aspects of the Internet became more central, for example, the International Telecommunications Union (ITU), an international organization dating to 1865, became the fulcrum for state-led regulatory efforts. In

²⁸ U.S. Department of Commerce, “Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers,” Sept. 30, 2000, <https://www.ntia.doc.gov/page/1998/memorandum-understanding-between-us-department-commerce-and-internet-corporation-assigned->.

²⁹ ICANN, “ICANN's Multistakeholder Model,” <https://www.icann.org/community>.

³⁰ “Paris Call for Trust and Security in Cyberspace,” November 12, 2018, <https://pariscall.international/en/>; Government of Canada, “FAQ—The Paris Call for Trust and Security in Cyberspace,” May 2020, <https://www.canada.ca/en/democratic-institutions/news/2020/05/frequently-asked-questions---paris-call-trust-and-security-in-cyberspace.html>; see also “Christchurch Call to eliminate terrorist and violent extremist content online,” <https://www.christchurchcall.com/supporters.html>.

2012, the ITU's adoption of the International Telecommunications Regulations at the World Conference on International Telecommunications included an assumption of authority over Internet governance that severely divided ITU members; dozens of states refused to participate in the new treaty, fragmenting ITU treaty commitments in the process.³¹ Earlier, in 1998, Russia had proposed that the UN consider devising a treaty to regulate "information weapons."³² Russia's proposal received a cool reception from states concerned that this would unduly limit political speech. Yet many warmed to the broader idea that states should prioritize the potential for online behavior to threaten international security. The result has been two decades of various UN "Groups of Governmental Experts" or GGEs – small, closed groups of between 15-25 states' representatives who issued various consensus reports identifying rules of the road for state behavior online through voluntary norms and calls to apply existing international law.³³ Alongside the most recent GGE, the UN also established a more accessible "Open Ended Working Group," open to all member states.³⁴

These efforts have been situated in the UN General Assembly First Committee, limiting their jurisdiction to "disarmament, global challenges and threats to peace that affect the international community."³⁵ Plans for negotiation of a UN Cybercrime Convention would, however, not only expand the UN's attention to regulating private actor behavior but also do so via legally binding mechanisms akin to those rejected at the ITU.³⁶ Meanwhile, other states have promoted a greater role in digital governance for non-UN multilateral institutions, including the Shanghai Cooperation Organization, the G7, and the G20.³⁷

³¹ See ITU, "Final Acts of WCIT-12, World Conference on International Telecommunications," Dec. 3-14, 2012, <http://www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf>; Tim Maurer and Robert Morgus, "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate" (Global Commission on Internet Governance, May 2014), https://www.cigionline.org/sites/default/files/no7_2.pdf.

³² See Russian Federation, "Letter dated September 23, 1998 from the Permanent Representative of the Russian Federation to the United Nations concerning Agenda Item 63," U.N. Doc. A/C.1/53/3, September 23, 1998, <https://digitallibrary.un.org/record/261158?ln=en#record-files-collapse-header> ("Russia Sept. 23, 1998 Letter").

³³ See, e.g., "Advancing responsible State behavior in cyberspace in the context of international security," UNGA Res. 73/266, UN Doc. A/Res/73/266, (Jan. 2, 2019); "Developments in the field of information and telecommunications in the context of international security," UNGA Res. 70/237, UN Doc. A/Res/70/237, (Dec. 30, 2015).

³⁴ "Developments in the field of information and telecommunications in the context of international security," UNGA Res. 73/27, UN Doc. A/Res/73/27, (Dec. 11, 2018).

³⁵ U.N. General Assembly, "Disarmament and International Security (First Committee)," <https://www.un.org/en/ga/first/>.

³⁶ UN Press Release, "General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations," United Nations GA/12328, May 21, 2021, <https://press.un.org/en/2021/ga12328.doc.htm>.

³⁷ See, e.g., Government of Canada, "The Charlevoix G7 Summit Communique," last modified June 9, 2019, <https://www.international.gc.ca/world-monde/international-relations-relations-internationales/g7/documents/2018-06-09-summit-communique-sommet.aspx?lang=eng>; G20, "Antalya Summit Leader's Communique," 2015, <http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/>; "Letter dated January 9,

Regional organizations like the European Union have also been active in digital governance issues.³⁸ The EU's most significant contribution is the EU's Global Data Protection Regulation (GDPR), an internal EU law that regulates the use of personal data and has had global impacts as even non-EU firms regularly conform to its terms to preserve an ability to market their services in the EU (and avoid huge fines for non-compliance).³⁹

Finally, information and communication technology (ICT) companies have demonstrated an interest in self-regulation. The two most prominent examples to date of such processes are the Microsoft-initiated Cybersecurity Tech Accord and the Siemens-led Charter of Trust.⁴⁰ Other actors, such as Google and Facebook/Meta, are so large and powerful that they effectively govern significant swaths of on-line behavior – including regulating what content is visible or accessible – via their own terms of service or by other innovative processes, such as the new and controversial Meta Oversight Board.⁴¹

Today, therefore, no one institution dominates or even sits at the center of the global digital regime complex. Manifold actors and institutions jockey for control of various facets of how the technology operates, what states and others can do with it, and the content it hosts. The prime political fault-line, however, has been between those states seeking a greater level of government control and those that seek to retain non-state actors as central voices and regulators. In short, the struggle has largely been between forces of multilateralism and forces of multistakeholderism; in a sense, the very divide identified by John Perry Barlow some 25 years ago.

While there are historical analogues to international institutions having private origins⁴², the pattern here remains striking nonetheless. Over the last several decades

2015, from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," UN Doc. A/69/723, annex, (Jan. 9., 2015), <https://digitallibrary.un.org/record/786846?ln=en> ("Revised SCO Code of Conduct").

³⁸ See, e.g., Council of Europe, "Convention on Cybercrime," CETS No 185, Nov. 23, 2001, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=185>; African Union, "AU Convention on Cyber Security and Personal Data Protection," AU Doc. EX.CL/846(XXV), June 27, 2014, <https://au.int/sites/default/files/treaties/29560-treaty-0048-african-union-convention-on-cyber-security-and-personal-data-protection-e.pdf> (not yet in force). The EU has also endorsed a diplomatic "toolbox" for responding to malicious cyber activities. EU, "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities," EU Doc. 10474/17, June 19, 2017, <https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf>.

³⁹ EU, "General Data Protection Regulation," <https://gdpr-info.eu/>. On the EU's capacity to regulate internally with global effect, see Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, (Oxford University Press, 2020).

⁴⁰ Tech Accord, "Cybersecurity Tech Accord," <https://cybertechaccord.org/>; "The Charter of Trust," <https://www.charteroftrust.com/>.

⁴¹ See, e.g., Kate Klonick, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression," *Yale L.J.* 129, no. 8 (June 2020): p. 2318, <https://www.yalelawjournal.org/feature/the-facebook-oversight-board>.

⁴² Consider, for example, the history of state-sanctioned business enterprises like the Dutch and British East India Companies laying a foundation for global trade regimes. And, despite the ITU's current multilateral orientation, it is worth noting that the telegraph itself originated with

most other domains of global governance have witnessed states ceding only limited – and often revocable – power and authority to non-state actors and international organizations.⁴³ In the digital domain, however, the process has moved in the opposite direction. States have gained greater authority and power over time in part by proliferating new institutions and governance bodies or confirming existing institutions' operation in or applicability to cyberspace.

For now, non-state actors still retain substantial power and authority. This may be a function of their own expertise and role as “owners” of so much of the digital ecosystem. But it is also at least in part due to key states (above all the US, but also many of its Western allies) preferring the multistakeholder approach, for reasons we explore more fully below. Here again the peculiar history of the Internet is essential: because the Internet was fundamentally an American project, the US had substantial control over its development. But over time, as the Internet grew and expanded globally, that level of control engendered growing criticism from other nations. Recognizing that the status quo of US contractual oversight of institutions like ICANN could not continue – and in order to retain the open, flexible Internet the U.S. liked (and American firms benefited hugely from) – the U.S. facilitated devolving more power to multistakeholder bodies, while working hard to block exclusively state-centric and formalized approaches pushed at multilateral conclaves such as the ITU and, to a lesser extent, the UN for fear they'd embolden more autocratic powers and their interests.

To date, therefore, the story of change in digital governance has often been one of reinforcing ordering principles evident since the Internet's early days. This has largely been a process of adaptation rather than transformation. The expanding range of institutions involved may also be cast as a story of specialization – specific institutions emerging to address particular governance challenges – rather than the fragmentation some fear may devolve the Internet into separate and competing institutional spheres.⁴⁴ Such a transformational, rather than adaptive, change to the extant regime complex would require not simply supplanting multistakeholder and industry self-governance with multilateral models but the substitution of those ordering principles with new principles grounded in sovereign control over digital flows—principles that, in practice, would dramatically alter the Internet as we know it.

IV. Macro-Level Competition – What is Cyberspace For?

The principles that guide the governance of the digital domain are deeply contested. The early Internet was guided by principles of openness that were largely

private entrepreneurs (Samuel Morse) and companies like the Western Union Telegraph Company.

⁴³ See, e.g., Kal Raustiala, “NGOs in International Treaty-Making,” in *The Oxford Guide to Treaties*, edited by Duncan B. Hollis (Oxford University Press, 2020): pp. 173-197.

⁴⁴ See, e.g., Raymond and DeNardis, “Multistakeholderism: Anatomy of an Inchoate Global Institution”; Christian Rhule, Duncan Hollis, Wyatt Hoffman, and Tim Maurer, “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads,” *Carnegie Endowment for Int'l Peace* (Feb. 26, 2020), <https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110>.

seen as apolitical and technical. Then, by the late 1990s, the Internet's commercial possibilities rose to the fore. The Internet became a mass phenomenon repurposed as an engine for economic prosperity. After the turn of the century, as new communications applications such as Facebook and Twitter were founded, the political, as opposed to the commercial, implications of the Internet became far more clear. The Arab Spring briefly suggested a human-centric Internet facilitating the advancement of democratic values and individual human rights. Governments in the region, however, took different lessons from those events; namely, that an open Internet was dangerous and that they could employ many of the same technologies as tools to control dissidents and political opposition.⁴⁵

These shifts in the Internet's objectives did not, however, occur in some linear progression. Rather, each "new" ordering function came to co-exist alongside, rather than supplant, the preexisting ones. The result is a digital domain where states and other stakeholders have dramatically divergent understandings of *why* governance is needed. Is the purpose to facilitate a functioning global communication network as multistakeholder communities like ICANN insist? To advance economic prosperity as the US history of support suggests? To secure human rights? To ensure the security of the state itself in ways that autocratic states like China prefer?⁴⁶ At the same time, different parts of the digital regime complex reflect different regulatory approaches to specific objectives. GDPR focuses on individuals; UN GGE reports assume the centrality of the state. And efforts to change or transform institutions, let alone the regime complex as a whole, often reflect an effort to prioritize a different ordering principle than that reflected in the status quo. Thus, as abstract as questions about *why* we govern cyberspace may seem, the answers have both descriptive value and significant normative implications for the future of the digital domain.

Three examples help illustrate the stakes of such macro-level machinations: (i) the treatment of cyberspace as a "military domain"; (ii) the susceptibility of digital technologies to regulation via existing institutions; and (iii) the push to transform cyberspace under the banner of "internet sovereignty."

First, for more than a decade, the U.S. has regarded cyberspace as a warfighting domain, akin to land, sea, or space.⁴⁷ This frame has had significant

⁴⁵ See, e.g., Jessi Hempel, "Social Media Made the Arab Spring, But Couldn't Save It," *WIRED* (Jan. 26, 2016), <https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/>.

⁴⁶ See Ron Deibert, "Toward a Human Centric Approach to Cybersecurity," *ETHICS & INT'L AFFAIRS* 32, no. 4 (Dec. 2018): p. 411, doi:10.1017/S0892679418000618; Daniel J. Weitzner, "Promoting Economic Prosperity in Cyberspace," *ETHICS & INT'L AFFAIRS* 32, no. 4 (Dec. 2018): p. 425, doi:10.1017/S0892679418000606; Duncan B. Hollis and Jens Ohlin, "What if Cyberspace was for Fighting?," *ETHICS & INT'L AFFAIRS* 32, no. 4 (Dec. 2018): p. 441, doi:10.1017/S089267941800059X.

⁴⁷ U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (2011): p. 5; see also U.S. Department of Defense, *Summary of 2018 National Defense Strategy of the United States of America* (2018): p. 6; Exec. Order No. 14028, *Fed. Reg.* 86, no. 93 (May 17, 2021): pp. 26, 647.

implications, including a rising militarization of the technology.⁴⁸ It has also led to the creation of new domestic institutions such as U.S. CyberCommand, a military branch for conducting cyber operations.⁴⁹ Other states have followed suit. Today, no less than 30 states reportedly have stood up dedicated military units capable of engaging in offensive cyber operations.⁵⁰

However, a number of states, notably China, have expressed resistance to openly adopting a “military paradigm” for cyberspace.⁵¹ Given China’s own highly regarded cyber forces, its position may appear politically convenient, if not hypocritical. Yet, there are significant institutional consequences to equating the digital domain with a military one. Most notably, if cyberspace qualifies as a military domain in which states may conduct armed conflict, then existing institutions – principally, international humanitarian law (IHL) and the right to engage in self-defense in response to an armed attack – govern state cyber operations. China and other states have resisted the application of IHL to the digital context on the grounds that it would accelerate militarization and deprive the Internet of its peaceful orientation.⁵² Indeed, it was not until May 2021 that China accepted any mention of IHL at the UN, with a passing reference to it in the latest GGE report.⁵³

Yet, even if IHL as an institution extends to cyber operations, the territorial implications of a “domain” framing continue, as seen, for example, in formulations prioritized in the influential *Tallinn Manuals*.⁵⁴ Yet, treating digital and military domains as synonymous also makes it harder to assess the existing law’s application to

⁴⁸ Jordan Branch, “What’s in a Name? Metaphors and Cybersecurity,” *INT’L ORG.* 75, no. 1 (Winter 2021): pp. 39, 41, 43, 61, doi:10.1017/s002081832000051X; see also Richard A. Clarke and Robert K. Knake, *The Fifth Domain* (Penguin, 2019).

⁴⁹ U.S. Secretary of Defense, “Memorandum: Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations, June 23, 2009, <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf>.

⁵⁰ Steve Ranger, “US Intelligence: 30 Countries Building Cyber Attack Capabilities,” *ZD NET*, (Jan. 2017), <https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/>.

⁵¹ Zhixiong Huang and Kubo Macak, “Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches,” *CHINESE J. INT’L L.* 16, no. 2 (June 2017): p. 21, doi:10.1093/chinesejil/jmx011.

⁵² See, e.g., Julian Ku, “How China’s Views on the Law *Jus Ad Bellum* Will Shape its Legal Approach to Cyberwarfare,” (Stanford: Hoover Institution, August 17, 2017), <https://www.hoover.org/research/how-chinas-views-law-jus-ad-bellum-will-shape-its-legal-approach-cyberwarfare>.

⁵³ “Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,” May 28, 2021, ¶71(f), <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf> (2021 GGE Report).

⁵⁴ See Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber-operations*, 2nd ed. (Cambridge University Press, 2017). For more on territorialization (and deterritorialization) of cyberspace, see Daniel Lambach, “The Territorialization of Cyberspace,” *INT’L STUD. REV.* 22, no. 3 (Sept. 2020): p. 482, <https://doi-org.eres.qnl.qa/10.1093/isr/viz022>.

behaviors that cannot be reduced to physical connection points (e.g., a server) as is the case with the rising tide of disinformation or misinformation campaigns.⁵⁵

This raises a second issue – whether the novelties of the digital domain mean that pre-existing institutions and legal regimes cannot effectively govern. The question has persisted since the Internet’s early days with proponents (a la Barlow) calling for tailor-made rules for digital technologies versus those insisting pre-existing rules and institutions provide appropriate governance. Thus, U.S. Judge Frank Easterbrook famously invoked the idea that, just as there is no “law of the horse,” but rather general principles of law that can be applied to horses, cyberspace does not require its own regulatory frameworks; a view later contested by Lessig’s exploration of how the technology’s architecture challenges the capacity of pre-existing legal institutions to govern effectively.⁵⁶

A similar dialectic has emerged in international relations. Some states insist existing institutions suffice to effectively govern cyberspace, while others suggest new and more particularized institutional frameworks are needed.⁶⁵ Russia, for example, has followed up its earlier calls for a treaty to regulate information weapons with a (successful) push to have the UN take up negotiations for a new Cybercrime Convention, notwithstanding the existing Budapest Convention on Cybercrime.⁵⁷ But authoritarian regimes are not the only proponents of new institutions; in February 2017, Microsoft President Brad Smith called for a “Digital Geneva Convention” that would, *inter alia*, protect otherwise innocent users.⁵⁸

The issue is not, however, a simple binary choice between preserving existing (often multistakeholder) institutions or devising new multilateral ones. After all, there are preexisting multilateral institutions that can govern cyberspace (e.g., IHL) in lieu of negotiating a new treaty. As such, these debates often implicate another issue – the sufficiency of existing analogies. Consider, for example, the rising problem of cyber-attacks, intrusions, and ransomware. For some, such malicious cyber behavior analogizes to existing criminal behavior (albeit through new tools and techniques), justifying the application of existing domestic criminal law institutions. In this context, some argue new transnational law enforcement vehicles are needed. For others, however, the criminal law analogy is insufficient; the significant effects of at least some cyber-attacks arguably rise to the level of a use of force. For still others, the *sui*

⁵⁵ Branch, “What’s in a Name?,” p. 60.

⁵⁶ Compare Frank H. Easterbrook, “Cyberspace & the Law of the Horse,” 1996 U. CHI. LEGAL F. 207 (1996), [https://heinonline.org/HOL/LandingPage?handle=hein.journals/uchclf1996&div=9&id=&page=](https://heinonline.org/HOL/LandingPage?handle=hein.journals/uchclf1996&div=9&id=&page=,), with Lawrence Lessig, “The Law of the Horse: What Cyberlaw Might Teach,” HARV. L. REV. 113, no. 2 (Dec. 1999): p. 501, doi:10.2307/1342331.

⁶⁵ In national statements accompanying the 2021 GGE report, Estonia, Norway, and Romania all rejected the need for a new cyber-specific treaty. 2021 GGE Report, annex: pp. 24 (Estonia), 66 (Norway), 75 (Romania). Russia, in contrast, urged the adoption of a “binding universal convention on international information security at the UN level.” *Id.* at 80.

⁵⁷ See, e.g., Russia Sept. 23, 1998 Letter.

⁵⁸ See Brad Smith, “The need for a Digital Geneva Convention,” RSA, Feb. 14, 2017, <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.

generis character of cyber-attacks belies relying on any existing institutions.⁵⁹ An array of different governance bodies have taken stabs at resolving these issues, with no clear hierarchy in place. The *Tallinn Manuals*, for instance, are a largely academic enterprise (yet sponsored by NATO) that have assumed the capacity of existing international legal institutions to analogize to the cyber context, a view that largely tracks views among Western states. Other approaches, like those proffered by the Shanghai Cooperation Organization, assume a novelty to cyber operations and their effects that requires new rules of the road.⁶⁰

Further complicating these analogies is the problem of attribution – it is necessary to know who authored a cyberattack to ascertain which institutions apply (i.e., criminal law governs individuals, international law governs states). If, as some experts assume, technical attribution is too difficult given the digital domain's architectural preferences for anonymity, that counsels in favor of new regulatory institutions.⁶¹ Over the last decade, however, states have claimed greater attribution capacities. In July 2021, for instance, NATO and EU members attributed a set of serious attacks to Chinese actors.⁶² Many other attacks on the West have been attributed to Russia, or (private) criminal elements allowed to operate from its territory. Such attributions remain politically controversial, and there is little agreement on the types, or sufficiency, of evidence necessary to establish responsibility politically, let alone legally.⁶³

As Internet usage has permeated every corner of the globe (4.66 billion estimated users⁶⁴), a third macro-level issue – increasing claims of sovereign control over the Internet, whether by individual states within their territories and/or by states acting collectively through multilateral institutions—has taken centerstage. The result of this evolution has been the rise of a new principle – *cyber sovereignty* – as a key counter-principle to the status quo of digital governance. While many states, especially authoritarian ones, favor cyber sovereignty as a core guiding principle, perhaps the most powerful and influential proponent is China. For China, the concept of *wangluo zhuquan* or “Internet sovereignty” puts states’ rights and their interests in controlling digital flows first.⁶⁵ This is of a piece with China’s larger effort to surveil

⁵⁹ See Thomas Rid, *Cyber War Will Not Take Place*, (Oxford University Press, 2013); Jon Lindsay, “Restrained by Design: The Political Economy of Cybersecurity,” *DIGITAL POL’Y REG. AND GOV.* 19 (Sep. 2011): p. 493, <https://www.emerald.com/insight/content/doi/10.1108/DPRG-05-2017-0023/full/html>.

⁶⁰ See, e.g., Revised SCO Code of Conduct.

⁶¹ See, e.g., Duncan B. Hollis, “An e-SOS for Cyberspace,” *HARVARD INT’L L. J.* 52, no. 2 (2011): p. 374, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1670330.

⁶² “United States Joins with Allies, Including NATO, to Attribute Malicious Cyber Activities to China,” *AM J. INT’L L.* 115, no. 4 (2021): p. 715.

⁶³ Kristen Eichensehr, “The Law and Politics of Cyberattack Attribution,” *UCLA L. REV.* 67 (2020): pp. 520, 538-39, <https://www.uclalawreview.org/wp-content/uploads/securepdfs/2020/09/Eichensehr-67-3.pdf>.

⁶⁴ Joseph Johnson, “How many people use the Internet,” Statista, April 2022, <https://www.statista.com/statistics/617136/digital-population-worldwide/> (4.66 billion).

⁶⁵ Adam Segal, “China’s Vision for Cyber Sovereignty and the Global Governance of Cyberspace,” *National Bureau of Asian Research Special Report No. 37*, (August 25, 2020),

and manage its populace and to limit information flows, including most famously by blocking large foreign applications such as Facebook and Twitter within its territory. By contrast, the principle of openness to digital flows that has guided the Internet since its inception in 1969 aspires to a largely frictionless mode of communication and interaction in which sovereign borders, as Barlow tried to claim, have little to no bearing.

Thus, at the most abstract level of an ordering principle, three broad visions or ideal types dominate debates over the governance of digital technologies, what we call the *Chinese, Californian, and Carolingian* visions of the Internet. The Californian vision was the first and has been dominant for a long time. The Carolingian vision, grounded in a powerful and active European regulatory state and focused on protecting consumers and Internet users' data on-line and its use by third parties, is rising in prominence and may prove potent throughout the West. But the war, it appears, is increasingly being won by the sovereignty-focused Chinese vision.⁶⁶

China is not the only state to severely curtail digital flows and to limit access to specific sites and applications. Other authoritarian states have done the same, sometimes for brief periods, sometimes longer.⁶⁷ Even in the West there is increasing attention to the dangers of disinformation and misinformation on platforms like Facebook, Google, and Twitter with increasing calls for greater government control over content. The huge dominance of American technology firms has, moreover, encouraged the Chinese vision. This is, in part, to blunt that dominance, but also in part because, with some reason, American firms are seen as especially reactive to American concerns. Facebook, for example, reportedly spends nearly 90% of its misinformation budget on English-speaking posts, despite its user base being only 9% English-speaking.⁶⁸ As a result, China has acted on its repeated calls for internet sovereignty as the appropriate guiding principle for the 21st century by building out its own digital ecosystem, populated by a set of Chinese firms—Weibo, WeChat—that mirror offerings from the United States.

And even though they may lack equivalent firms, other states are finding the lure of employing their sovereign authorities via internal regulation appealing. The EU, for example, has doubled-down on its own regulatory approach as it looks to pair GDPR with new regulatory authorities to fine Internet platforms for posting illegal content, control artificial intelligence applications, and potentially break up technology companies on antitrust grounds.⁶⁹ Europe, in short, offers a vision of Internet governance in which openness is curtailed but only in a limited fashion consistent with

<https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/>.

⁶⁶ See Graham Webster and Justin Sherman, "The Fall and Rise of Techno-Globalism," *Foreign Affairs*, (Oct. 2021), <https://www.foreignaffairs.com/articles/world/2021-10-28/fall-and-rise-techno-globalism>.

⁶⁷ See, e.g., Tina Freyburg and Lisa Garbe, "Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa," *INT'L J. COMM.* 12, (Oct. 2018): p. 3896, <https://www.alexandria.unisg.ch/255303/>.

⁶⁸ Colm Quinn, "Facebook's Problems Aren't Only in Washington," *Foreign Policy Morning Brief*, Oct. 7, 2021, <https://foreignpolicy.com/2021/10/07/facebook-problem-washington-haugen/>.

⁶⁹ EU, "General Data Protection Regulation"; Bremmer, "The Technopopular Moment," p. 6.

the protection of individual rights to privacy and control over personal data. One might broadly analogize this emergent European approach to what John Ruggie decades ago characterized as the “compromise of embedded liberalism”: a broadly open but socially regulated system. This Carolingian model, which utilizes the EU’s historically strong regulatory apparatus, is distinct from the Californian and Chinese models but arguably sits somewhere between them.

One result of these trends is the prospect, growing ever more likely, of a set of internets rather than a single comprehensive network. Sometimes termed the “splinternet” scenario, this is generally viewed as a degradation of the value of the global Internet.⁷⁰ Yet the political incentives for greater national control seem to be increasingly pushing in this direction. A free and open Internet, like the concept of free trade, offers an appealing principle, but one that often faces difficult politics.

Conclusions

Our brief survey of global governance in the digital domain reveals a heterogenous, dynamic, multi-layered set of principles, regimes and institutions that not only govern cyberspace, but have adapted and transformed along pathways that may serve as signposts for other international institutions involved in issues of global governance. Here we offer a few thoughts on the most significant dimensions and implications of this evolution.

First, by identifying the “social-technical institution” that is the digital domain, we have identified not only the central aspect of digital governance but a factor that increasingly touches all areas of human engagement.

Second, the digital domain is one of the most complex systems in existence (and certainly the most complex that is man-made) and yet it does not appear to require *multilateral* governance. The story of ICANN and the larger history and ordering of governance in the digital domain suggest multistakeholder governance can operate effectively, even as security and other concerns complicate its future. The balance between the two forms, as we have emphasized, remains hotly contested and still to be determined.

Of course, classical economists thought much the same about the international economy and the trading system. If only certain limited commitments were made, such as no tariffs, use of the gold standard, and the like—the system would be allegedly self-regulating. But politics intruded to disrupt this system, which never really operated without state action anyway. And by the mid-20th century, after the world was wracked by war and depression, the compromise of embedded liberalism, in Ruggie’s famous phrase, took hold.⁷¹ Perhaps the same broad process is occurring today in the digital domain, as witnessed by increasing calls for tech company regulation. If so, over time some kind of embedded digital openness may take root, in which the Internet

⁷⁰ See Webster and Sherman, “The Fall and Rise of Techno-Globalism”; Mark A. Lemley, “The Splinternet,” *DUKE L. J.* 70, no. 6 (2021): p. 1397; but see Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, (Polity, 2017): p. 18.

⁷¹ John Gerard Ruggie, “International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order,” *Int’l Org.* 36, no. 2 (Spring 1982): pp. 379, 393-98, doi:10.1017/S0020818300018993.

remains a single, broadly cohesive network, but with many national level controls to rein in the worst excesses of unfettered digital flows. Arguably the move to greater content regulation and moderation, the many restrictions on data and privacy being promulgated around the world, and new efforts to devise cyber norms for state operations in cyberspace are evidence of such an emergent—and broadly Carolingian—compromise.

The alternative, often bemoaned by cyber analysts, is the “splinternet”: the idea that instead of a broadly global resource, we are moving rapidly toward discrete sets of smaller Internets, each subject to its own governing principles and rules. In this fashion, perhaps, the Californian, Chinese, and Carolingian visions can coexist, much as during the Cold War the capitalist and communist economies coexisted with limited interaction across domains, but substantial interactions within them. For those who fear that outcome, a compromise of embedded openness may yet prove attractive.