University of Pennsylvania Carey Law School

ILE

INSTITUTE FOR LAW AND ECONOMICS

A Joint Research Center of the Law School, the Wharton School,
and the Department of Economics in the School of Arts and Sciences
at the University of Pennsylvania

RESEARCH PAPER NO. 23-33

Crouching Tiger, Hidden Agenda?: The Emergence of China in the Global Internet Standard-Setting Arena

Alex Mueller
UNIVERSITY OF PENNSYLVANIA CAREY LAW SCHOOL

Christopher S. Yoo
UNIVERSITY OF PENNSYLVANIA CAREY LAW SCHOOL

Crouching Tiger, Hidden Agenda?: The Emergence of China in the Global Internet Standard-Setting Arena

Alex Mueller[*] and Christopher S. Yoo[†]

ABSTRACT

China is making an active push to enlarge its role in the development of Internet-related technical standards. The prevailing narrative surrounding this trend suggests that Beijing is aiming to uproot the liberal, democratic values embedded in the Internet's technical foundation and governance arrangements in favor of authoritarian-friendly alternatives. For many, these fears were fully realized when Chinese tech giant Huawei came to the UN-affiliated International Telecommunications Union (ITU) and proposed the development of a future core Internet protocol called "New IP". This proposal allegedly sought to redesign the architecture of the Internet in a way that would both enhance and export the Chinese government's capacity for digital repression. Informed by the understanding of Chinese standards influence as a geopolitical and ideological threat, many are now calling for a more aggressive response to countering Chinese engagement in Internet standards bodies. But is this conventional account missing something?

Yet, the conventional narrative seems to be missing something. Specifically, it overlooks the fact that the sophisticated Internet control apparatus China has developed over the years can already censor and surveil quite effectively at present and that shifting responsibility for core protocol development to the state-driven ITU would not necessarily enhance its ability to do so. A more comprehensive understanding of this trend is needed.

Using New IP as the primary case study, this article examines China's standard-setting push, its potential motivations, and its implications for the future of the global Internet. We conclude that it is far from clear that New IP was indeed intended as a trojan horse for digital authoritarianism. Observing that technical evolution of the Internet—particularly the type endorsed in Huawei's proposal—plays a prominent role in China's long-term industrial policy strategy, we find it equally plausible that New IP was motivated by economic considerations, something that has largely been absent from the debate over China's standards ambitions. We thus caution against the presumption that Chinese-developed standards are intended to advance the cause of digital repression as well as against politically driven opposition to growing Chinese participation at Internet standard-setting bodies. This insight is crucial, as the way American policymakers and Internet stakeholders respond to this trend will undoubtedly impact both the future of the global Internet and U.S. technological leadership in this domain.

[*] CTIC Research Fellow, University of Pennsylvania Carey Law School.

[†] John H. Chestnut Professor of Law, Communication, and Computer & Information Science and Founding Director of the Center for Technology, Innovation & Competition, University of Pennsylvania.

INTRODUCTION

In March of 2020, the *Financial Times* reported that China had introduced a new proposal at the International Telecommunications Union (ITU), an independent treaty-based organization acting as a U.N. Specialized Agency, purportedly seeking to initiate a radical, top-down re-design of the Internet.[1] The proposal revolved around something called "New IP," a new core Internet protocol that Chinese tech giant Huawei was reportedly pushing to develop at the ITU's Telecommunications Standardization sector (ITU-T).[2] The *Financial Times* article proceeded to explain that New IP would equip networks with built-in "tracking features" and a "shut up command" for blocking communications, leading it to declare that the future protocols would "bake authoritarianism" into the technical foundation of the Internet.[3] News of Huawei's proposal elicited further criticism from other Western media outlets as well as from various civil society and industry groups that urged ITU Member State delegations to oppose it.[4] Many even cited New IP as evidence of the dangers an unchecked China and/or ITU could pose to the free and open Internet.[5]

In the end, Huawei's efforts provided unsuccessful. Though it attempted to frame the initiative as a necessary technical evolution—arguing the existing Internet architecture was ill-equipped for supporting network use cases anticipated in the future—many were unpersuaded.[6] When it came time to decide whether New IP standardization activities should be initiated at the ITU-T, objections raised by several participating Member States effectively killed the proposal.[7]

Following its unceremonious demise, one might be tempted to let the New IP fade into the annals of Internet history without thinking twice about it. However, the New IP saga offers a valuable case study, one that highlights an important ongoing development in the world of Internet governance. Asin many other domains across the global governance system, China is widely

---

[1] *See generally* Anna Gross & Madhumita Murgia, *China and Huawei propose reinvention of the internet*, FIN. TIMES (Mar. 27, 2020), https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2.

[2] *Id*.

[3] *Id*.

[4] *See, e.g.*, Margi Murphy, *Internet pioneer Vint Cerf says China's plans to rewrite the web are a "dog's breakfast,"* TELEGRAPH (July 2, 2020), https://www.telegraph.co.uk/technology/2020/07/02/internet-pioneer-vint-cerf-says-chinas-plans-rewrite-web-dogs/; Stephen Shankland, *China has big ideas for the internet. Too bad no one else likes them*, CNET (July 17, 2020), https://www.cnet.com/tech/computing/china-has-big-ideas-for-the-internet-too-bad-no-one-else-likes-them/; Jon Fingas, *China, Huawei propose internet protocol with a built-in killswitch*, ENGADGET (Mar. 30, 2020), https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html; *see also, e.g.*, Ctr. for Democracy & Tech & Mozilla, Comment Letter on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly (June 8, 2020), https://ntia.gov/sites/default/files/publications/cdt-mozilla-06082020_0.pdf (urging U.S. delegates to the ITU-T to oppose New IP activities due in part to its centralized, top-down development approach).

[5] *See, e.g.*, Tom Wheeler, *The most important election you never heard of*, BROOKINGS TECHTANK (Aug. 12, 2022), https://www.brookings.edu/blog/techtank/2022/08/12/the-most-important-election-you-never-heard-of/ (citing China's push of standards like New IP, which would "give governments more control over internet activities," as a reason why the 2022 ITU Secretary General election is pivotal.); Lindsay Gorman, *Why Biden and Blinken Are Backing a Candidate for a Little-Known U.N. Internet Agency*, LAWFARE (Sept. 28, 2022), https://www.lawfareblog.com/why-biden-and-blinken-are-backing-candidate-little-known-un-internet-agency (arguing that if countries like China and Russia succeed in pushing their agenda at the ITU, then technical proposals like New IP "could provide states the ability to control access to the internet itself.").

[6] *See* Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], "*New IP, Shaping Future Network": Propose to initiate the discussion of strategy transformation for ITU-T*, TSAG-C83 (Sept. 2019), https://www.itu.int/md/T17-TSAG-C-0083 [hereinafter TSAG-C83].

[7] *See infra* note 177 and accompanying text.

regarded as making concerted efforts to increase its role and influence in the development of international technical standards, particularly those involving information and communications technologies (ICTs), such as the Internet.[8] This push is typically viewed as part of the broader Chinese project to enhance its position within the international order and to strengthen its "discourse power"—its ability to shape global governance institutions and norms.[9] Disagreement remains over the specific ends to which China intends to use this discursive power within the standards development system as well as the extent to which it seeks to disrupt the status quo.

An increasingly common understanding of this trend sees China's foray into the standard-setting arena as a trojan horse whose true purpose is to uproot the liberal values embedded in the Internet's technical design and governance arrangements.[10] In their place, it intends to install alternatives the enable greater state control and thus align with the concept of "Internet sovereignty," the principle said to represent China's normative position on the governance of global cyberspace.[11] In other words, Beijing intends to use the country's growing standard-setting influence to design a future Internet that is more regulable, inscribing authoritarian norms of information control and surveillance into its technical foundation.[12] If successful, critics warn it would empower world governments to commit human rights violations at unprecedented scale, lead to the widespread diffusion of Chinese-style digital authoritarianism, and potentially even

[8] *See infra* Part I.B (discussing how China is increasing engagement within the ICT standards ecosystem).

[9] *See* Nadège Rolland, *China's Vision for a New World Order* 7-11 (Nat'l Bureau Asian Rsch., Special Rep. No. 83, Jan. 2020); Toni Friedman, *Lexicon: "Discourse Power" or the "Right to Speak" (话语权, Huàyǔ Quán)*, DIGICHINA (Mar. 17, 2022), https://digichina.stanford.edu/work/lexicon-discourse-power-or-the-right-to-speak-huayu-quan/.

[10] *See, e.g.*, U.S.-CHINA ECON. & SEC. REV. COMM'N, 2022 REPORT TO CONGRESS 459 (Nov. 2022) [hereinafter USCC 2022 Report]; DEMOCRATIC STAFF OF S. COMM. ON FOREIGN RELS., 116TH CONG., THE NEW BIG BROTHER: CHINA AND DIGITAL AUTHORITARIANISM 1-2 (July 21, 2020), https://www.govinfo.gov/content/pkg/CPRT-116SPRT42356/pdf/CPRT-116SPRT42356.pdf [hereinafter THE NEW BIG BROTHER]; Melanie Hart & Baline Johnson, *Mapping China's Global Governance Ambitions*, CTR. AM. PROGRESS 15-16 (2019), https://www.americanprogress.org/wp-content/uploads/sites/2/2019/02/China-Global-Governance-2.pdf.

[11] *See* USCC 2022 Report, *supra* note 10, at 460; Samm Sacks, *Beijing Wants to Rewrite the Rules of the Internet*, ATLANTIC (June 18, 2018) https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/; KENTON THIBAUT, CHINESE DISCOURSE POWER: ASPIRATIONS REALITY AND THE DIGITAL DOMAIN 23 (Aug. 24, 2022), *available at* https://www.atlanticcouncil.org/in-depth-research-reports/report/chinese-discourse-power-ambitions-and-reality-in-the-digital-domain/.

[12] *See* Daniel F. Runde & Sundar R. Ramanujam, *Digital Governance: It Is Time for the United States to Lead Again*, CTR. STRATEGIC & INT'L STUD. (Aug. 2, 2021) (stating China wants to reinvent the Internet in the name of regulating it); Paul Scharre, *The Dangers of the Global Spread of China's Digital Authoritarianism*, CTR. NEW AM. SEC. (May 4, 2023), https://www.cnas.org/publications/congressional-testimony/the-dangers-of-the-global-spread-of-chinas-digital-authoritarianism (cautioning that China's growing standard-setting influence risks spreading standards that enable "Chinese-style surveillance and repression").

bifurcate the global Internet along multipolar lines.[13] Although most of these concerns predate New IP, some regard the events at the ITU as the moment China tipped its hand.[14]

At the same time, there are reasons to question the conventional account of China's standard-setting push. The United States' foreign policy apparatus, and its so-called "Internet freedom" agenda, has long regarded the Internet as a type of unstoppable, emancipatory force that would inevitably democratize the societies in which it was embedded.[15] Meanwhile, having maintained a firm grasp over its domestic Internet for nearly three decades, China achieved what was once thought to be impossible: as President Bill Clinton famously described it, "nail[ing] Jell-O to the wall."[16] China's existing Internet control capabilities—the complex legal and technical architectures that enabled it to do so—beg the question: does China need to highjack the global standard-setting process and push through protocols like New IP just to make the Internet more regulable? To be sure, legal scholarship has long recognized how design choices underlying the Internet's technical architecture can function as the "law of cyberspace," shaping and constraining how individuals use the network much like a traditional regulatory regime.[17] Still, the nearly insurmountable difficulty of replacing the global Internet's common foundation makes it natural to ask why China would attempt to do so in the name of greater control despite having largely achieved this through other means.

As ICT standard-setting bodies become increasingly seen as sites of ideological and geopolitical contention, calls grow louder for a more aggressive approach to countering Chinese

[13] *See* Douglas W. Arner et al., *The Transnational Data Governance Problem*, 37 BERKELEY TECH. L.J. 623, 681 (2022) (arguing China is attempting to internationalize its centralized Internet structure and, consequently, create a parallel digital market dominated by Chinese firms and technologies); Joshua Kurlantzick, *How China Is Attempting to Control the "Information Pipes,"* DIPLOMAT (Mar. 03, 2023), https://thediplomat.com/2023/03/how-china-is-attempting-to-control-the-information-pipes/ (suggesting the pursuit of influence over ICT infrastructure would enable China to export its "vision of a closed and controlled domestic internet"); Stacie Hoffman et al., Standardising *the Splinternet: How China's Technical Standards Could Fragment the Internet*, 5 J. CYBER POL'Y 241, 252-53 (2020), https://doi.org/10.1080/23738871.2020.1805482 (warning that proposals like New IP could splinter the global Internet).

[14] *See, e.g.*, Emily Taylor et al., *Technical Standards and Human Rights: The Case of New IP*, *in* RECLAIMING HUMAN RIGHTS IN A CHANGING WORLD ORDER 185, 186 (Christopher Sabatini ed., 2022) (arguing New IP reveals a lot about China's ambitions and serves as a wake-up call about its potential impact on global Internet governance and standards).

[15] *See* Jack Goldsmith, *The Failure of Internet Freedom*, 18-03 KNIGHT FIRST AMEND. INST. 2-4 (June 13, 2018), https://knightcolumbia.org/content/failure-internet-freedom (examining the Internet freedom agenda that first emerged during the Clinton administration and its two main attributes: commercial non-regulation and anti-censorship); EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM xii–xiv (2012) (defining this belief in the inherently democratizing nature of the Internet as a naïve "cyber-utopianism").

[16] William J. Clinton, Remarks at the Paul H. Nitze School of Advanced International Studies (March 8, 2000), http://www.presidency.ucsb.edu/ws/index.php?pid=87714; see also Goldsmith, supra note 15, at 9 ("[A] decade after Bill Clinton's presidency had ended, China was doing a pretty good job of nailing the Jell-O of undesirable speech to the wall of Party control.").

[17] For leading early statements, see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) [hereinafter LESSIG, CODE]; Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) For later discussions, Daniel Benoliel, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology*, 92 CALIF. L. REV. 1069 (2004); Kevin Werbach, *Higher Standards Regulation in the Network Age*, 23 HARV. J.L. & TECH. 179 (2009); Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance by Design*, 106 CALIF. L. REV. 697 (2018).

influence in this sphere.[18] Yet, if the trojan horse narrative is going to inform how policymakers and participants in the global standard-setting process respond to the growing involvement of Chinese actors, it is clear that a more comprehensive understanding of the trend is needed.

This Article thus sets out to answer two primary questions. First, we ask whether China's growing standard-setting ambitions are indeed motivated by a desire to fundamentally change the Internet's technical architecture and the institutional arrangements through which it is shaped, re-aligning both with its state-centric normative orientation. Second, we inquire into what the trend of increasing Chinese engagement holds for the future of a unified, global Internet. In attempting to answer these questions, we draw primarily on a case study of New IP. Although a more measured analysis of Huawei's proposal reveals several flaws, we ultimately find reason to doubt that its sole motivations were to embed authoritarian values and to expand state control over the Internet. Instead, most of the features discussed by the proposal align closely with the type of future network capabilities China has deemed necessary for supporting its lofty industrial policy goals as well as Huawei's own financial interests. This leads us to argue that New IP may well have been motivated by economic considerations, something frequently overlooked in the broader debate over China's growing role in standards development and requires a more nuanced than countenanced by the conventional account. In other words, it cannot be assumed that every Chinese-produced technology or technical standard is intended to enable digital repression or undermine liberal, democratic values. This will become an increasingly important lesson as Chinese actors continue to grow their presence within mainstream Internet standards development bodies; the American response will undoubtedly have implications for both the future of the global Internet and U.S. technological leadership.

The remainder of this Article is organized as follows: Part I better situates our discussion by providing an overview of the Internet standards development landscape and China's evolving role therein, as by well examining China's alternative vision for the global Internet and digital governance organized around the concept "cyber sovereignty." In Part II, we shift our focus to the Article's primary case study, the New IP proposal, and construct a clearer picture of what Huawei was proposing to help better understand its possible motives. New IP was alleged to propose fundamental changes to the way the Internet works, but *how*? Part III grapples with the conventional explanation of China's standards push as a trojan horse for a more state-centric Internet architecture and standards development model. It identifies several of the theoretical shortcomings behind this framing and demonstrates how they manifest prominently in the case of New IP. Part IV then offers an alternative account of China's standard-setting ambitions, arguing they are motivated to a significant extent by economic factors. Finally, Part V explores what this trend means for the future of the global Internet and standards development. Contrary to predictions of an impending global "splinternet" or an ITU Internet takeover, we find that China has grown increasingly accepting of the existing industry-led, bottom-up, incremental approach to

[18] *See, e.g.*, U.S.-CHINA ECON. & SEC. REV. COMM'N, 2020 REPORT TO CONGRESS 537 (Dec. 2020), https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf [hereinafter USCC 2020 Report] (recommending the creation of a government committee that would coordinate the activities of private sector participants at standards bodies in order to compete with China); Sophie Faaborg-Andersen & Lindsay Temes, *The Geopolitics of Digital Standards* 1-2 (Belfer Ctr. Sci. & Int'l Affs., Harv. Kennedy Sch., Paper, July 2022), https://www.belfercenter.org/sites/default/files/files/publication/geopolitics-of-digital-standards.pdf (arguing that market-driven standards development is not equipped to repel the creep of digital authoritarianism and that the U.S. should reverse its historically hands-off approach); Bradley A. Thayer & Lianchao Han, *We cannot let China set the standards for 21st century technologies*, HILL (Apr. 16, 2021), https://thehill.com/opinion/technology/548048-we-cannot-let-china-set-the-standards-for-21st-century-technologies/.

shaping the Internet's architecture. Our conclusion thus offers a warning that coordinated and politically motivated opposition to Chinese engagement risks undermining the standards development model that has contributed to the Internet's extraordinary success.

I. CHINA'S STANDARD-SETTING AMBITIONS: A BACKGROUNDER

Protocols are the lifeblood of the Internet. They are standardized rules for formatting, interpreting, and reacting to a communication, thereby establishing a common language that enables components of a communications system to interoperate and exchange data.[19] The overall architecture of the Internet is comprised of many protocols spread across different functional "layers" into which the various tasks of the communications process are divided. The vertical combination of protocols at each layer, all of which work together to provide a full communications service, is known as the protocol stack. Protocols at the bottom layers of the stack are responsible for managing the physical transmission of data, while those in the upper layers provide features for supporting specific applications (e.g., email or web) without needing to worry about how lower-layer functions have been implemented.

However, the most fundamental protocol resides in the very middle and is simply called the Internet Protocol (IP). When data is transmitted over the Internet, it is divided into smaller packets that a system of interconnected routers then forwards along to the intended destination based on an address specified in each packet's header. It is IP that defines the structure and format of both these packets and addresses. Although there are a variety of protocols that can be used in the upper layers (e.g., HTTP for web, SMTP for email) and bottom layers (e.g., Ethernet or Wi-Fi), virtually every communication over the Internet relies on IP in the middle.[20] The centrality of IP, along with that of another important protocol called TCP at the layer above, is why the Internet as we know is said to run on the TCP/IP suite.

As implied by its name, Huawei's New IP initiative sought to undertake the modernization of this crucial Internet Protocol. Yet, before diving fully into the case of New IP, there is some important background information needed to understand why the proposal was so controversial and to fully appreciate the larger trend at the heart of this Article. The remainder of this Part will set the stage for our subsequent discussion on the underlying motives and future implications of China's Internet standards ambitions. It will do so first by introducing the system that has emerged for developing protocols and other Internet technical standards, then by outlining how China's role within this system has been quickly evolving, and finally by examining the concept cyber sovereignty which is said to inform China's goals and engagement in this sphere.

A, A Condensed Overview of the Internet Standards Development Landscape

The development of standards is an essential function of Internet governance, a term which refers to the different activities for coordinating and managing the Internet's technical infrastructure to ensure it remains operational, stable, and secure.[21] The existing system of global

[19] Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707, 1716 (2013).

[20] Due to the wide diversity of protocols at the upper and lower layers but with just one core protocol in the middle, the Internet architecture is often said to resemble an hourglass figure.

[21] Although the precise definition of Internet governance is still somewhat contested, the way we use the term here is consistent with the relatively narrow definition offered by Laura DeNardis which focuses on issues unique to the Internet's technical infrastructure. *See* LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 18-20

Internet governance is considered to be polycentric; its constituent functions are spread out across multiple different institutions, each with a unique configuration and makeup.[22] Moreover, though the term "global governance" may be commonly associated with multilateralism (i.e., state-actors engaging in collective decision-making at intergovernmental bodies like the U.N.), some of the most important functions of global *Internet* governance are performed with limited to no government involvement.[23] Instead, these functions are carried out through institutions that embody a multistakeholder governance approach, engaging a wide range of non-state actors including those from industry, civil society, and academia.[24] These defining characteristics of the Internet governance system as a whole—its polycentricity and the prominent role afforded to non-state actors—can also be found in the Internet standards development ecosystem, which consists of several primarily industry-driven, private standards development organizations (SDOs).

As mentioned above, the Internet architecture consists of many protocols spread across different functional layers of the Internet stack. The scope of responsibilities among different SDOs in the ecosystem tends to reflect the modularity of the Internet's layered architecture, with each SDO limiting their focus to a specific layer or layers of the stack. The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), for example, develops lower-layer protocols and physical infrastructure standards, most recognizably the IEEE 802.3 series (Ethernet) and IEEE 802.11 series (Wi-Fi). Similarly, a consortium of regional telecom SDOs called the Third-Generation Partnership (3GPP) defines wireless communications protocols (e.g., 5G-NR) that perform lower-layer functions in mobile broadband networks. At the topmost layer, typically referred to as the Application Layer, the World Wide Web Consortium (W3C) focuses on protocols and other standards related to web technologies.

However, the most important SDO in the Internet standard-setting ecosystem is the Internet Engineering Task Force (IETF). The IETF is an open, international community of volunteers that has traditionally been responsible for maintaining and evolving the core protocols towards the middle of the stack—including both the IP and TCP in the TCP/IP suite—as well as a significant number of different Application Layer protocols. The organization's history is closely tied to that of the Internet itself, having evolved out of the same community of U.S. government-funded network researchers and engineers that laid the foundation of what would eventually become the modern Internet.[25]

While most of the other SDOs described above could be considered "open" to varying degrees, the IETF is notoriously so.[26] All IETF standards, published in the form of documents called RFCs, are made publicly available online along with just about every other conceivable piece of information produced within the organization.[27] The IETF also has no formal membership

---

(2014) [hereinafter DENARDIS, GLOBAL WAR]; *see also* Mark Raymond & Laura DeNardis *Multistakeholderism: Anatomy of an Inchoate Global Institution*, 7 INT'L THEORY 572, 588-92 (2015) (providing a taxonomy of the different activities that fall underneath the umbrella of Internet governance).

[22] *See* DENARDIS, GLOBAL WAR, *supra* note 21, at 22-23 (describing the distributed nature of Internet governance); *see also* Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities* 7 (Ctr. Int'l. Governance Innovation, Paper No. 264, 2014) (locating Internet governance within the broader "cyber regime complex," a collection of loosely connected, non-hierarchical norms and institutions for governing cyberspace).

[23] Raymond & DeNardis, *supra* note 21, at 585.

[24] *See id*.

[25] *See* DENARDIS, GLOBAL WAR, *supra* note 21, at 67-71 (providing an overview of the IETF's historical origins).

[26] *See* A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 799 (2003); Werbach, *supra* note 17, at 199.

[27] *See* DENARDIS, GLOBAL WAR, *supra* note 21, at 71.

and thus no membership fees.[28] Any individual who wishes to participate can do so in full.[29] This includes attending any of the three annual in-persons meetings, submitting an Internet Draft (i.e., a proposed standard or informational document), or joining one of the Working Group mailing lists where much of the discussion takes place. Though a large share of participants tends to be affiliated with network operators, equipment vendors, or other companies that implement IETF standards, many also come from civil society organizations, universities, and even government agencies. That said, participants are expected to act in their individual capacities rather than as representatives of corporations or governments.[30]

The IETF is also renowned for its informal, collaborative ethos. Participants openly debate the technical merits of a proposed standard based on its real-world implementations, advancing it along the standards track only if there is widespread agreement among the group.[31] A famous adage from Internet pioneer David Clark perhaps best captures the spirit of the organization's modus operandi: "We reject kings, presidents and voting; we believe in rough consensus and running code."[32] Though certainly not without criticism, the IETF has remained the preeminent Internet standards body for nearly forty years. It is the organization's participatory and radically transparent nature to which many attribute its enduring legitimacy.[33]

It is important to keep in mind when discussing the Internet standards ecosystem that, even though a division of responsibility has emerged among the different SDOs, this has largely been the result of private self-ordering.[34] For example, there was never an inter-governmental agreement granting the IETF exclusive authority over the middle layers of the Internet stack.[35] Instead, these polycentric arrangements are informal and took shape organically over time.[36] There is often nothing preventing one SDO from engaging in standards work that has traditionally fallen under the purview of another. Nonetheless, SDOs tend to respect each other's remits and coordinate in

---

[28] *The Tao of the IETF: A Novice's Guide to the Internet Engineering Task Force*, IETF (last updated Nov. 17, 2022), https://www.ietf.org/about/participate/tao/ ("The IETF has no members and no dues.").

[29] *Id*.

[30] Harald Tveit Alvestrand, *A Mission Statement for the IETF* (IETF Network Working Grp., RFC No. 3935, 2004), http://www.ietf.org/rfc/rfc3935.txt ("The IETF has found that the process works best when focused around people, rather than around organizations, companies, governments or interest groups.") Although norms strongly discourage individual participants from representing the interests of their employers, that does not mean commercial interests do not find their way into the IETF. This can have an impact on the standard-setting process, as one empirical analysis found a statistically significant relationship between the concentration of private-sector participants in a working group—a so-called "beard-to-suit ratio"—and lengthier delays in reaching consensus. *See generally* Timothy Simcoe, *Standard Setting Committees: Consensus Governance for Shared Technology Platforms*, 102 AM. ECON. REV. 305 (2012).

[31] *See* Scott Bradner, IETF Working Group Guidelines and Procedures § 3.3 (IETF Network Working Grp., RFC No. 2418, 1998), http://www.ietf.org/rfc/rfc2418.txt.

[32] David D. Clark, *A Cloudy Crystal Ball: Visions of the Future*, *in* PROC. 24TH INTERNET ENG'G TASK FORCE 543 (Megan Davies et al. eds. 1992), *available at* https://www.ietf.org/proceedings/24.pdf.

[33] *See, e.g.*, A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 798-805 (2003) (examining the IETF through the lens of Habermas's discourse ethics, arguing that it satisfies the procedural conditions the generate legitimacy.).

[34] *See id*. at 755-56 (describing the Internet, a largely self-regulating system that emerged in the absence of an international legal framework, as a type of "orderly anarchy").

[35] Joseph Liu, *Legitimacy and Authority in Internet Coordination: A Domain Name Case Study*, 74 IND. L.J. 587, 588 (1999) (noting that working groups have no formal legal authority, not do the standards they produce have legally binding effects).

[36] *See* MILTON MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 217 (2010) [hereinafter MUELLER, NETWORKS AND STATES] (using the term "organically developed Internet institutions" to refer to the transnational groups of actors that took shape with the Internet outside of the nation-state system.).

order to avoid inefficiently duplicating work, creating of incompatible standards, or causing uncertainty in the marketplace.[37]

There is one SDO, however, that has somewhat of a history of encroaching on others' technical mandates while attempting to enlarge its own.[38] We are talking of course about ITU-T, the Geneva-based venue where Huawei presented its controversial New IP proposal. Although ITU-T and its standards were instrumental in enabling international interoperability among public switched telephone networks, this did not translate into a significant role within the modern Internet standards ecosystem.[39] Instead, its involvement has been mostly limited to lower-layer Internet access technologies such as Digital Subscriber Line (DSL), which uses standard telephone lines as a transmission medium, as well as the optical fiber used in carrier networks.[40]

To get a more complete picture of ITU-T, one of the three sectors of the ITU, it is helpful to know a bit of its history. The ITU was established in 1865, when twenty European countries signed a treaty intended to facilitate policy coordination and technical interoperability among the Continent's telegraph networks.[41] It then gradually expanded over the next eighty years, admitting new member states and adding new forms of telecommunications, such as radio and telephony to its remit.[42] This continued until 1947, when it became officially recognized as a specialized agency of the United Nations.[43] It now consists of 193 Member States (i.e., countries that acceded to the ITU Constitution and Convention) that are typically represented by their respective national telecommunications administrations.[44]

As an international multilateral body with roots in pre-war Europe, the ITU and its standardization sector unsurprisingly embody a much more formal, top-down style of governance than the IETF.[45] Participation in ITU-T is restricted to its members, a category which includes both Member States as well as any companies, civil society groups, or academic institutions that have

---

[37] *See* NIZAR ABDELKAF ET AL., UNDERSTANDING ICT STANDARDIZATION: PRINCIPLES AND PRACTICE 62 (2018), *available at* www.etsi.org/images/files/Education/Understanding_ICT_Standardization_LoResWeb_20190524.pdf (describing this coordination as "inherent to the spirit of standardization"). By uncertainty, we refer to situations in which the market hesitates to adopt either of two competing standards due to fears of selecting the loser and stranding one's investment. *See* CARL L. SHAPIRO & HAL R. VARIAN, INFORMATION RULES 230 (1998).

[38] The New IP proposal is far from the only example of the ITU-T entertaining possible standards work that would have overlapped with another SDO. *See, e.g.*, Stanley M. Besen & George Sadowsky, *The Economics of Internet Standards*, *in* HANDBOOK ON THE ECONOMICS OF THE INTERNET 211 (Johannes M. Bauer & Michale Latzer eds., 2017); Iljitsch van Beijnum, *ITU bellheads and IETF netheads clash over transport networks*, ARS TECHNICA (Mar. 3, 2011, 10:25 AM), https://arstechnica.com/tech-policy/2011/03/itu-bellheads-and-ietf-netheads-clash-over-mpls-tp/ ; Jorge L. Contreras, *Divergent Patterns of Engagement in Internet Standardization: Japan, Korea and China*, 38 TELECOMM. POL'Y 914, 920 (2014).

[39] *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 125 (2014).

[40] The ITU-T's limited role is not for a lack of trying. Throughout its history, the institution has been involved in multiple attempts at developing data networking standards as alternatives to TCP/IP. However, each of these failed to gain significant long-term adoption. *See infra* Part III.A.

[41] *The 1865 International Telegraph Conference*, INT'L TELECOMM. UNION (last accessed May 25, 2023), http://handle.itu.int/11.1004/020.2000/s.138.

[42] *Overview of ITU's History (3)*, INT'L TELECOMM. UNION (last accessed May 25, 2023), http://handle.itu.int/11.1004/020.2000/s.210.

[43] *Id*.

[44] Raymond & DeNardis, *supra* note 23, at 598-99.

[45] Patrick S. Ryan, *The ITU and the Internet's Titanic Moment*, 2012 STAN. TECH. L. REV. 8 ¶ 26 (2012).

been formally admitted as dues-paying "sector members."[46] However, the participation rights granted to non-state sector members come with limitations, as there are certain privileges within ITU-T enjoyed exclusively by Member States. This hierarchical membership structure is not reflected much in the day-to-day standardization work taking place within ITU-T Study Groups, but it does exclude these sector members from involvement in major internal governance decisions.[47]

Another area of sharp contrast between the IETF and ITU-T is with regards to transparency.[48] While final versions of approved ITU-T standards (called "recommendations") are made public, all other working documents are stored in an internal database accessible only to its members.[49] This effectively prevents any visibility into ongoing developments within ITU-T, making it difficult for both civil society and the general public to play an oversight role. When paired with the superior decision-making authority it grants to government actors, the behind-closed-doors nature of the ITU thus appears to be more amenable to the style of governance preferred by states like China. In fact, we need not even speculate here, as China itself has been quite vocal in its support for expanding the ITU's role within the global Internet governance system.[50]

B. International Standardization with Chinese Characteristics

Having arrived at the subject of China, it is useful to see how its own role within Internet-related SDOs and the broader ICT standard-setting environment has been evolving. Despite having boasted the world's largest number of Internet users for quite some time, the influence of Chinese actors here has historically been limited. This is largely due to China's status as a latecomer.[51] During the period when many modern ICTs and corresponding SDOs were beginning to take shape, China was still undergoing major economic reforms and lacked much of a domestic technology sector.[52] As a result, Chinese actors were forced to play catch-up with those from the U.S., EU, and Japan who had already established themselves.[53] This meant they played the part of global standards taker much more often than standards maker. Yet, over the last decade, the Chinese government—led by and inextricably entwined with the Chinese Communist Party (CCP)—has taken major steps to change that.

Much has already been written about the strategic framework China has adopted for expanding its international technical standards footprint, so we intend only to summarize it briefly

---

[46] *See* Raymond & DeNardis, *supra* note 23, at 598-99. In 2023, the standard ITU-T annual membership fee was 31,800 CHF for sector members and 3,975 CHF for academic members. *Fees*, INT'L TELECOMM. UNION (last visited Feb. 26, 2023), https://www.itu.int/en/ITU-T/membership/Pages/Categories-and-Fees.aspx.

[47] Raymond & DeNardis, *supra* note 23, at 599.

[48] Ryan, *supra* note 49, at ¶ 39 ("[T]he IETF's philosophy of access and transparency could not be more different than that of the ITU.").

[49] *Id*.

[50] *See, e.g. Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development*, KREMLIN.RU (Feb. 4, 2022) ("The sides support the internationalization of Internet governance . . . [and] are interested in greater participation of the International Telecommunication Union in addressing these issues.").

[51] *See* Lennart Schott & Kerstin J. Schaefer, *Acceptance of Chinese Latecomers' Technological Contributions in International ICT Standardization — The Role of Origin, Experience and Collaboration*, 52 RSCH. POL'Y 1-2 (2023).

[52] Contreras, *supra* note 38, at 918.

[53] *Id*.

here.[54] The strategy, whose focus is not just limited to ICT standards, has been described as comprising two tracks.[55] Each of these tracks represents a separate avenue through which Chinese-developed standards are to be proliferated.

The first track focuses on international SDOs, seeking to increase both the representation of Chinese actors and the competitiveness of their contributions. To do so, China has been known to offer financial support and incentives intended to boost engagement at prioritized SDOs.[56] This includes subsidizing participation costs (e.g., membership fees, travel, training, etc.) as well as providing monetary awards to those who submit contributions or secure leadership positions.[57] Within these SDOs, there are many reports of Chinese participants acting in a highly coordinated manner such as by voting blocs.[58] The precise mechanism for achieving this coordination is not entirely known, but most assume it involves some degree of direction from the party-state.[59]

The second track of China's strategy operates outside the conventional institutional framework for global standard-setting and instead facilitates international adoption of Chinese-developed standards through its various bilateral trade and investment relationships.[60] This approach can be characterized as a de facto standardization strategy, wherein Chinese domestic standards are elevated to global status through widespread market acceptance rather than formal recognition by an international body. Though the diffusion of Chinese standards might initially be focused on those countries with whom China has close economic linkages, the rest of the world may begin to quickly follow once the level of global adoption reaches a critical mass.[61]

---

[54] *See generally* John Seaman, *China and the New Geopolitics of Technical Standardization*, NOTES DE L'IFRI (Jan. 2020), https://www.ifri.org/en/publications/notes-de-lifri/china-and-new-geopolitics-technical-standardization; Sorina Teleanu, *The geopolitics of digital standards: China's role in standard-setting organisations*, DIPLOFOUNDATION (Dec. 2021). https://www.diplomacy.edu/resource/report-the-geopolitics-of-digital-standards-chinas-role-in-standard-setting-organisations/; Tim Rühlig, *Chinese Influence through Technical Standardization Power*, 32 J. CONTEMPORARY CHINA 54 (2023); Julia Voo & Rogier Creemers, *China's Role in Digital Standards for Emerging Technologies – Impacts on the Netherlands and Europe*, LEIDEN ASIA CENTRE (2021), https://leidenasiacentre.nl/wp-content/uploads/2021/05/Chinas-Role-in-Digital-Standards-for-Emerging-Technologies-1.pdf; Emily de la Bruyère, *Setting the Standards: Locking in China's Technological Influence*, *in* CHINA'S DIGITAL AMBITIONS: A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER 49 (Nat'l Bureau Asian Rsch., NBR Special Rep. No. 97, Emily de la Bruyère et al. eds., 2022); Daniel R. Russel & Blake H. Berger, *Stacking the Deck: China's Influence in International Technology Standards Setting*, ASIA SOC'Y POL'Y INST. (2021), https://asiasociety.org/sites/default/files/2021-11/ASPI_StacktheDeckreport_final.pdf.

[55] Seaman, *supra* note 54, at 20.

[56] Rühlig, *supra* note 54, at 66-67.

[57] de la Bruyère, *supra* note 54, at 57.

[58] de la Bruyère, *supra* note 54, at 59 (quoting one interviewed SDO participant as saying "other countries' delegates act like individuals. China's act like a group"); Russel & Berger, *supra* note 54, at 12 (stating that Chinese firms flood SDOs with large volumes of standards proposals and vote in a single bloc). *But see infra* notes 70-72 and accompanying text (finding that China's use of manipulative tactics has been overstated and that its growing success at SDOs is more attributable to improvements in standards proposal quality).

[59] Rühlig, *supra* note 54, at 67-68 (explaining that party-state's level of involvement and control makes it possible for a strategy in which Chinese actors "speak with one voice" at SDOs); de la Bruyère, *supra* note 54, at 60 (indicating that the party-state is uniquely positioned to influence how Chinese firms engage with SDOs).

[60] Seaman *supra* note 54, at 24-25; de la Bruyère, *supra* note 54, at 61.

[61] *See* SHAPIRO & VARIAN, *supra* note 37, at 13-14 (explaining that adoption of technologies subject network effects can begin to experience explosive growth once it reaches the point where demand-side economies of scale begin to kick in).

This de facto standardization track is closely related to China's Digital Silk Road (DSR), which has become a component of its larger Belt and Road Initiative.[62] The DSR seeks to enhance digital connectivity and trade between China and other partner countries through ICT infrastructure construction projects.[63] The financing for these projects, typically offered on generous terms by one of China's state-owned development banks, is conditioned on the use of Chinese-manufactured components.[64] The DSR thus helps externalize Chinese domestic ICT standards by facilitating the export of products that adhere to them.[65]

The results of China's efforts thus far have been mixed but trending upwards. Whether the expanded international market for Chinese ICTs enabled by the DSR will provide a durable source of de facto standards power still remains to be seen.[66] When looking at the global ICT standards environment in general, China's influence is still overshadowed by that of the U.S. and some other Western counterparts. However, there has been an observed increase in Chinese participation and submissions across several SDOs.[67] This participation is not just limited to venues endorsed by China, such as ITU-T, but includes those like the 3GPP, IEEE-SA, and—as we will highlight later—the IETF.[68] Further, as demonstrated by the success enjoyed by Chinese firms like Huawei during the 5G standardization process, there is mounting evidence that China's impact within these SDOs is growing.[69]

It would be a mistake to dismiss these recent successes as the product of tactics like packing SDOs with participants or flooding them with high volumes of standards proposals.[70] Quantity alone does not necessarily translate to influence within SDOs, especially since most of them utilize consensus-based decision-making.[71] Instead, there seems to be an emerging consensus that Chinese actors have made steady improvements in the quality of their contributions at ICT-related

---

[62] *See* Alex He, *The Digital Silk Road and China's Influence on Standard Setting* 2-3 (Ctr. Int'l. Governance Innovation, Paper No. 264, Apr. 2022) (providing an overview of how digital "standards connectivity" fits into the DSR initiative).

[63] Unlike most major Chinese political initiatives, the DSR is not the result of the CPC's top-down planning. Instead, it evolved out of the natural efforts of Chinese multi-national tech companies to begin expanding into relatively untapped international markets. The party-state eventually embraced this trend and began to promote it as a formal initiative under the BRI. *See* Robert Greene & Paul Triolo, *Will China Control the Global Internet Via its Digital Silk Road?*, CARNEGIE ENDOWMENT INT'L PEACE (May 08, 2020), https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857.

[64] Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 N.Y.U. J. INT'L L. & POL. 1, 53 (2021).

[65] *Id*. at 45.

[66] *See* Telanu, *supra* note 54, at 63.

[67] *See* Telanu, *supra* note 54, at 63 (summarizing the report's analysis of trends in Chinese engagement at ICT SDOs).

[68] *See id*.; *see also infra* Part V.B (discussing Chinese actors' increasing engagement at the IETF).

[69] *See* Voo & Creemers, supra note 54, at 11-13.

[70] Matt Sheehan & Jacob Feldgoise, *What Washington Gets Wrong About China and Technical Standards*, CARNEGIE ENDOWMENT INT'L PEACE (Feb. 27, 2023), https://carnegieendowment.org/2023/02/27/what-washington-gets-wrong-about-china-and-technical-standards-pub-89110 (finding that the general belief among the peers of Chinese SDO participants is that manipulative tactics are the exception rather than the rule).

[71] Giulia Neaher et al., *How Can the United States Navigate the Geopolitics of International Technology Standards?*, ATL. COUNCIL 16 (Oct. 2021), https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Standardizing-the-future-How-can-the-United-States-navigate-the-geopolitics-of-international-technology-standards.pdf; Naomi Wilson, *China Standards 2035 and the Plan for World Domination—Don't Believe China's Hype*, COUNCIL FOREIGN RELS. (June 3, 2020) https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype.

SDOs.[72] The competitiveness of Chinese standards contributions has also benefited—even if indirectly—from China's large investments into developing national technical expertise and innovation capacity in areas it deems strategically important.[73] Since standards influence remains a major priority for the CCP, such progress should only be expected to continue.

C. China's Alternative Vision for Cyberspace

As China has turned its strategic focus towards the development global technical standards and provided an increasingly formidable source of competition for Western participants, the perception of standards bodies as a type of political battlegrounds has become more common. However, this is unlikely to be much of a revelation to those who have long studied the field. There is a vast body of literature, spanning several decades and different academic disciplines, examining the political nature of technical standards and standardization. To summarize it in just a few words, protocols are political.[74]

The Internet standard-setting process brings together a diverse collection of actors with disparate goals and interests. There is often a tremendous amount at stake in the outcome, as decisions here can tilt entire markets in a company's favor and/or have consequences in the form of millions of dollars.[75] At a more macro level, standards power can promote domestic industries and bolster national prestige by signaling a country's technological prowess.[76] The standards arena thus serves as a site of mediation among these many competing interests, where the different stakeholders vying for influence must engage in a series of tradeoffs and compromises over choices that have the potential to shift the balance of economic power. [77] In this sense, the process is political.[78]

Yet, there is a different way in which Internet standard-setting might be understood as political, one that resonates more with the dominant narrative of China's standards ambitions. Beyond the economic interests at stake, the standards process often involves choices over the

[72] Rühlig, *supra* note 54, at 60 (reporting that most interviewed SDO participants acknowledged an improvement in the quality of Chinese proposed standards); Teleanu, *supra* note 54, at 41 (noting there has been an observed increase in the quality of Chinese proposals over time as resources have been allocated to training); Riccardo Nanni, *Digital Sovereignty and Internet Standards: Normative Implications of Public-Private Relations Among Chinese Stakeholders in the Internet Engineering Task Force*, 16 INFO., COMM. & SOC'Y 2342, 2355 (2022) (finding that interviewed IETF participants generally agreed that Chinese actors have grown more effective within the IETF as they have gained experience).

[73] *See* Voo & Creemers, supra note 54, at 7; Rühlig, *supra* note 54, at 66.

[74] LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE 71 (2009) [hereinafter DENARDIS PROTOCOL POLITICS]; *see also* JANET ABBATE, INVENTING THE INTERNET (1999) ("The debate over network protocols illustrates how standards can be politics by other means"); SHAPIRO & VARIAN, *supra* note 37, at 13 (describing the formal standard-setting process as a "wild mix of politics and economics"); LAWRENCE LESSIG, CODE VERSION 2.0 78 (2006) [hereinafter LESSIG, CODE 2.0].

[75] *See* Froomkin, *supra* note 33, at 795 ("Decisions regarding standards now have important financial consequences for would-be providers of Internet hardware and software, and tempers can flare when tens of millions of dollars are at stake").

[76] *See* ABBATE, *supra* note 74, at 147-48.

[77] *See* SHAPIRO & VARIAN, *supra* note 37, at 240 (describing the "logrolling" that can take place in formal standardization venues.); *see also* Colin J. Kiernan & Milton L. Mueller, *Standardizing Security: Surveillance, Human Rights, and the Battle Over TLS 1.3*, 11 J. INFO. POL'Y 4 (2021) (offering the term "political economy of standardization" to capture the political nature of this process more accurately).

[78] Kiernan & Mueller, *supra* note 77, at 4.

values that should inform and be prioritized in the design of a protocol.[79] Not only does a protocol reflect these normative choices made by its designers, but the values embedded in its design can have important implications for civil liberties (e.g., privacy, free expression) as well as the distribution of power and authority in society.[80] Similarly, as legal scholars such as Lawrence Lessig and Joel Reidenberg observed over two decades ago, the technical design and implementation of the Internet's architecture is capable of serving a regulatory function that supplements or even supplants law in cyberspace.[81] A logical extension of this metaphor is that those who control the development of protocol standards—the common blueprints for implementing different parts of the Internet's architecture—assume the role of lawmakers.[82] Hence, the competition over influencing Internet standards might be framed as a struggle over a private, transnational regulatory power and the values that should guide its use.[83]

According to the prevailing narrative, the impetus behind China's growing presence in the global standards arena is the goal of contesting the Western liberal values.[84] In their place, China intends to install a set of norms and values that reflects it competing vision for the global Internet, the alternative it offers to the "free and open" version historically championed by the United States. At the center of this vision is a new guiding principle for governing and building order in international cyberspace, a concept China refers to as cyber sovereignty (*wangluo zhuquan*).[85]

The starting point for any discussion of Chinese cyber sovereignty should be to recognize that China's own articulation of the concept, found across various policy documents and speeches by Party officials, has been vague and even logically inconsistent at times.[86] China has insistently

---

[79] *See* Mulligan & Bamberger, *supra* note 17, at 707 (explaining that decisions in the design process have become sites for resolving value disputes).

[80] DENARDIS PROTOCOL POLITICS, *supra* note 74, at 71; Ian Brown, David D. Clark & Dirk Trossen, *Should Specific Values Be Embedded in the Internet Architecture?*, PROC. RE-ARCHITECTING INTERNET WORKSHOP, art. no. 10 (2010). It should be noted that this claim about protocols, embedded values, and their social impact is not uncontested. Milton Mueller and Farzaneh Badiei direct several challenges at this notion, pointing out both the voluntary nature of protocol adoption and the difficulty of knowing *a priori* how a given design choice will impact a set of values once introduced into a complex real-world setting. *See generally* Milton Mueller & Farzaneh Badiei, *Requiem for a Dream: On Advancing Human Rights via Internet Architecture*, 11 POL'Y & INTERNET 61-83 (2019). Even those who generally accept the premise nonetheless acknowledge that translating values into technical designs that uphold or enforce those values is not always straightforward, often leading to unforeseen or unintended consequences. *See* Helen Nissenbaum, *From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?*, 26 BERKELEY TECH. L.J. 1367, 1370 (2011); Mulligan & Bamberger, *supra* note 17, at 710.

[81] Reidenberg, *supra* note 17, at 568 ("Rules established in this fashion form a legal regulatory regime. In the context of information flows on networks, the technical solutions begin to illustrate that network technology itself imposes rules for the access to and use of information."); LESSIG, CODE, *supra* note 17, at 89 ("The code or software or architecture or protocols . . . constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation . . . .").

[82] LESSIG, CODE, *supra* note 17, at 60; Mulligan & Bamberger, *supra* note 17, at 713.

[83] *See* LESSIG, CODE, *supra* note 17, at 60 ("How the code regulates, who the code writers are, and who controls the code writers . . . reveal how cyberspace is regulated."); DENARDIS PROTOCOL POLITICS, *supra* note 74, at 91 (analogizing power over standards to the ability to enact public policy that directly impacts individuals who use a technology).

[84] *See supra* notes 10-12 and accompanying text.

[85] This term is often translated as Internet sovereignty or network sovereignty.

[86] *See* Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 107 (Dennis Broeders & Bibi van den Berg eds., 2020) [hereinafter Creemers, China's Conception of Cyber Sovereignty](noting official documents tend to define cyber-

characterized cyber sovereignty as the natural extension of national sovereignty—a "basic norm in contemporary international relations"—into the domain of cyberspace.[87] Yet, these explanations offer little in the way of clarification, as the principle of sovereignty itself frequently takes on different meanings and is invoked by states to advance a wide range of political objectives.[88] Multiple commentators who have undertaken the task of deciphering China's conception of cyber sovereignty have instead observed that it consists of at least three separate dimensions: a national security dimension, a domestic governance dimension, and international governance dimension.[89]

The national defense dimension implicitly links cyber sovereignty to territorial integrity, a widely accepted norm derived from the principle of sovereignty under international law.[90] From this perspective, respect for cyber sovereignty as a primary rule of international law would prohibit a state from promoting, supporting, or condoning cyber-activities that harm ICT infrastructure located within another state's territorial borders.[91] This dimension is thus consistent with the way cyber sovereignty has been frequently discussed in the American legal-academic context over the last decade, where the discourse has concentrated on how sovereignty and derivative norms should apply to cyber-conflict and state conduct in cyberspace.[92] However, China has tended to emphasize this dimension far less than the others, perhaps understandably given the history of Chinese state-sponsored extraterritorial cyber-operations.[93]

China's conception of cyber sovereignty is much more concerned with ideological security than it is with the security of cyber-infrastructure residing within its territory.[94] Beijing sees the West's idealization of an open, borderless global Internet that permits the unimpeded flow of

---

sovereignty in broad, vague terms); Katharin Tai & Yuan Yi Zhu, *A Historical Explanation of Chinese Cyber-Sovereignty*, 22 INT'L RELS. ASIA-PAC. 469, 484-86 (2022) (arguing that cyber sovereignty's "seeming lack of coherence" is due to its origin as a domestic propaganda device rather than part of a clear, comprehensive vision.).

[87] *International Strategy of Cooperation on Cyberspace*, MINISTRY FOREIGN AFFS. PEOPLE'S REPUBLIC CHINA (Mar. 01, 2017) [hereinafter International Strategy of Cooperation] (describing cyberspace as a "new domain of state sovereignty"); *Full Text: Jointly Build a Community with a Shared Future in Cyberspace*, CHINA DAILY § IV (Nov. 2022), https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html [hereinafter SCIO, Shared Future in Cyberspace] (reprinting white paper issued by the China's State Council Information Office) ("China advocates . . . that a just and rational international order in cyberspace be built on the basis of national sovereignty.").

[88] *See* Henning Lahmann, *On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace*, 32 DUKE J. COMP. & INTL. L. 61, 91 (2021); HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION ¶ 62 (2019), *available at* https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

[89] Sarah McKune & Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMM. 3835, 3837 (2018); *see also* Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 403 (2020) (presenting a similar yet slightly modified tri-dimensional framework).

[90] International Strategy of Cooperation, *supra* note 87 (asserting that states "exercise jurisdiction over ICT infrastructure, resources and activities within their territories" and have the right to protect them from "from threat, disruption, attack and destruction"); *see also* Anupam Chander & Haochen Sun, *Sovereignty 2.0*, 55 VAND. J. TRANSNAT'L L. 283, 294 (2022) (noting the emphasis on territoriality appears to be a nod to international law).

[91] Xi Jinping, President of the People's Republic of China, Remarks at the Opening Ceremony of the Second World Internet Conference (Dec. 16, 2015), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml [hereinafter Xi WIC speech] (stating that no country should "connive at or support cyber activities that undermine other countries' national security.").

[92] *See generally* Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT'L L.J. 275 (2014); Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639 (2017); Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207 (2017).

[93] *See* Lahmann, *supra* note 88, at 80-81.

[94] *See id. at 82*; Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 86, at 130.

information as a threat to domestic stability and Party rule.[95] As a direct response, the second dimension of Chinese cyber sovereignty—the domestic governance dimension—asserts that all sovereign states have the right to choose their own "path of cyber development, model of cyber regulation, and Internet public policies" without foreign interference.[96] If a country wants to restrict certain information flows or pursue technological independence in the name of security, it should be able to do so without being undermined from the outside (e.g., by foreign states providing locals with circumvention tools).[97]

Having been described as a "cyber-Westphalia,"[98] China thus envisions a global cyberspace where states have exclusive control over deciding how Internet infrastructure and activities within their territories are regulated.[99] To lend legitimacy to this interpretation of cyber sovereignty, China again appeals to widely accepted international legal principles, this time those of non-intervention and self-determination. Yet, as many have noted, the widespread acceptance of these principles has never been invitation for states to disregard other international legal commitments, namely the rights to free expression and access to information enshrined in international human rights law.[100] This is what China is ostensibly trying to justify when it asserts cyber sovereignty.[101]

The use of cyber sovereignty as a pretext for censorship and other forms of Internet control is why China's global promotion of the principle has many alarmed. When concerns are raised over China's purported strategy to re-organize the global Internet around cyber sovereignty, it is this second dimension that is typically being referenced. Understood this way, modifying the Internet's technical architecture to better align with cyber sovereignty would seem to entail equipping networks with features that provide states the option to exert greater control over information flows or to identify users so they can be held accountable for violations of domestic law. In other words, it would involve the development of a new Internet architecture that, by default, is more regulable.

Finally, China's conception of cyber sovereignty also has an international governance dimension. Citing the principle of sovereign equality enshrined in the U.N. Charter, China maintains that all countries have the right to participate on equal footing in the governance of the

---

[95] Wang, *supra* note 89, at 406.

[96] International Strategy of Cooperation, *supra* note 87; *see also* Adam Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*, *in* AN EMERGING CHINA-CENTRIC ORDER: CHINA'S VISION FOR A NEW WORLD ORDER IN PRACTICE (Nat'l Bureau Asian Rsch., NBR Special Rep. No. 87, Nadège Rolland ed., 2020) (interpreting Chinese cyber-sovereignty as a pushback against the West's insistence on the universality of values like free expression, access to information, and privacy from the state.); Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 86, at 129 (recognizing the concept's defensive, reactive nature).

[97] A 2010 speech by then Secretary of State Hillary Clinton's, in which she admonished China for its Internet censorship and reaffirmed the U.S.'s commitment to empowering foreign citizens with the tools for bypassing it, is often recognized as a catalyst behind China increasingly assertive stance on cyber sovereignty. *See* Tai & Zhu, *supra* note 86, at 490. Segal, *supra* note 96, at 91; Goldsmith, *supra* note 15, at 4-6.

[98] *See, e.g.*, Chris C. Demchak, *Uncivil and Post-Modern Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age*, 1 CYBER DEF. REV. 49, 55-64 (2016).

[99] *See, e.g.*, Lahmann, *supra* note 88, at 77.

[100] *See id*. at 106; McKune & Ahmed, *supra* note 89, at 3849.

[101] *See* Tai & Zhu *supra* note 86, at 491-92 (illustrating how China will invoke cyber sovereignty as a reaction to those provoking the tension between its system and human rights, the latter of which it believes are subordinate to national sovereignty).

Internet and global cyberspace.[102] It has stated that no state should pursue or maintain "cyber-hegemony" and that decisions in this sphere "should not be made with one party calling the shots."[103] As suggested by these subtle jabs at a particular unnamed country, this dimension was heavily influenced by China's discontentment with how the existing system of Internet governance privileges the United States and reflects its preferences for a multistakeholder, limited-government model.[104] Although the alternative China offers to this system would allow industry and civil society to participate in consultative role, it would—for all intents and purposes—represent a much more state-centric form of governance.[105]

Equally notable is the rhetorical move China makes when promoting this international governance dimension of cyber sovereignty. Here, it characterizes cyberspace as a shared, global commons for which all countries bear the responsibility of preserving together.[106] On its face, this depiction of cyberspace appears to directly contradict the highly territorialized version it uses to justify its Internet control regime.[107] Although the contradiction could theoretically be reconciled by introducing a principle that clearly demarcates common cyberspace from national cyberspace, there has yet to be a serious attempt at doing so. Some have argued that contradictions like these are why China has struggled thus far to gain international acceptance for its interpretation of cyber sovereignty.[108] However, this early lack of success has certainly not stopped it from continuing to try.

II. WHAT WAS NEW IP?

The New IP proposal involved several elements that caused it to attract an unusual amount of attention: an emerging global superpower, its controversial national tech champion, potential implications for civil liberties, and at the center of it all, alterations to a revolutionary technology that has woven itself into the fabric of everyday life. Given what was potentially at stake, it should come as no surprise that along with this attention, the proposal attracted a great deal of speculation. Yet, if we are to draw any valuable conclusions about New IP, its purpose, and what it spells for the future direction of the global Internet, it is necessary to first separate hype from reality.

In this section, we offer a clearer, more precise picture of what was being proposed using internal ITU-T documents along with other Huawei-authored research and SDO contributions.

---

[102] Shared Future in Cyberspace, *supa* note 87, § III.3 ("It has been China's consistent view that all countries, big or small, strong or weak, rich or poor, are equal members of the international community and are entitled to equal participation in developing a global order and international rules, to ensure that the future development of cyberspace is decided by people of the world").

[103] Xi WIC speech, *supra* note 91.

[104] *See* Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 86, at 130; Wang, *supra* note 89, at 44-46.

[105] *See* Xi WIC speech, *supra* note 91 (describing China's envisioned governance model as a "multilateral approach with multi-party participation").

[106] *Id*. ("The Internet is the common home of mankind. Making it better, cleaner and safer is the common responsibility of the international community."); International Strategy of Cooperation, *supra* note 87 ("Cyberspace is the common space of activities for mankind, hence needs to be built and managed by all countries.").

[107] *See, e.g.*, *The Internet in China*, STATE COUNCIL INFO. OFF. § VI (June 8, 2010), http://www.china.org.cn/government/whitepaper/node_7093508.htm [hereinafter Internet in China whitepaper] ("Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. . . . [L]egal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China . . .").

[108] *See, e.g.*, McKune & Ahmed, *supra* note 89, at 3846-50 (highlighting contradictions of the Internet sovereignty promoted by China and explaining how this has served as a barrier to gaining international acceptance).

Despite some reports to the contrary, nothing contained in the New IP proposals approximated an actual technical standard, at least not the type capable of being adopted and implemented.[109] The proposals instead sought to initiate preliminary, high-level planning activities for the future protocols. Thus, our goal here is not to make predictions about what New IP would have looked like in its final form, as it is impossible to predict how the full process would have played out. However, the high-level solutions and underlying technical justifications contained in the proposal materials still provide valuable insights into the problems New IP is attempting to solve as Huawei understands them. This, in turn, sheds light on what Huawei and China might hope to accomplish. The remainder of this section will examine the three main functional features advanced by the proposal.

A. Better-than-Best Effort Service

Transmission of data packets over the IP-based public Internet typically occurs on a "best effort" basis. This means the network provides neither a guarantee that traffic will reach its destination within a certain amount of time, nor that it will get there at all. A data packet traveling over the public Internet typically passes through several intermediate routers, each one of which decides where to forward the packet next based on the destination address specified in its header.[110] When a packet arrives at an intermediate router, it is placed in a queue where it typically waits until all the packets arriving earlier have been processed and forwarded. Under the best effort delivery model, packets in a router queue are effectively treated equally, meaning no packet is given special priority.[111] Longer queues translate to longer waiting times, and when a queue becomes too long, the router may be forced to beginning dropping excess packets. Thus, when the network load increases, it is not unusual to experience higher levels of packet loss, delay (latency), and delay variation (jitter).

This best effort service model has worked well for traditional applications like email, while modern applications like real-time video have also managed to adapt. However, Huawei argues that best effort service will be inadequate to meet the needs of many future network use cases that have uniquely high sensitivity to different quality of service (QoS) dimensions like latency, jitter, and packet loss.[112] Such use cases include telemedicine operations (i.e., remote surgeries), autonomous vehicle traffic management, and most prominently, the industrial Internet.[113] Consider an industrial automation scenario where machinery is remotely monitored and controlled in real time through Internet-connected sensor and actuator devices, a use case that routinely appears in

[109] *See, e.g.*, Madhumita Murgia & Anna Gross, *Inside China's controversial mission to reinvent the internet*, FT MAG. (Mar. 27, 2020) (suggesting that ITU participants would decide whether to adopt New IP at the 2020 World Telecommunications Standardization Assembly).

[110] *See generally What is routing?*, CLOUDFLARE (last visited Feb. 19, 2023), https://www.cloudflare.com/learning/network-layer/what-is-routing/.

[111] LARRY L. PETERSON & BRUCE S. DAVIE, COMPUTER NETWORKS: A SYSTEMS APPROACH 492-94 (5th ed. 2012) (providing an overview of the first-in, first-out queuing associated with best effort delivery).

[112] Richard Li et al., *New IP: A Data Packet Framework to Evolve the Internet*, *in* 2020 IEEE 21ST INT'L CONF. ON HIGH PERFORMANCE SWITCHING & ROUTING (HSPR) 3 (Conference 2020), https://doi.org/10.1109/HPSR48589.2020.9098996 [hereinafter Li et al., *New IP Data Packet Framework*].

[113] *See, e.g.*, *id.* at 8; Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Tutorial on C83 - New IP: Shaping the Future Network*, TSAG-TD598/GEN at 7 (Sept. 2019), https://www.itu.int/md/T17-TSAG-190923-TD-GEN-0598 [hereinafter TSAG Tutorial].

New IP documents.[114] Here, the consequences of packet loss or severe latency could be costly, leading to disruptions in the manufacturing process, product defects, or damage to machinery. Hence, one of the proposed requirements for New IP is the ability to achieve deterministic QoS—end-to-end transmission of data flows with guaranteed maximum/minimum levels of reliability, latency, and/or jitter—over large-scale networks.[115]

Huawei is far from the first one to take an interest in these capabilities, as efforts to enable differentiated QoS in packet switched networks have been taking place for well over three decades. The IETF has undertaken two major initiatives aimed at defining new QoS models as alternatives to best effort delivery. The first attempt came in the form of Integrated Services (*IntServ*), which was initiated in 1994.[116] *IntServ* enables users/applications to reserve the necessary resources (i.e., bandwidth) from each router along a network path in order guarantee that subsequent packets in a flow receive a particular level of service. *IntServ* was followed by Differentiated Services (*DiffServ*), first proposed in 1998.[117] *DiffServ* involves categorizing network traffic into different pre-defined classes which can be specified in an IP packet header field. A *DiffServ*-enabled router uses this information to determine how to prioritize traffic (something called a per-hop-behavior or PHB), giving preferential treatment to high-priority classes while giving lower-priority ones traditional best effort service.

As suggested by the fact that this QoS discussion is still occurring several decades later, neither of the solutions above have succeeded in gaining significant traction, at least on an Internet-wide scale.[118] Indeed, each of them has proven to face various technical limitations, many of which Huawei notes in its justification for New IP. *IntServ*, for instance, involves complex signaling between endpoints and routers, including the initial setup which itself can contribute to delay.[119] It also requires routers to store and continuously process information about each active flow it has reserved resources for, something that can add significant overhead in large networks and thus limiting its scalability. *DiffServ*, on the other hand, avoids most of these limitations but comes with a major downside in that it cannot provide strict end-to-end QoS guarantees.[120] It offers only to

---

[114] *See, e.g.*, *id.* at 7; Richard Li, Chief Scientist, Huawei R&D, New IP and Market Opportunities, Keynote Address at the IEEE International Conference on High Performance Switching and Routing (HSPR) 8 (May 12, 2020), https://hpsr2020.ieee-hpsr.org/wp-content/uploads/sites/118/2020/05/Richard-HPSR-2020-v1.0.pdf [hereinafter Li, *Market Opportunities*].

[115] This "large-scale networks" part is important because it is how Huawei distinguishes what it is proposes from similar ongoing work at other SDOs, such as the IEEE's Time Sensitive Networking and IETF's Deterministic Networking working groups. *See* Richard Li, *Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T,"* INTERNET EVOLUTION (June 2, 2020), https://internet4future.wordpress.com/; Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], Proposal of text amendments to the Terms of Reference of the proposed new Question F (Q.F) for the next study period of SG13, SG13-C994 2 (July. 2020), https://www.itu.int/md/T17-SG13-C-0994.

[116] *See generally* Robert Braden et al., Integrated Services in the Internet Architecture: an Overview (IETF Network Working Grp., RFC No. 1633, 1994), http://www.ietf.org/rfc/rfc1633.txt.

[117] *See generally* Steven Blake et al., An Architecture for Differentiated Services (IETF Network Working Grp., RFC No. 2475, 1998), http://www.ietf.org/rfc/rfc2475.txt.

[118] kc claffy & David D. Clark, *Adding Enhanced Services to the Internet*, 6 J. INFO. POL'Y (2016); Geoff Huston, *The elusive nature of QoS in the Internet*, APNIC (Sept. 30, 2021), https://blog.apnic.net/2021/09/30/the-elusive-nature-of-qos-in-the-internet/.

[119] *See* PETERSON & DAVIE, *supra* note 111, at 548-49 (explaining the scalability issues of IntServ); Lijun Dong & Lin Han, *New IP Enabled In-Band Signaling for Accurate Latency Guarantee Service*, *in* 2021 IEEE WIRELESS COMM. & NETWORKING CONF 1 (2021), https://doi.org/10.1109/WCNC49053.2021.9417598 (identifying poor scalability, large overhead, and difficult implementation as main limitations of IntServ).

[120] *See* Dong & Han, *supra* note 119, at 2 (citing the raw granularity of traffic class-based differentiation, which prevents precise end-to-end guarantees, as main limitation of *DiffServ*).

prioritize traffic based on broadly defined classes, which increases the probability that packet will arrive within a certain amount of time rather than provide deterministic guarantees, and the way both classification and prioritization are implemented in different networks often varies considerably.

Despite the aforementioned technical limitations, many maintain that economic and business-related obstacles have played a larger role in the failure of these solutions to achieve widespread implementation across the public Internet.[121] From this perspective, providing end-to-end QoS guarantees in a multi-operator network environment is more of a coordination problem than an engineering one. Although it is not uncommon for ISPs and large enterprises to use *DiffServ* for prioritizing certain types of traffic within the confines their own networks, end-to-end QoS on an inter-network level requires significant coordination between operators.[122] Negotiating service level agreements and pricing arrangements, already obstacles in their own right, can also entail providing other competing ISPs with greater visibility into one's internal network operations, creating further disincentives to such coordination.[123]

The New IP proposals, on the other hand, make it clear that Huawei sees this primarily as a technical problem rather than a coordination one. The general solution it outlines in various proposal documents and research papers revolves around the idea of altering the IP packet structure to include a "contract," which would be located between the header and payload.[124] The contract would be able to carry in-band signaling information for the setup of resource reservations along a network path as well as richer semantics (aka "contract clauses") for the specification of more granular QoS requirements and PHBs.[125] In simpler terms, Huawei believes the longstanding QoS problem can be overcome with a new model that combines *IntServ*'s fine-grained end-to-end guarantees but with *DiffServ*'s scalability and lack of complicated out-of-band signaling. Yet, none of what is contemplated here would obviate the need for coordination between operators in order to enable these capabilities at the inter-network level. It is possible, perhaps even likely, that all this would do is equip networks with yet another set of tools for providing differentiated QoS that go largely unused in practice. Thus, despite taking aim at a legitimate problem the technical

---

[121] *See* claffy & Clark, *supra* note 118, at 227-32 (arguing economic obstacles to widespread QoS implementation have proven to be larger than the technical ones); Hascall Sharp & Olaf Kolkman, *An Analysis of the "New IP" Proposal to the ITU-T* 6-7 (Internet Soc'y, Discussion Paper, 2020), https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/ (arguing business and regulatory problems involved in inter-domain deterministic networking will not be solved by a new protocol system).

[122] claffy & Clark, *supra* note 118, at 229 ("[T]he QoS technology developed by the IETF was in use in many IP-based enterprise networks, for example, corporate intranets"); Christopher S. Yoo, *Network Neutrality and the Need for a Technological Turn in Internet Scholarship*, in HANDBOOK OF MEDIA LAW AND POLICY: A SOCIO-LEGAL EXPLORATION 539, 543–44 (Monroe E. Price & Stefaan G. Verhulst eds., Routledge 2012) (explaining that operators like Comcast and AT&T use *DiffServ* to prioritize delay-sensitive traffic within their internal networks).

[123] *See* claffy & Clark, *supra* note 118, at 230-32.

[124] *See* Richard Li, Chief Scientist, Huawei R&D, Network 2030 and New IP, Keynote Address at the 2019 15th International Conference on Network and Service Management (CNSM) 23, 25 (Oct. 23, 2019), http://www.cnsm-conf.org/2019/files/slides-Richard.pdf [hereinafter Li, *Network 2030 and New IP*] (providing a high-level visual depiction of the New IP packet structure and describing the capabilities of its "contract spec").

[125] Lijun Dong & Lin Han, *New IP Enabled In-Band Signaling for Accurate Latency Guarantee Service* (IEEE WCNC 2021), https://ieeexplore.ieee.org/document/9417598 ("A contract clause describes how the routers treat the packet as it traverses the network based on the predefined triggering event and condition."); Lin Han et al., *A Framework for Bandwidth and Latency Guaranteed Service in New IP Network*, *in* IEEE INFOCOM 2020 – IEEE CONF. ON COMPUTER COMM. WORKSHOPS (INFOCOM WKSHPS) 85 (2020),https://ieeexplore.ieee.org/document/9162747.

community has long struggled to solve, questions remain about the potential effectiveness of Huawei's general approach.

B. Intrinsic Security

The most controversial part of the New IP proposal relates to its so-called "intrinsic security" features. Were it not for this component, which included the now notorious "shut up command," it is possible Huawei's proposal receives little outside attention.[126] However, this part of New IP is also the most difficult to appraise, as unlike many of the other proposed features, intrinsic security cannot be traced back to a large body of research published by New IP contributors. It is also notably absent from several of Huawei's New IP presentations outside the ITU.[127] Fortunately, months after Huawei's original presentation to ITU-T, it followed up with a new contribution that provided a slightly more detailed look at New IP's "Intrinsic Security Framework."[128] Here, it claims that security was an oversight in the design of the TCP/IP Internet and that the subsequent patchwork of solutions are no substitute for an Internet architecture with security embedded into its design from the beginning.[129] Huawei identifies the Internet's primary security weakness as the inability to verify the authenticity of a packet's source. It argues that the ability to hide or misrepresent the origin of network traffic through methods like IP spoofing can be used to help carry out DDoS and Man-in-the-Middle attacks as well as to evade accountability for harm and illegal acts online.[130]

In response, proposal documents depict a high-level architecture for verifying source address authenticity and enabling "privacy-preserving" user accountability.[131] Routers within the originating network domain would check that the source identifier included in a packet's header is legitimate and then add a cryptographically verifiable authentication code, which routers in the destination domain would then use to determine the packet's authenticity and integrity.[132] Packets whose source cannot be authenticated are then filtered out by routers in the destination domain, frustrating one's ability to spoof an IP address or other identifier. As an additional layer of protection against abnormally large volumes of authenticated traffic making it through the filters, the architecture specifies a feature whereby the destination domain could send a request to an "accountability agent" running in the source domain to cut off the responsible party.[133] This is the source of the widely-reported "shut up command" or "kill-switch," although the feature's purported justification is to prevent and mitigate DDoS attacks.[134] Finally, a separate encrypted value, partially derived from an alpha-numeric identifier tied to an Internet subscriber's real identity, would be included in the packet header and verified by internal routers before leaving the source domain.[135] This would theoretically enable the traceback of illegal or malicious traffic to a

[126] *See supra* note 3 and accompanying text.

[127] *See generally, e.g.*, *id*; Li, *Market Opportunities*, *supra* note 114 (containing no references to New IP's intrinsic security features).

[128] Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Overview New IP Networking & Intrinsic Security Framework*, SG17-C788 (Mar. 03, 2020), https://www.itu.int/md/T17-SG17-C-0788 [hereinafter SG17-C788].

[129] *Id*. at 14.

[130] *Id*. at 8.

[131] *Id*. at 15.

[132] *Id*. at 16.

[133] *Id*. at 22-24.

[134] *Id*.

[135] *Id*. at 18-19.

particular individual, although the assistance of the source network operator would be necessary in order to reveal the subscriber information linked to a given identifier.

The intrinsic security architecture shown in the proposal does raise legitimate concerns. The shutoff feature is ripe for abuse, as it is conceivable that spurious requests to silence a host on a different network are sent for purposes like censorship rather than terminating a DDoS attack.[136] The embedding of traceable identifiers into the packet header is also problematic, although the concerns raised here should be prefaced by reiterating that these identifiers would be encrypted using a symmetric key possessed only by the network operator. The ciphertext would also change on a per-flow basis to prevent third parties from being able to correlate all of an individual's network activities.[137] Regardless, the simple possibility of tracing traffic back to an individual person comes at the cost of reducing anonymity while likely having only limited effectiveness in deterring malicious actors.[138] This is because a large share of modern cyberattacks are carried out through compromised hosts (e.g., as part of a botnet), meaning the individuals to whom the attacks are directly traceable are not actually responsible.[139]

Simultaneously, there are doubts over just how "intrinsic" these security features are to New IP.[140] The architecture depicted in Huawei's proposal bears a close resemblance to a technology developed in China over a decade earlier called the Source Address Validation Architecture (SAVA).[141] Designed around IPv6, SAVA is also capable of verifying the authenticity of the source IP address and filtering network packets at both the inter and intra-domain level.[142] An enhanced version of this architecture (called Source Address Validation Improvements or SAVI) was successfully implemented on CNGI-CERNET2, the IPv6-only backbone network constructed as part of the "China Next Generation Internet" initiative that began in 2003.[143] The proposed intrinsic security features thus appear to be largely independent of the underlying network architecture, as there is no obvious reason why most of these same capabilities could not be implemented on existing IPv6 networks.[144]

---

[136] The proposal documents do not indicate whether granting these shutoff requests would be left to the discretion the network operator or is instead carried out through some automated process.

[137] *See* SG17-C788, *supra* note 128, at 18-19.

[138] *See* David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 323, 325 (Mar. 2011) (arguing that redesigning the Internet so that all actions can be attributed to an individual person would not help deter sophisticated cyberattacks, though it would raise issues related to privacy and freedom of expression).

[139] *See id.* at 334-35 (explaining that many attacks are now multi-stage in nature, meaning the owner of a host to which an attack can be directly traced is not actually the attack's source, but instead a victim).

[140] *See* Sharp & Kolkman, *supra* note 121, at 7.

[141] SAVA was developed by researchers from Tsinghua University as part of the state-funded "Research of Future Internet Architecture" project in the early 2000s. *See generally* Jianping Wu et al., *Theoretical Research Progress in New-Generation Internet Architecture*, SCI. CHINA SER. F-INF. SCI. 1634 (Oct. 2008), https://link.springer.com/article/10.1007/s11432-008-0160-8.

[142] *See* Ying Liu et al., *Recent Progress in the Study of the Next Generation Internet in China*, 371 PHIL. TRANSACTIONS ROYAL SOC'Y A 20120387, at 13-16 (Mar. 2013), https://doi.org/10.1098/rsta.2012.0387.

[143] *See* Jianping Wu et al., *CNGI-CERNET2: An IPv6 Deployment in China*, 41 ACM SIGCOMM COMPUTER COM. REV. 48, 50 (2011) (detailing the implementation of SAVA/SAVI on CERNET2); The success of the SAVA/SAVI deployment was even touted in the seminal *Internet in China* whitepaper released by the State Council in 2010. *See* Internet in China whitepaper, *supra* note 107, § 1 (identifying "true IPv6 source address validation" as one of the technologies successfully implemented on "the world largest IPv6 demonstration network.").

[144] Huawei researchers seemed to admit as much when they published a research paper months later containing an architecture nearly identical to the "Intrinsic Security Framework" but oriented around IPv6 instead of New IP. *See generally* Weiyu Jiang et al., *Security-Oriented Network Architecture*, SEC. & COMM. NETWORKS, May 2021, https://doi.org/10.1155/2021/6694650.

C. Flexible Addressing for the Connection of "ManyNets"

The simplest way to describe the Internet is as "a network of networks," a diverse collection of smaller independently operated networks called autonomous systems that are interconnected via a common protocol (IP) that was designed to prioritize universal connectivity. Yet, Huawei observes that the global network environment is becoming increasingly heterogenous as different network types emerge, such as those connecting new non-traditional devices and/or consisting of more dynamic topologies.[145] It characterizes this trend as a shift from "OneNet" to "ManyNets" and expects it to continue in the future as novel use cases with unique technical demands arise.[146]

Despite IP's emphasis on global connectivity, Huawei contends that the way devices are attached to and identified on the existing IP-based Internet will no longer be sufficient to accommodate the "ManyNets" of the future.[147] It identifies two primary limitations. The first is the fixed-length of existing IP addresses, as Huawei holds that IPv6's one-size-fits-all 128-bit addresses create challenges for smaller, less expensive devices with limited memory and processing power.[148] It highlights industrial networks comprised of interconnected low-power devices—part of the Industrial IoT (IIoT)—as an emerging use case for which fixed 128-bit addresses unnecessarily contribute to increased packet overhead and reduced transmission efficiency.[149] The other limitation is that existing IP addresses were originally designed to identify physical devices attached to the network at a fixed location, an assumption that most routing protocols have been built around.[150] Huawei argues this precludes optimal routing in a growing number of scenarios where, for example, the intended destination is not a specific host device but rather a service, person, or piece of content.[151] It also emphasizes the challenges this presents for networks comprised of several moving parts, namely integrated ground/satellite networks.[152]

If these limitations are not addressed by a single holistic solution, Huawei claims that an inconsistent patchwork of solutions will emerge instead, some of which will bypass the Internet altogether.[153] This would push the global network environment further towards fragmentation and risk creating several non-interoperable communication "islands," an outcome Huawei believes

---

[145] TSAG C-83, *supra* note 6, at 2.

[146] Li et al., *New IP Data Packet Framework*, *supra* note 112, at 3 (explaining the phenomenon it refers to as ManyNets and arguing that today's public Internet will eventually be only one such Internet in this collection); Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Report of NSP e-meeting (23 June 2020)*, SG13-TD456/GEN (July. 2020), https://www.itu.int/md/T17-SG13-200720-TD-GEN-0456 (clarifying that ManyNets is an ongoing phenomenon New IP is intended to address, not a goal or end state it is trying to achieve).

[147] *See* TSAG-C83, *supra* note 6, (describing the current design of the Internet as "vastly insufficient"); Zhe Chen et al., *NEW IP Framework and Protocol for Future Applications*, *in* PROC. IEEE/IFIP NETWORK OPERATIONS & MGMT. SYMP. 1 (2020), https://doi.org/10.1109/NOMS47738.2020.9110352 [hereinafter Chen et al., *NEW IP Framework*] ("The current TCP/IP protocols and framework contain limitations for the ManyNets interconnectivity.").

[148] Li, *Network 2030 and New IP*, *supra* note 124, at 25 (describing 128-bit addresses as "overkill" for low-power devices).

[149] Chen et al., *NEW IP Framework*, *supra* note 147, at 1.

[150] *Id*.

[151] *Id*.

[152] Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Proposal of text amendments to the Terms of Reference of the proposed new Question G (Q.G) for the next study period of SG13*, SG13-C995 (July. 2020), https://www.itu.int/md/T17-SG13-C-0995 ("Furthermore, most of the existing interconnection methods are essentially designed based on static physical network topologies. . . . The current addressing and routing schemes were not designed to support such network dynamicity.").

[153] *See* TSAG-C83, *supra* note 6, at 2.

should be avoided.[154] Hence, the motivating force behind New IP's changes to Internet addressing, at least on the proposal's face, is accommodating and maintaining interconnectivity among ManyNets by overcoming the aforementioned limitations of IP addressing.

One of the primary functional requirements for New IP would be to provide a common, universal address format capable of supporting variable-length addresses as well as multiple semantics. Whereas the former is fairly self-explanatory, support for multiple address semantics essentially means the ability for network devices to interpret an IP address as something other than a location on the network's topology. For instance, the address format may be defined such that those starting with a certain sequence of bits are interpreted as identifying a piece of content rather than a host.[155] Routers would then use the remaining bits in the address to make a forwarding decision based on the nearest instance of that content.[156] Similarly, a different leading sequence of bits may be designated to signify the address is instead carrying geographic location information, which may be used in Low Earth Orbit satellite networks to calculate the shortest path to a ground destination based on the relative positions of satellites at the time.[157]

Some New IP critics have raised concerns about the use of content or person-based identifiers in the address field.[158] They argue it would facilitate tracking and censorship by exposing information about the requested content or recipient in the packet header for intermediate network elements to see.[159] Yet, it is important to recognize that the proposal does not prescribe or endorse a particular address type, only a format flexible enough to accommodate the many possible address types that could emerge in the future.[160] While New IP could support content or identity-based addressing and forwarding schemes, they would still need to be separately developed and implemented. The extent to which these schemes would be averse to privacy or information freedom would be determined almost entirely by the choices made during the design and implementation processes.[161] Until this actually happens, it would be speculative to draw any conclusions about whether these features were intended to facilitate censorship or surveillance.

That said, this dimension of New IP still leaves some major questions unanswered. The most crucial such question pertains to its intended scope, as it is unclear whether New IP addressing was intended to be a general purpose solution, providing globally-routable and unique identifiers that would supplant IPv6, or if they are intended to have a more limited application to those environments where existing address limitations present issues. This question is of great

---

[154] *Id*.

[155] *See* Chen et al., *NEW IP Framework*, *supra* note 147, at 2 (describing an address format that would encode information about the size, structure, and semantics into the beginning addresses first 8 bits).

[156] *See* TSAG Tutorial, *supra* note 113, at 20.

[157] *See id*. at 19 (depicting geography-based addressing and routing in ground-satellite networks); Li et al., *supra* note 146, at 8 (explaining the new address format accommodates "the need for geographic address structures for the networks involving satellites.").

[158] *See, e.g.*, Taylor et al., *supra* note 14, at 196 (arguing the use of persistent object identifiers "would enable unparalleled tracing over the internet").

[159] *Id*.

[160] Sharp & Kolkman, *supra* note 121, at 4 ("[T]he New IP framework proposes a flexible length address space to subsume all the possible future types of addresses").

[161] There is nothing inherently privacy compromising about Information-Centric Networking (ICN). Consider, for example, Named Data Networking (NDN), a proposed ICN-based architecture initially developed through the NSF-funded Future Internet Architecture project. Largely due to its stateful forwarding plane, NDN enables content to be anonymously requested and retrieved over a network without any information about the requestor (e.g., a source address) being included in a packet. *See Named Data Networking: Motivation & Details*, NAMED DATA NETWORKING (last visited July 7, 2023), https://named-data.net/project/archoverview/.

significance, as if the answer is the former, it would seemingly introduce several new challenges from both a technical and governance perspective. For instance, who would be the entity responsible for managing the new global address space? How would they break up and allocate these addresses? Would requiring every router to support forwarding based on several different address semantics—greatly increasing the amount routing information that would need to be exchanged and stored—have a detrimental impact on the complexity and scalability of the routing system?[162] Unless the benefits are overwhelming, issues like these, along with the arduous and costly transition process, would make it difficult to justify a new global addressing scheme.

Conversely, it is possible New IP's flexible addressing was not intended to replace IPv6 addresses but to instead serve as a complement whose use is limited to scenarios where conventional addressing is inadequate. Limiting it to smaller special-purpose networks (e.g., industrial, ground-satellite, etc.) would obviate the need for these addresses to be globally unique, although they would be routable only within the smaller network. In order to travel over the public Internet, a packet with a flexible address would either need to be translated into a unique IPv6 address or encapsulated into an IPv6 packet that is then sent over the public Internet and unwrapped when it reaches the destination network (a process called tunneling). Understood this way, New IP's flexible addressing features would function as a Swiss-army knife for connecting special purpose networks to the Internet, providing one standard mechanism for turning packets with heterogenous private addresses into globally routable ones. Although this would avoid many of the challenges associated with a new global addressing scheme, it is uncertain just how strong of a value proposition it offers.

The questions about New IP's intended scope turn out to be a major theme throughout Huawei's proposal. Earlier descriptions of New IP paint a far more ambitious picture and seem to operate on the assumption that the new protocol would indeed act as a successor to IP.[163] Yet, a notable shift in direction can be seen in later New IP materials. Several months after first introducing New IP, Huawei effectively rebranded its initiative within ITU-T with the title Future Vertical Communications Networks (FVCN).[164] While retaining nearly all of the original's proposed features, FVCN emphasized a more limited application of the future protocols within the networks of certain industry verticals (e.g., manufacturing, energy, etc.) rather than globally.[165]

Even in discussions outside of the ITU, Huawei began to advertise a more complementary role for New IP, characterizing it as a fully TCP/IP-compatible solution for connecting industrial networks with unique requirements directly to the Internet.[166] Although none of this was ultimately

[162] *See* TSAG Tutorial, *supra* note 113, at 20 (indicating New IP would be capable of direct routing based on diverse IDs through "maintaining diverse ID routing tables in the network").

[163] This is on display from the very first substantive slide of Huawei's initial New IP presentation at the ITU-T. Here, it shows a graphic in which TCP/IP and several other non-IP network types all converge into one future network (New IP). *See* TSAG Tutorial, *supra* note 113, at 3.

[164] *See generally* Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Encourage study on future network evolution supporting vertical applications including Future Vertical Communication Networks*, SG13-C1062 (July 2020), https://www.itu.int/md/T17-SG13-C-1062/en.

[165] Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], Supporting contribution to the two contributions submitted into the July 2020 SG13 meeting which propose text amendments to the Terms of Reference of, respectively, draft Questions F and G of SG13 (Q.F/13 and Q.G/13) for the next study period of SG13, SG13-C996 at 2-5 (July 2020), https://www.itu.int/md/T17-SG13-C-0996 (clarifying that FVCN protocols "are not meant to replace the existing Internet protocols," but instead to complement them in "business-critical industrial" use cases.).

[166] In response to the initial wave of criticism, Dr. Richard Li, chief scientist at Huawei's U.S.-based research arm and one of the central most figures behind New IP, setup a website where he re-iterated this more limited role.

enough to save New IP, there was still a noticeable pivot away from portraying it as a TCP/IP replacement. Of course, a more cynical interpretation of this pivot might simply dismiss it as a rhetorical strategy in response to the initial public blowback the proposal drew. Yet, it is also possible to see this as an act of pragmatism, whereby Huawei realized the proposal's most important goals could be achieved through less radical changes. This narrowed focus on industrial use cases should thus be kept in mind when debating the underlying motives of New IP, as it arguably provides another hint about what the proposal was really out to accomplish.

III. CONFRONTING THE "TROJAN HORSE" NARRATIVE

A more robust understanding of the New IP proposal better positions us to address one of this Article's animating questions: Are China's efforts to enhance its position within the international standard-setting landscape really just a trojan horse, a hidden strategy for giving the global Internet's architecture and governance arrangements an authoritarian overhaul? This is indeed the way it has been framed by many predominantly Western actors, and the New IP initiative—having become largely understood as a calculated attempt to expand state control over the Internet—is regularly cited as validation.[167] However, we argue this type of framing provides, at best, a reductive understanding China's Internet standard-setting ambitions, inflating many of the interests involved while neglecting others. This Part addresses two major problems with the trojan horse narrative. The first concerns limitations within ITU-T to the state-centric approach to global standard-setting that China purportedly favors, while the second involves flawed assumptions about the regulability of the existing TCP/IP Internet. We find that both issues become particularly glaring when the narrative framework is superimposed onto the case of New IP.

A. The Limits of the ITU-T and Multilateral Approaches to Standard Setting

According to the conventional account, one of the primary goals in China's pursuit of greater influence over the standard-setting process is to reshape the institutional landscape, moving functions away from open, privatized, multistakeholder bodies in favor of those that provide a stronger voice to governments.[168] This type of multilateral approach to standard-setting would be consistent with China's endorsement of cyber sovereignty as an alternative normative foundation for global Internet governance. It has also been suggested that China finds a "one country, one

Richard Li, *Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T,"* INTERNET EVOLUTION (June 2, 2020), https://internet4future.wordpress.com/ ("New IP complements IP and is intended to connect to the Internet the networks and their terminals that have not been connected to the Internet for certain types of business-critical industrial use.").

[167] *See, e.g.*, Taylor et al., *supra* note 14, at 186 ("China's New IP has an authoritarian flavor. It is designed to capture large amounts of data and enable centralized controls that could be harnessed for government surveillance."); Freedom House, *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet* 16 (2022), https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf (describing New IP as a plan to redesign common protocols to "facilitate greater state control over domestic networks.").

[168] *See, e.g.*, USCC 2022 Report, *supra* note 10, at 459-60; Shane Tews, *China's Tech Ambitions Threaten to Fundamentally Change How the Internet Functions*, AM. ENTER. INST. (July 7, 2020), https://www.aei.org/technology-and-innovation/chinas-tech-ambitions-threaten-to-fundamentally-change-how-the-internet-functions/ (claiming China seeks to "destabilize" existing governance arrangements in favor of a centralized top-down model).

vote" system attractive because it could court like-minded countries to help push through controversial standards that would otherwise fail in an open, consensus-based model.[169]

In terms of a venue, the prevailing assumption has been that China sees ITU-T as an ideal fit. Indeed, China has been quite explicit in its support for expanding the ITU's role within the broader Internet governance system, which can be interpreted as including the development of technical standards.[170] It was thus seen as little coincidence that Huawei brought the New IP proposal to ITU-T instead of a body like the IETF.[171]

On the surface, this part of the trojan horse narrative appears perfectly reasonable. Yet, in reality, shifting Internet standard setting away from a multistakeholder model towards a more multilateral approach would provide China with much more limited ability to achieve many of the goals attributed to it than is generally realized and thus lacks much of the appeal suggested by most observers. Venues like ITU-T are not a panacea that allow authoritarian-leaning countries magically to overcome Western opposition to controversial proposed standards and ensure their global adoption. Moreover, as China's national champions in the ICT sector grow stronger, moving away from an industry-led standards development model may actually work to its detriment.

1. Adherence to Consensus-Based Decisionmaking

First, consider China's purported venue of choice, ITU-T. Despite the numerous differences between ITU-T and bodies like the IETF, the former still largely adheres to consensus-based decision making. It has not, at least in practice, proven to be substantially different from the "rough consensus" of the IETF.[172] During a study period, there are two separate tracks that a recommendation can travel through to gain approval for final publication.[173] In both such tracks, opposition from a single member state delegation is sufficient to stop a draft from proceeding.[174] The Alternative Approval Process, which despite its name is the track selected for an

---

[169] *See* Mark Montgomery & Theo Lebryk, *China's Dystopian "New IP" Plan Shows Need for Renewed US Commitment to Internet Governance*, JUST SEC. (Apr. 13, 2021) https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/; Russel & Berger, *supra* note 54, at 23-24; Hoffman et al., *supra* note 13, at 253.

[170] *See supra* note 50.

[171] *See, e.g.*, Tony Blair Inst., *The Open Internet on the Brink: A Model to Save Its Future* 24 (Sept. 2021), https://institute.global/policy/open-internet-brink-model-save-its-future ("China's proposal provides the opportunity for national governments, which support more tightly censored and regulated models of the internet, to have greater power in shaping its future"); Marco Hogewoning, *Do We Need a New IP?*, RIPE.NET (Apr. 22, 2020), https://labs.ripe.net/author/marco_hogewoning/do-we-need-a-new-ip/ (arguing New IP is being leveraged as an opportunity to redesign internet governance to have a more "top-down structure").

[172] *See* Bradner, *supra* note 31, § 3.3 (stating working groups make decisions through "rough consensus," some level of agreement between a simple majority and unanimity that satisfies the judgement of the group's chair); see also Voo & Creemers, supra note 54, at 11 (noting ITU Study Groups also require approval by consensus similar to many other SDOs).

[173] *See generally* World Telecomm. Standardization Assembly, *Resolution 1 - Rules of procedure of the ITU Telecommunication Standardization Sector*, INT'L TELECOMM. UNION TELECOMM. STANDARDIZATION SECTOR [ITU-T] § 8 (Rev. 2022), https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.1-2022-PDF-E.pdf [hereinafter WTSA Res. 1]; Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Recommendation A.8 - Alternative approval process for new and revised ITU-T Recommendations*, (Rev. 2022), https://www.itu.int/rec/T-REC-A.8-202203-I/en [hereinafter ITU-T Rec. A.8].

[174] *See* WTSA Res. 1, *supra* note 173, § 9.5.3 ("[D]ecision of the delegations . . . to approve the Recommendation under this approval procedure must be unopposed").

overwhelming majority of recommendations, even permits a lone non-state sector member to prevent the requisite "unopposed agreement" from being reached at the final stage.[175]

In essence, this means countries like China are unable to leverage U.N.-style voting-bloc politics to successfully push through contentious standards.[176] Consensus-based decision making, which also applies to the approval of new ITU-T study questions, is precisely what prevented New IP from moving forward.[177] This is not a limitation that can be changed without consequence. To understand why, one must turn to the law of international trade, or more specifically, the World Trade Organization's Agreement on Technical Barriers to Trade (TBT).[178]

A component of the overall WTO agreement, and thus binding on all WTO Members, the TBT agreement's primary goal is to ensure that standards and standards-based technical regulations do not create unnecessary obstacles to international trade.[179] It requires that Members, to the extent they mandate adherence to a standard through national regulation, base such regulations on "relevant international standards."[180] This provision is intended to prevent countries from using technical regulations to serve protectionist ends, favoring domestic firms by conditioning the market access of their foreign competitors on adherence to unique national standards.[181]

The reason the TBT regime is germane to the ITU and its internal decision-making procedures involves the "relevant international standards" language mentioned above.[182] The ITU is generally considered one of the few recognized "international standardizing bodies" capable of producing standards that meet this definition, which in turn, gives them a (rebuttable) presumption of compliance with the TBT agreement when used as the basis for national technical regulations.[183] Some have hypothesized this special status is part of what China finds attractive about ITU-T as

---

[175] *See* ITU-T Rec. A.8, *supra* note 173, §§ 4.3, 5.3; however, opposition from a lone Sector Member during the final stage may effectively be overridden if there have been repeated attempts to reach unopposed agreement and no more than one Member State present is in opposition. *See id*. § 5.4.

[176] It should be noted that there are limited circumstances where a draft recommendation that has failed to gain consensus in a Study Group may be deferred to the World Telecommunication Standardization Assembly (WTSA), the ITU-T's full governing body, at which point it is possible for the recommendation to be adopted through a simple majority vote of Member States. *See* WTSA Res. 1, *supra* note 173, § 9.2.2. However, these circumstances are rare, and to the extent they do occur, almost always involve recommendations related to economic and policy matters instead of technical ones. At the previous two WTSAs, the only draft recommendations submitted for consideration were all Series D, which involve accounting, tariffs, and other policy issues. *See* Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Proceedings of the World Telecommunication Standardization Assembly*, Part V-15.18 (2016), https://www.itu.int/pub/T-REG-LIV.1-2016/en.

[177] *See* Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Report of the ITU-T Study Group 13 Meeting*, SG13-R40 4 (Dec. 17, 2020), https://www.itu.int/md/T17-SG13-R-0040 [hereinafter SG13 December 2020 Meeting Report] (recording that Huawei's proposed study questions were not approved due to a "significant number of objections.").

[178] *See generally* Agreement on Technical Barriers to Trade, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, annex lA, 1868 U.N.T.S. 120 [hereinafter TBT Agreement].

[179] DENARDIS, GLOBAL WAR, *supra* note 21, at 83.

[180] TBT Agreement, *supra* note 177, art. 2.4.

[181] Olia Kanevskaia, *Governance of ICT Standardization: Due Process in Technocratic Decision-Making*, 45 N.C. J. INT'L L. 549, 573 (2020); Panagiotis Delimatsis, *Global Standard-Setting 2.0: How the WTO Spotlights ISO and Impacts the Transnational Standard-Setting Process*, 28 DUKE J. COMP. & INT'L L. 273, 278 (2018).

[182] TBT Agreement, *supra* note 177, annex 1.2 (defining standard to mean those approved by a "recognized body").

[183] *See id*. at 299; Kanevskaia, *supra* note 181, at 605; *see also* TBT Agreement, *supra* note 177, art. 2.5 (stating that technical regulations serving a legitimate objective and that are consistent with relevant international standards are "rebuttably presumed not to create an unnecessary obstacle to international trade").

the venue is uniquely positioned to legitimize standards and give them a pre-emptive effect over inconsistent national technical regulations enacted by WTO members.[184]

However, there is an important caveat here. The WTO's Appellate Body has indicated this status is contingent on a standards body's adherence to a number of procedural principles that are outlined in a Decision from the WTO's TBT Committee.[185] Along with familiar principles like transparency and openness to participation, this Decision states that bodies preparing international standards should ensure that "impartiality and consensus" are observed.[186] More specifically, it directs them to establish consensus procedures that "take into account the views of all parties concerned and to reconcile any conflicting arguments."[187] Moving away from consensus-based decision-making—a widely-accepted best practice for standards development—would thus not only damage ITU-T's legitimacy; it would threaten one of the venue's few remaining value propositions by seriously jeopardizing its status as a recognized international standardizing body under the TBT.

2. The Need for Voluntary Adoption

Even if one disregards the obstacles presented by consensus-based standards development, several challenges would remain even if China were to push a controversial new protocol suite through a venue like ITU-T. The largest such challenge would be getting the manufacturers and operators of Internet infrastructure around the world, most of whom are private actors, to implement these new standards. The successful standardization of an alternative Internet architecture, even by a multilateral body, far from guarantees its adoption in the real-world. ITU-T knows this all too well, having been behind not one but two unsuccessful attempts in its history.

The first came in the mid-1970s when ITU-T (then known as the CCITT) developed a standard for data networking called X.25.[188] Since ITU-T was dominated by state-owned telephone monopolies at the time, X.25's highly network-centric and connection-oriented design was naturally modeled after the way circuit-switched telephone networks operated. However, as Internet historian Janet Abbate writes, "the 'telephone model' of computer networking did not fit well with the way computer users actually wanted to use networks."[189] The second attempt took place during the so-called "Internet standards wars" of the late 1980s and early 1990s when ITU-T, in collaboration with the International Organization for Standardization, championed the Open Systems Interconnection (OSI) protocol suite.[190] However, OSI's overall architecture proved far

---

[184] *See, e.g.*, Taylor et al., *supra* note 14, at 188-89; Hoffman et al., *supra* note 13, at 246.

[185] Appellate Body Report, *United States - Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products* ¶ 379, WTO Doc. WT/DS381/AB/R (adopted June 13, 2012) ("[T]he TBT Committee Decision, reflect the intent of WTO Members to ensure that the development of international standards take place transparently and with wide participation. . . . In analyzing whether an entity is an 'international standardizing body,' a panel needs to balance these considerations."); *see also* Delimatsis, *supra* note 181, at 281-84 (explaining how "recognized international body" has come to be interpreted under WTO case law).

[186] Comm. on Tech. Barriers to Trade, *Second Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers to Trade, Annex 4: Decision on Principles for the Development of International Standards, Guides and Recommendations with Relation to Articles 2, 5 and Annex 3 of the TBT Agreement*, WTO Doc. G/TBT/9 25-26 (Nov. 13, 2000).

[187] *Id*.

[188] *See* ABBATE, *supra* note 74, at 152.

[189] *Id*. at 156-57.

[190] *See* Andrew L. Russell, *The Internet that Wasn't*, IEEE SPECTRUM, Aug. 2013, at 39, 40-42 (2013) (providing a history of the Open Systems Interconnection standards).

more complex than was practical, and its development was prolonged by slow bureaucratic processes that allowed the competing TCP/IP suite enough time to firmly establish itself.[191]

Although X.25 and the OSI protocols each saw periods of modest adoption, most of that coming outside of the United States, TCP/IP ultimately prevailed.[192] A significant reason these alternative protocol suites were unsuccessful is that they failed to account for the type of network capabilities for which there was legitimate demand at the time and that had been proven to work in practice.[193] This an inherent limitation of developing Internet standards through a top-down, anticipatory approach instead of in a more responsive, bottom-up fashion (*à la* the IETF).[194] Absent a government mandate, the choice to adopt a particular standard will be left up to market actors to decide based on a variety of technical, economic, and political considerations. If an alternative set of core protocols developed by ITU-T or any other multilateral venue is to avoid the same fate as X.25 and OSI, it will need to justify itself to these market actors. History has shown this to be no easy task.

The aforementioned limitations of multilateral Internet standard-setting do not necessarily mean China has no reason to favor this approach over the existing multistakeholder model. Despite having of a fair degree of political control over Chinese firms and thus being able to shape their engagement at multistakeholder SDOs, agency problems still exist.[195] These could effectively be eliminated through a system in which States are involved more directly in the standard-setting process. Given its public support for expanding the ITU's role within the Internet governance ecosystem, China obviously sees *some* benefit in trying to shift functions to Geneva. At the same time, it is important that we focus on China's actions just as much as we focus on its rhetoric. These actions reveal a growing acceptance of the current institutional arrangements for standards development. As explained in Part I, China has been heavily promoting the engagement of domestic firms in the existing industry-driven ICT standards environment. Although it has yet to surpass the United States, the results thus far are fairly promising. As the influence of Chinese actors in this domain continues to grow, China's support for a "one country, one vote" style of multilateralism may become even more difficult to justify.

B. How China Made Its Internet Regulable

The second component of the trojan horse narrative posits that China's standard-setting agenda is motivated by a desire to reinvent the Internet's technical architecture in its own image. Not only might this result in an Internet architecture that streamlines China's ability to censor and surveil its citizens, but fears exist that this architecture would export embedded authoritarian values around the globe in service of legitimizing alternative norms like cyber sovereignty.[196]

---

[191] *See* ANDREW S. TANENBAUM, COMPUTER NETWORKS 51-53 (5th ed. 2010) (examining several of the reasons OSI failed).

[192] *See* ABBATE, *supra* note 74, at 167, 176 (summarizing the fates of X.25 and OSI protocols).

[193] *See* Russell, *supra* note 190, at 43 (acknowledging that, while OSI's reputation as a total failure is not entirely fair, it is frequently portrayed as a cautionary tale of overly bureaucratic "anticipatory standardization.").

[194] *See* Benoliel, *supra* note 17, at 1094-95 (explaining that the limitations of anticipatory standardization are why it eventually gave way to participatory approaches which directly involve stakeholders through a more iterative process).

[195] *See* Erie & Streinz, *supra* note 64, at 55 (acknowledging that agency issues even exist between the government and state-owned enterprises)

[196] These fears are not unique to the standard-setting context but have accompanied China's general rise as technological power. For example, a 2020 document released by the Trump Whitehouse on its China strategy charged

The concerns surrounding China's purported interest in radically reshaping core Internet protocols appear consistent with one of early cyberlaw's most influential insights: the capacity of the Internet's technical architecture to regulate user behavior.[197] Scholars such as Lawrence Lessig even predicted that governments of the future would increasingly attempt to alter the Internet's architecture, either directly or indirectly, seeking to transform it from a freedom-enabling unregulable space towards one that can be easily and effectively controlled.[198] Yet, the proposition that fundamental changes to core protocols are either a necessary or especially compelling means of enabling such control contains shades of Internet exceptionalism, a once common view of the Internet as unique in its transcendence of territorial jurisdiction and thus resistant to traditional forms of regulation.[199] Needless to say, history has not been kind to this perspective which, if not already dead, is still on life-support.[200]

Perhaps no single actor contributed more to the shattering of this exceptionalist paradigm than China, the country that demonstrated that it was indeed possible to "nail[] Jell-O to the wall"—to borrow once again President Clinton's famous metaphor.[201] Many are already familiar with the so-called Great Firewall surrounding China, the "semipermeable membrane that lets in what the government wants and blocks what it doesn't," but this only begins to scratch the surface.[202] China has built the world's most sophisticated Internet control regime, comprised of complementary legal and technical architectures whose effects extend from the network's physical infrastructure to the content/applications running on top of it. Most of what critics fear that authoritarian-aligned protocols would enable is not only possible with the existing TCP/IP Internet; it is already being done in China.

1. Licensing

First, the Chinese party-state exercises strict control over who can provide Internet-related services within its borders. At the infrastructure level, an entity seeking to provide Internet access

---

the CPC with attempting to spread its ideology beyond China's borders by actively exporting the tools of its "techno-authoritarian model" around the world. *United States Strategic Approach to the People's Republic of China*, WHITE HOUSE 5 (May 20, 2020) https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf.

[197] *See supra* note 81 and accompanying text.

[198] *See* Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 763 (1999). It should be noted here that in using the term "architecture," Lessig explicitly clarified he was not necessarily speaking about core protocols but was referring broadly to the design of all the various hardware and software components that makeup cyberspace. LESSIG, CODE, *supra* note 74, at 62, 72.

[199] The most famous enunciation of this exceptionalist position (or at least its descriptive variety) came from EFF co-founder John Perry Barlow, who boldly pronounced that world governments "have no sovereignty" in this newly formed cyberspace and that the legal concepts which govern the physical world do not apply. *See generally* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence. However, that Barlow's *Declaration* has become a punching bag for those taking jabs at the naivete of early techno-libertarianism is rather unfair. It was a piece of lyrical prose meant to capture the promethean optimism evoked by the nascent Internet, not a nuanced argument about the possibility of public legal order in cyberspace. For a highly-cited attempt at the latter, *see generally* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[200] *See generally* Tim Wu, *Is Internet Exceptionalism Dead?*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 179 (Berin Szoka & Adam Marcus eds., 2010).

[201] *See supra* note 16 and accompanying text.

[202] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 92 (2006).

or transit services must first obtain the appropriate state-issued operating license.[203] Eligibility for an operating permit is contingent on conforming to certain ownership restrictions: foreign equity in last-mile ISPs and backbone network operators must be no greater than 50% and 49%, respectively, with the latter being at least 51% state owned.[204] Although the regulations as written appear to permit some degree of foreign ownership, this is not the case in practice as very few foreign invested entities have been successful in obtaining requisite licenses.[205]

None of what China does here is revolutionary. Many other countries limit foreign access to their domestic telecommunications markets, and even more of them impose similar licensing requirements, especially those applicable to the provision of wireless access services as these can be found in virtually every country. However, part of what distinguishes China from the rest is that it extends its licensing regime to the application/content level. Entities seeking to provide commercial information services over the Internet, such as operators of a website or mobile application, must first obtain an Information Content Provider (ICP) license.[206] Further requirements exist for special types of information services, such as those that distribute news or audiovisual content.[207] In both the case of ICPs and ISPs, those operating without a licenses face the risk of receiving large fines as well as closure/termination of their services.[208] In requiring prior authorization to operate such services, placing limitations on foreign and private ownership, and imposing the threat of license revocation for non-compliance with accompanying regulatory obligations, the party-state puts itself in a much stronger position to control domestic Internet activity both directly and indirectly.[209]

---

[203] Zhonghua Renmin Gongheguo Dianxin Tiaoli (中华人民共和国电信条例) [*Telecommunication Regulation of the People's Republic of China*] (promulgated by State Council Sept. 25, 2000, effective Sept. 25, 2000, amended Feb. 6, 2016), art. 7, CLI.2.267182 (EN) (PKULaw) [hereinafter Telecommunication Regulation] (establishing licensing requirements for the provision of various telecommunications services). Under China's telecommunications regulatory framework, Internet access services are classified as value-added telecom services, whereas Internet transmission (i.e., backbone) services are categorized as basic telecom services. This classification is what determines the applicable foreign-ownership restrictions. *Id*. at Appendix – Catalogue of Telecommunications Business.

[204] *See id*. art. 10; *see also* Waishang Touzi Dianxin Qiye Guanli Guiding (外商投资电信企业管理规定) [*Provisions on the Administration of Foreign-funded Telecommunications Enterprises*] (promulgated by State Council Jan. 1, 2001, effective Jan. 1, 2002, amended May 1, 2022), art. 6, LEXIS CHINA ONLINE, htttp://www.lexiscn.com.

[205] STAFF OF PERMANENT SUBCOMM. ON INVESTIGATIONS, S. COMM. ON HOMELAND SEC. & GOVT'L AFFS., 116TH CONG., THREATS TO U.S. NETWORKS: OVERSIGHT OF CHINESE GOVERNMENT-OWNED CARRIERS 19 (2020) (noting that no foreign entity has ever been successful in meeting the requirements for offering basic telecom services, while only a few dozen have successfully secured value-added licenses.).

[206] Hulianwang Xinxi Fuwu Guanli Banfa (互联网信息服务管理办法) [Measures for the Administration of Internet Information Services] (promulgated by the State Council, Sept. 25, 2000, effective Sept. 25, 2000, amended Jan. 8, 2011), art. 4, CLI.2.174868 (EN) (PKULaw) [hereinafter Internet Information Service Measures]. Commercial Internet information services are considered value-added telecommunication services, meaning they must comply with foreign-ownership restrictions to obtain a license. *See supra* note 204 and accompanying text. Non-commercial Internet information services—those that operate without compensation and are purely informational—must only submit an ICP filing also known as a "bei'an" (备案). *See* Hulianwang Xinxi Fuwu Guanli Banfa, *supra*, art. 7, 8.

[207] Rogier Creemers, *The Privilege of Speech and New Media: Conceptualizing China's Communications Law in the Internet Era*, *in* THE INTERNET, SOCIAL MEDIA AND A CHANGING CHINA 92-93 (Jacques deLisle et al. eds., 2016).

[208] *See* Internet Information Service Measures, *supra* note 206, arts. 19-23.

[209] *See* Henry Gao, *Data Regulation with Chinese Characteristics*, *in* BIG DATA AND TRADE 245, 258 (Mira Burri ed., 2021) (stating that the threat of having a license revoked or website shut down is what gives the regulations "real teeth").

2. State Controlled Chokepoints

Second, from the early stages of China's connection to the global Internet, it began taking measures to limit the channels over which information was allowed to flow in and out of its territorial borders. In 1996, the State Council issued a set of administrative regulations mandating that "interconnecting networks," those directly connecting to networks outside China, achieve this interconnection though international Internet gateways designated and supervised by the Ministry of Posts and Telecommunications, a predecessor to what is now the Ministry of Industry and Information Technology (MIIT).[210] Entities are prohibited from connecting internationally through any channels—physical or virtual (i.e., VPNs)—outside of the approved gateways.[211] Moreover, the day-to-day operation of these gateways must be carried out by state-owned entities that are subject to the supervision, inspection, and guidance of MIIT.[212]

Funneling all internationally inbound and outbound traffic through a small number of state-managed Internet "chokepoints," makes information flows much easier to control than in a flatter, more decentralized network topology.[213] Under this architecture, one can no longer simply "route around" the censorship, as digital pioneer John Gilmore once famously said the TCP/IP Internet permits by default.[214] This is thus one of the biggest reasons why China's Great Firewall is even remotely effective.[215]

Much of what is publicly known about the Great Firewall and how it operates is the result of black box testing conducted by outside Great Firewall. Though we will not expound much on this here, the Great Firewall is believed to employ a variety of techniques, including simple IP

---

[210] *See* Zixiang Alex Tan et al., *China's New Internet Regulations: Two Steps Forward, One Step Back*, COMM. ACM, Dec. 1997, at 11 (analyzing the State Council's [then] newly issued *Interim Regulations on International Interconnection of Computer Information Networks*).

[211] Gao, *Data Regulation with Chinese Characteristics*, *supra* note 209, at 248.

[212] Guoji Tongxin Churukou Ju Guanli Banfa (国际通信出入口局管理办法) [*Measures on the Administration of International Communication Accesses*] (promulgated by Ministry of Info. Indus. Mar. 14, 2002, effective Oct. 1, 2002) Art. 7, CLI.4.40342 (EN) (PKULaw).

[213] This is consistent with the empirical findings of researchers over the years who have attempted to map the topology of China's Internet, observing that traced inbound traffic traveled through just a small number of ASes belonging to state-owned backbone operators like China Telecom and China Unicom, or one of non-commercial networks like CERNET. *See, e.g.*, Hal Roberts et al., *Mapping Local Internet Control* (Oct. 2011) (paper presented at the 25th IEEE Annual Computer Communications Workshop (CCW)), *available at* https://cyber.harvard.edu/netmaps/mlic_20110513.pdf; Guangchao Charles Feng & Steve Zhongshi Guo, *Tracing the Route of China's Internet Censorship: An Empirical Study*, 30 TELEMATICS & INFORMATICS 335 (2013), https://doi.org/10.1016/j.tele.2012.09.002.

[214] Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME (Dec. 6, 1993), https://content.time.com/time/subscriber/article/0,33009,979768-3,00.html (quoting John Gilmore as saying "[t]he Net interprets censorship as damage and routes around it"). Although it may be difficult to route around these chokepoints, the emergence of Internet access technologies like low Earth orbit (LEO) satellite broadband could provide a means of going over the top of the Great Firewall. This is because LEO satellite constellations can deliver Internet connectivity directly to end-user terminals without needing to be relayed through an ISP-controlled ground station. Even though the leading provider of this service—SpaceX's Starlink—is not currently available in China (reportedly at the government's request), and China is currently constructing a large State-owned LEO constellation of its own, this technology still has the potential to present serious challenges to China's Internet control regime in the future. *See* Russel Brandom, *China asked Elon Musk not to sell Starlink within the country*, VERGE (Oct. 10, 2022), https://www.theverge.com/2022/10/10/23397301/elon-musk-starlink-china-great-firewall-censorship; *see also* Cate Cadell, *China's military aims to launch 13,000 satellites to rival Elon Musk's Starlink*, WASH. POST (Apr. 6, 2023), https://www.washingtonpost.com/national-security/2023/04/06/elon-musk-china-starlink-pla/.

[215] GOLDSMITH & WU, *supra* note 202, at 93.

address-based blocking, DNS manipulation, and URL/keyword filtering using Deep Packet Inspection (DPI).[216] Just as importantly, it has continued to evolve over time to keep pace with new circumvention techniques, as is demonstrated by its ability to block the use of privacy enhancing technologies such as the Tor network.[217] While far from perfect, it is effective enough against the average Chinese netizen to prevent the spread of unfavorable information from reaching the critical mass where it becomes a serious problem for the Party.[218]

3. Intermediary Liability and Self-Censorship

Third, while the Great Firewall is the primary means of controlling transnational Internet information flows, the approach for regulating domestic ones relies heavily on a form of intermediary liability in which censorship is effectively outsourced to ISPs and ICPs in exchange for their avoidance of license revocation, fines, and other administrative punishments.[219] There are several different sources of law in China that impose obligations on both ISPs and ICPs to record, report, and prevent users' dissemination of prohibited content through their services, either upon discovering it or being given notice.[220] Prohibited content in this context refers to a number of broadly defined categories that appear uniformly across major Internet laws and regulations.[221] It ranges from content that undermines state security, public order, social stability, or national honor to content that promotes vulgarity, pornography, gambling, or violence.[222] Some of these

---

[216] *See* Daniel Anderson, *Splinternet Behind the Great Firewall of China*, ACM QUEUE , Nov. 2012, at 40, 41-42 (describing the use of null routing or "blackholing," in which false routing information is advertised and propagated across border ASes so that routers drop traffic bound for blacklisted IP ranges instead of correctly forwarding it.); Richard Clayton et al., Ignoring the Great Firewall of China, *in* Privacy Enhancing Technologies 20 (George Danezis & Philippe Golle, eds., 2006) (explaining that the Great Firewall functions like an Intrusion Detection System, analyzing passing traffic out-of-band and, if found to violate policy, sending TCP resets to both endpoints to terminate sessions before data transfer can be completed); Graham Lowe et al., *The Great DNS Wall of China* (2007), https://censorbib.nymity.ch/pdf/Lowe2007a.pdf (demonstrating how the Great Firewall falsifies bad responses to DNS queries).

[217] *See* Roya Ensafi et al., *Examining How the Great Firewall Discovers Hidden Circumvention Servers*, *in* IMC'15: PROC. 2015 INTERNET MEASUREMENT CONF. 445, 446-47 (2015), https://dl.acm.org/doi/10.1145/2815675.2815690 (finding the Great Firewall uses "active probing" to discover and block hidden Tor bridges); *see also* Simon Sharwood, *China upgrades Great Firewall to defeat censor-beating TLS tools*, REGISTER (Oct. 6, 2022), https://www.theregister.com/2022/10/06/great_firewall_of_china_upgrades/.

[218] *See* Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J.L. SCI. & TECH. 125, 146-47 (2012).

[219] *See, e.g.*, REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 36 (2012) ("[D]omestic companies are the stewards and handmaidens, the tools and enforcers, of China's inner layer of Internet censorship").

[220] In terms of legal authority, the highest-ranking source of these obligations is China's Cybersecurity Law. Zhonghua Renmin Gongheguo Wanglao Anquan Fa (中华人民共和国网络安全法) [*Cybersecurity Law of the People's Republic of China*] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 47-48, CLI.1.283838 (EN) (PKULaw) [hereinafter Cybersecurity Law]. However, more detailed articulations can be found in prior administrative regulations. *See* Internet Information Service Measures, *supra* note 206, at 15-16; Telecommunication Regulation, *supra* note 203, arts. 56, 61.

[221] *See* Gao, *supra* note 209, at 257 (noting that the list has remained largely constant for the past twenty years).

[222] *See, e.g.*, Internet Information Service Measures, *supra* note 206, at 15.

categories are noticeably vague, which may be deliberate so as to create chilling effects and induce companies to err on the side of caution by over-censoring.[223]

On top of all this, Internet-related companies sign a public "self-disciplinary" pledge that is administered and enforced by the quasi-governmental Internet Society of China.[224] This pledge, whereby signatories commit to adopting more proactive measures for monitoring and disposing of harmful information, is nominally voluntary. However, it appears as a practical matter to be yet another requisite to operating in China.[225]

Given the sheer number of Chinese netizens, prohibited content still frequently slips through the cracks. For this reason, the government has become increasingly proactive in policing Internet content itself. The Cyberspace Administration of China (CAC), the dual state/Party entity overseen by the Xi Jinping-led Central Cyberspace Affairs Commission, functions as a coordinating body on Internet censorship, and its provincial-level offices are tasked with monitoring and demanding removal of prohibited content online.[226] China has also taken steps to heighten enforcement of Internet companies' legal obligations, granting public security bureaus broad authority to conduct random inspections where they verify, among other things, that satisfactory measures for preventing dissemination of prohibited content are in place.[227] Internet companies have very little latitude when it comes to responding to demands from Chinese authorities if they intend to retain their operating licenses. When the party-state can simply order an ISP to cut off a subscriber and they have no real choice but to comply, there is only a small amount of value to be derived from a built-in "shutoff" protocol like that shown in the New IP proposal.

4. Real-Name Registration and Record-Keeping

Next, ISPs and ICPs in China have become subject to an increasing number of subscriber/user registration and record-keeping obligations that together have greatly eroded the

---

[223] *See* Bryan Druzin & Jessica Li, *Censorship's Fragile Grip on the Internet: Can Online Speech Be Controlled?*, 49 CORNELL INT'L L.J. 369, 376 (2016) ("Indeed, the genius of this statute is that it is fantastically vague. The precise ambit of permissible speech is left unclear to encourage self-censorship and maximize the range within which people voluntarily restrain their behavior online.").

[224] Internet Soc'y China, *Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry*, CHINA DAILY (Mar. 26, 2002), *available at* https://govt.chinadaily.com.cn/s/201812/26/WS5c23261f498eb4f01ff253d2/public-pledge-of-self-regulation-and-professional-ethics-for-china-internet-industry.html.

[225] *See* CREEMERS, *supra* note 207, at 94 (noting that compliance with the pledge has become a de facto soft requirement for having one's licensing renewed.).

[226] *See* Jamie P. Horsley, *Behind the Facade of China's Cyber Super-Regulator*, STAN. DIGICHINA (Aug. 4, 2022), https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/ (providing an overview of the rapidly ascendent and equally complex Cyberspace Administration of China); *see also* Ryan Fedasiuk, *Buying Silence: The Price of Internet Censorship in China*, JAMESTOWN Found. (Jan. 12, 2021), https://jamestown.org/program/buying-silence-the-price-of-internet-censorship-in-china/ (estimating Chinese government's on expenditures on direct censorship activities); Henry L. Hu, *The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration*, 207 CHINA Q. 523, 526-27 (2011) (detailing the of use coordinated, periodic "strikes" against unlawful content carried out through ISPs even before the CAC was established).

[227] *See* Gong'an Jiguan Hulianwang Anquan Jiandu Jiancha Guiding (公安机关互联网安全监督检查规定) [*Provisions on Internet Security Supervision and Inspection by Public Security Organs*] (Promulgated by Ministry of Pub. Security Sept. 5, 2018, effective Nov. 1, 2018), art. 10, CLI.4.322375 (EN) (PKULaw).

anonymity enjoyed by Chinese netizens.[228] At the content/application level, virtually any online service that enables users to post, publish, or send information is legally required to register them using authenticated real-identity information.[229] This includes microblogs, forums, instant messaging applications, and websites with comment sections.[230] Failure to comply can lead to large fines, license forfeiture, and even secondary tort liability for acts committed by an anonymous user that the online service provider failed to properly register.[231]

As an additional layer of protection, a similar set of requirements exists at the infrastructure level. Network operators, both fixed line and mobile, are legally required to register subscribers using authentic identity information.[232] The requirement extends to Internet access offered to patrons at places of business, meaning an individual who wishes to connect to the Wi-Fi at their neighborhood Internet café must first show their government-issued ID card to be verified and recorded.[233] ISPs are further required to keep and preserve detailed records about subscribers, most notably the IP address(es) assigned to them at any given time, and to disclose this information to state authorities upon request.[234] MIIT also maintains a centralized database of IP address blocks assigned to ISPs.[235] ISPs are obligated to promptly update the database whenever this information changes.[236] The database is accessible by the public security bureaus, so that upon discovering illegal content posted by someone who is identifiable only by IP address, they know exactly to which ISP to go in order to compel disclosure of a subscriber's identity. New IP's controversial "intrinsic security" features would do little to streamline this process, as the assistance of ISPs would still be needed to decrypt an embedded identifier and provide the corresponding real-identity information.

---

[228] *See* Jyh-An Lee & Ching-Yi Liu, *Real-Name Registration Rules and the Fading Digital Anonymity in China*, 25 WASH. INT'L L.J. 1, 10-17 (2016) (examining the historical evolution of China's "real-name registration" policy).

[229] *See, e.g.*, Cybersecurity Law, *supra* note 220, art. 24; China's real-name registration policy reflects the principle of "foreground voluntary name, background real name." While users must register their legal name with the platform operator, they are still able to choose their public display name on the platform. Samm Sacks & Paul Triolo, *Shrinking Anonymity in Chinese Cyberspace*, LAWFARE (Sept. 25, 2017), https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

[230] *See id*. (discussing several regulations involving real-name registration that were released shortly after China's Cybersecurity Law took effect).

[231] *See* Rogier Creemers, *The Pivot in Chinese Cybergovernance: Integrating Internet Control in Xi Jinping's China*, 2015/4 CHINA PERSP. 10 (2015), https://journals.openedition.org/chinaperspectives/6835 [hereinafter Creemers, *Pivot in Chinese Cybergovernance*].

[232] *See, e.g.*, Cybersecurity Law, *supra* note 220, art. 24.

[233] Hulianwang Shangwang Fuwu Yingye Changsuo Guanli Tiaoli (互联网上网服务营业场所管理条例) [*Regulations on the Administration of Business Sites of Internet Access Services*] (promulgated by State Council, Sept. 29, 2002, effective Nov. 15, 2002, amended Mar. 24, 2019), art. 23, CLI.2.331350 (EN) (PKULaw). However, the thoroughness of this verification process appears to be somewhat inconsistent. It was reported in 2013 that several individuals had been regularly accessing the Internet at a café by using forged IDs that contained the name and image of U.S. President Barack Obama. *See Manager forged ID card to make "Obama" a regular at Chinese Internet café*, GLOBAL TIMES (May. 30, 2013), https://www.globaltimes.cn/content/785616.shtml.

[234] Hulianwang Anquan Baohu Jishu Cuoshi Guiding (互联网安全保护技术措施规定) [*Provisions on the Technical Measures for the Protection of the Security of the Internet*] (promulgated by Ministry of Public Security Nov. 23, 2005, effective Mar. 1, 2006), art. 8, CLI.4.73057 (EN) (PKULaw).

[235] Hulianwang IP Dizhi Beian Guanli Banfa (互联网IP地址备案管理办法) [*Measures for the Administration of IP Address Archiving*] (promulgated by Ministry of Info. Indus. Jan. 28, 2005, effective Mar. 20, 2005), art. 6, CLI.4.56965 (EN) (PKULaw).

[236] *Id*. at 9.

5. Promotion of IPv6 Deployment

China has been strongly promoting domestic IPv6 deployment for nearly two decades and has accelerated its efforts in recent years with the hope of achieving 100% adoption by 2025.[237] Some have long suspected that one of the primary motives behind China's IPv6 push is the fact that the expanded address pool would enable every device to have a globally unique identifier, making it easier to trace traffic back to its source.[238] This is because the scarcity of IPv4 addresses led to heavy reliance on Network Address Translation (NAT), which allows several devices share the same public-facing IP address and thus enjoy a degree of practical anonymity. IPv6 has no such constraints, obviating the need for NAT and enabling a one-to-one mapping between address and device.[239] Ironically, some of the discussion around China's embrace of IPv6 in the mid-2000s is closely reminiscent of that surrounding New IP. For instance, a *New York Times* article from 2006 described IPv6 as "new technical standard enthusiastically embraced by China [that] will allow greater traceability of Internet users, potentially endangering those expressing views counter to the government's."[240]

Admittedly, the impending exhaustion of the IPv4 address space and the desire to obtain first-mover advantages were likely important motivations for China's IPv6 push.[241] In any case, China has undeniably welcomed the possibilities opened up by each device globally having a globally unique identifier.[242] The development of the aforementioned SAVA, designed with IPv6 in mind, is one illustration of this.[243] Having already been implemented on one of the country's major non-commercial backbone networks, it is still undergoing improvements and appears to remain a large part of China's plans. A new working group within the IETF titled "Source Address Validation in Intra-domain and Inter-domain Networks" was established in 2022, and Chinese

---

[237] *See* Yuedong Zhang, *100% by 2025: China getting serious about IPv6*, APNIC (June 6, 2019), https://blog.apnic.net/2019/01/03/ipv6-in-china/ (highlighting some of the goals outlined in the 2017 Party/State-issued IPv6 deployment plan and subsequent progress made towards achieving them).

[238] Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 601 (2011) ("Indeed, part of China's push to deploy IPv6 is the country's desire to increase attribution and accountability online.").

[239] The ability to externally track a user by IPv6 address is largely dependent on how frequently an ISP rotates the network prefix (i.e., the assigned series of leading bits that devices then use to derive a full IPv6 address) delegated to a subscriber site. Though IPv6 privacy extensions have been designed to frequently change a device's address, all of these addresses would still have the same network prefix; where this prefix is relatively static and its length is known, the IPv6 address could be used as the basis for tracking. *See* Erik Rye et al., *Following the Scent: Defeating IPv6 Prefix Rotation Privacy*, *in* IMC'21: PROC. 21ST ACM INTERNET MEASUREMENT CONF. 739, 740 (2021), https://arxiv.org/pdf/2102.00542.pdf ("While privacy extensions protect clients when changing networks, IP-based tracking is still possible via the customer's assigned prefix.").

[240] Thomas Crampton, *Innovation may lower Net users' privacy*, N.Y. TIMES (Mar. 19, 2006), https://www.nytimes.com/2006/03/19/business/worldbusiness/innovation-may-lower-net-users-privacy.html.

[241] *See* DENARDIS, PROTOCOL POLITICS, *supra* note 74, 109-10 (discussing the history of China's IPv6 strategy and its underlying motivations); Li Weitao, *Future of the Internet begins to take shape*, CHINA DAILY (last updated Sept. 25, 2006), http://www.chinadaily.com.cn/china/2006-09/25/content_695792.htm (highlighting the opportunities presented by IPv6).

[242] *Cash for acquiescence*, GUARDIAN (Apr. 4, 2006), https://www.theguardian.com/technology/2006/apr/04/comment.china ("Hu Qiheng, chair of the Internet Society of China warmly embraced IPv6, which . . . empowers governments like China's to track down individuals who might "misbehave" online").

[243] *See supra* note 141 and accompanying text.

participants look to be heavily involved.[244] This would provide much of the same functionality as New IP's end-to-end "intrinsic security," but without the need for an entirely new protocol.

* * *

In summary, while the conventional narrative charges the CCP with wanting to fundamentally change the Internet in order to provide governments with significant control over how their citizens use it, a careful examination of the legal and technical situation reveals that the existing protocol stack already gives China much of the power needed to accomplish these goals.. It is true that China's current system is imperfect, expensive, and dependent on many non-technological forces outside the CCP's direct control.[245] Likewise, control-obsessed regimes like Beijing are not known to grow complacent with the status quo of their surveillance and censorship apparatus. Yet, as has been demonstrated throughout this Section, the type of architectural changes Chinese actors have endorsed through proposals like New IP would not represent a significant improvement over China's existing control regime.

Nor would they be an especially effective vehicle for spreading the so-called "Chinese model" around the world by giving aspiring digital-authoritarian countries tools that enable them to emulate China.[246] The effective use of such tools is dependent on, rather than a viable substitute for, China's sophisticated Internet control architecture. Consider some examples from the New IP proposal. A feature which cryptographically binds a personal identifier to all of a user's packets would be of little utility if the ISPs in a country are not already forced to preserve accurate records about subscribers' real identities and IP address assignments at all times. Similarly, a government hoping to use content-based addressing schemes (which New IP could hypothetically support in the future) as a censorship mechanism would have very limited success unless they possess the power to force the exclusive use of these schemes and the means to control cross-border Internet traffic. This censorship could otherwise be easily circumvented by accessing content the traditional way (i.e., using host-based identifiers like an IP address), especially when that content is hosted outside the country's jurisdictional reach.

More fundamentally, the premise that China threatens to increase international acceptance of authoritarianism by exporting related values through Internet infrastructure warrants greater skepticism. It appears to reflect the same type of soft-technological determinism as the United States' early "Internet Freedom" agenda that saw the Internet an unstoppable vehicle for democracy.[247] Just as the existing Internet failed to liberate China, Russia, and Iran, a cyber-sovereign Internet should be no more likely to increase the level of digital repression among governments that have not already embraced authoritarianism.[248]

---

[244] *Source Address Validation in Intra-domain and Inter-domain Networks (savnet)*, IETF (2022), https://datatracker.ietf.org/wg/savnet/about/.

[245] *See* Lee & Liu, *supra* note 228, at 26 (recognizing that real-name registration would likely be impossible to enforce without the co-operation of ISPs or other Internet companies.); Druzin & Li, *supra* note 223, at 408-09 (arguing the heavy reliance of China's Internet control regime on self-censorship and private sector enforcement, rather than direct censorship through technological measures, makes it vulnerable to collapse.).

[246] *See* Erie & Streinz, *supra* note 64, at 14-16 (casting doubt on the ability of Chinse "digital authoritarianism" to be exported because, insofar as a "China model" exists, it is enabled by set of internal power relations, state capacities, and other historically conditioned features relatively unique to China.).

[247] *See supra* note 15 and accompanying text.

[248] Jessica Chen Weiss, *A World Safe for Autocracy? China's Rise and the Future of Global Politics*, FOREIGN AFFS., July-Aug. 2019, at 92, 98; *see also* STEVEN FELDSTEIN, THE RISE OF DIGITAL REPRESSION: HOW TECHNOLOGY

This, of course, should not be construed as defense of authoritarian values or protocols that reflect these values. Nor is it a denial that China is attempting to facilitate the acceptance of cyber sovereignty around the globe. Instead, it is merely a recognition that if China is serious about spreading its alternative vision and enhancing its control capabilities, the realities of ITU-T governance and the private nature of standards adoption mean that re-inventing core Internet protocols through the global standard-setting process hardly represents a foolproof way to accomplishing those goals. The Internet architecture is, after all, just an architecture, and it can be used to support a variety of different implementations.[249] China has already demonstrated how the existing architecture can be implemented and configured in a way that enables state control while still preserving (selective) global interoperability. All of this thus strongly points to the possible existence of something more behind China's Internet standards agenda than the conventional accounts suggest.

IV. TOWARDS AN ALTERNATIVE UNDERSTANDING

If the desire for enhanced Internet control capabilities or a more state-centric standards development model cannot fully explain China's advocacy of New IP, then what does? In this Part, we explore the role that economic interests play. This is readily visible in the case of New IP. Even though components such as "intrinsic security" raised some valid concerns, other features such as deterministic QoS appear to be more than just a smokescreen to conceal ulterior purposes. These features and the sector-specific use cases to which they are tailored are better understood in light of China's long-term growth and development planning, which seeks to transform Chinese industry through the deep integration of ICTs. The remainder of Part IV will both examine how Internet infrastructure innovation fits into China's industrial policy strategy as well as another frequently overlooked consideration—the role and economic interests of Chinese companies like Huawei—in order to construct a more compelling explanation of what is driving China's standards push.

A. The Internet in Chinese Industrial Policy

One way to understand China's current campaign to evolve the Internet's architecture is as part of its lofty ambitions to transform the country into both a "cyber great power" and a modern "manufacturing power."[250] For the past decade, the highest levels of both the state and the party have repeatedly emphasized that realization of these goals depends heavily on the development of a new generation of information communication network infrastructure and capabilities. Rather

IS RESHAPING POWER, POLITICS, AND RESISTANCE 48 (2021) (arguing that although Chinese firms make digital surveillance tools available to countries at low costs, domestic factors that generate demand for these tools are the main driver of digital repression); Segal, *supra* note 96, at 88 (offering countries' growing disillusionment over issues like disinformation and security as the primary driver of this demand).

[249] David D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, 18 ACM COMPUTER COMM. REV. 106, 111 (1988) ("The Internet architecture tolerates this variety of realization by design."

[250] These are common English translations of two important buzzwords that have appeared with increasing frequency across official Chinese policy, planning, and strategy documents over the past decade. *See* Rogier Creemers et al., *Lexicon: 网络强国 Wǎngluò Qiángguó*, STAN. DIGICHINA (May 31, 2018), https://digichina.stanford.edu/work/lexicon-%E7%BD%91%E7%BB%9C%E5%BC%BA%E5%9B%BD-wangluo-qiangguo/; *制造强国 (zhizao qiangguo): Manufacturing Power*, CHINA DAILY (June 29, 2015), https://www.chinadaily.com.cn/opinion/2015-06/29/content_21128372.htm.

than shape the future direction of the Internet's architecture towards greater state control, it appears much more interested in an architecture that is conducive to achieving its industrial policy goals.[251] In fact, nearly every dimension of Huawei's New IP proposal can be traced back to some economic development priority outlined in China's state-driven planning process.

A good place to start is the Five-Year development plans that the CCC-led government has used to shape the long-term direction of the country since the 1950s by outlining economic and social goals for the next period along with high-level strategies for achieving them.[252] The Twelfth such plan was published in 2011. It heavily prioritized the continued development of China's ICT sector, identifying it as one of just a handful of "strategic emerging industries" expected to be a future driver of economic growth.[253] It also listed the improvement of China's science and technology innovation capacity as one of the main objectives for the period.[254] This was to be achieved through accelerating the transition to a predominantly enterprise-driven innovation system, increasing the support and resources available to industry, constructing major technology innovation infrastructure, and promoting breakthroughs in major areas like, inter alia, information networks.[255]

China's promotion of innovation and investment in the ICT sector is hardly a new development. It has long fallen under the rubric of "informatization" (*xinxihua*), the upgrading of social and economic processes through the application of ICTs.[256] This has been a central pillar of its development strategy for well over two decades.[257] What was new, however, was the elevated importance these goals were given.[258] The Plan was widely understood as an attempt to re-orient China's economy, shifting it away from a resource-dependent export-driven model and towards a more sustainable one fueled by indigenous innovation, specifically within emerging areas like next-generation ICTs.[259] Moreover, the plan made clear that enterprise was to play a leading role

---

[251] Designing a future Internet around the need to support future economic goals is not necessarily an unusual idea. David Clark's work studying proposed future architectures has identified and categorized some of the distinct aspirational goals underlying various proposals. Among them is one that promotes the future Internet as a "platform for innovation," serving as a driver of economic growth by enabling new applications, technology development, and the disruption of industries. *See* DAVID D. CLARK, DESIGNING AN INTERNET 288, 291 (2018).

[252] *What is China's five-year plan?*, ECONOMIST (Mar. 4, 2021), https://www.economist.com/the-economist-explains/2021/03/04/what-is-chinas-five-year-plan.

[253] Robert D. Atkinson, *ICT Innovation Policy in China: A Review*, INFO. TECH. & INNOVATION FOUND. 2 (2014), https://www2.itif.org/2014-china-ict.pdf.

[254] Zhonghua Renmin Gongheguo Guomin Jingji He Shehui Fazhan Di Shier Ge Wu Nian Guihua Gangyao (中华人民共和国国民经济和社会发展第十二个五年规划纲要) [*The Twelfth Five-Year Plan for National Economic and Social Development of the People's Republic of China*], chap. 27, CLI.1.146717 (EN) (PKULaw).

[255] *Id*.

[256] Creemers, *Pivot in Chinese Cybergovernance*, *supra* note 231, at 6.

[257] Informatization has been a crucial component of China's developmental and industrial policy since at least the late 1990s. It is on the back of this informatization agenda that Chinese leaders have pinned their hopes of "leapfrog development" through which it catches up to and eventually surpasses the industrialized West. *See* Xiudian Dai, *ICTs in China's Development Strategy*, *in* CHINA AND THE INTERNET: POLITICS OF THE DIGITAL LEAP FORWARD 8 (Christopher R. Hughes & Gudrun Wacker eds., 2003).

[258] *See* Yu Hong, *Reading the 13th Five-Year Plan: Reflections on China's ICT Policy*, 11 INT'L J. COMM. 1755, 1758-59 (2017) (stating that the status of ICTs in the 12YP was one of "unprecedented importance").

[259] *See, e.g.*, Joseph Casey & Katherine Koleski, *Backgrounder: China's 12th Five-Year Plan*, U.S.-CHINA ECON. & SEC. REV. COMM'N 3-4 (June 24, 2011), https://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf (suggesting the shift towards a steadier growth model may have been partially motivated by the 2008 financial crisis, which saw the collapse in global demand for Chinese exports, and in turn, Chinese economic growth).

in this innovation-driven economy and that the state should strengthen science and technology infrastructure in order to facilitate private innovation in key areas.[260]

Shortly thereafter, the State Council released more detailed implementation plan for carrying out a number of science and technology infrastructure construction projects pursuant to the Twelfth Five-Year Plan.[261] Among the sixteen major projects outlined was one titled "future network test facilities," a large-scale experimental network infrastructure and test environment intended to promote breakthroughs in future networks.[262] Interestingly, the State Council offers many of the same arguments here that Huawei would later use to justify New IP. It claims that the TCP/IP Internet is unable to meet the needs of future development, as emergence of technologies such as cloud computing and IoT have posed large challenges to Internet security, service quality, and mobility.[263] It is likely no coincidence that nearly a decade afterward, the experimental network testbed constructed as part of this very project was where Huawei completed large-scale testing of certain New IP-related features.[264]

The subsequent development period, marked by the issuance of 13th Five-Year Plan in 2016, saw the continuation of many key initiatives from the previous Plan.[265] Just as importantly, it was during this period that China announced Internet Plus, an initiative seeking to promote the integration of ICTs into traditional industries—manufacturing, healthcare, energy, agriculture, and finance—in order to fuel economic growth and innovation.[266] The manufacturing dimension of the Internet Plus initiative is particularly relevant, as it helps shed light on why use cases like smart

[260] ROBERT ASH, ROBIN PORTER & TIM SUMMERS, CHINA, THE EU AND CHINA'S TWELFTH FIVE-YEAR PROGRAMME 88-89 (2012), *available at* https://www.chathamhouse.org/sites/default/files/public/Research/Asia/0312ecran_ashportersummers.pdf.

[261] *China approves science infrastructure plan*, CHINA DAILY (Jan. 16, 2013), http://www.chinadaily.com.cn/china/2013-01/16/content_16127710.htm.

[262] Guojia Zhongda Keji Jichu Sheshi Jianshe Zhong Chanqi Guiha 2012-2030 Nian (国家重大科技基础设施建设中长期规划2012—2030年) [Medium and Long-Term Plan for National Major Scientific and Technological Infrastructure Construction 2012-2030], (issued by State Council Mar. 4, 2013), http://www.gov.cn/zwgk/2013-03/04/content_2344891.htm [hereinafter Medium and Long-Term Infrastructure Construction Plan]. The future network test environment that was eventually built is called the China Environment for Network Innovations (CENI) and is supported by a new high performance backbone network connecting 40 different Chinese universities. *See* Stephen Chen, *China starts large-scale testing of its internet of the future*, SOUTH CHINA MORNING POST (Apr. 20, 2021), https://www.scmp.com/news/china/science/article/3130338/china-starts-large-scale-testing-its-internet-future. Predictably, Huawei was selected as one of the primary vendors for the project and supplied much of the equipment underlying this new infrastructure. *See Jiangsu Future Networks Innovation Institute Uses Huawei's WDM Technologies to Build National Network Test Facilities in China*, HUAWEI (Aug. 29, 2019), https://e.huawei.com/se/news/ebg/2019/Jiangsu-future-network-huawei-wdm-technology.

[263] *See* Medium and Long-Term Infrastructure Construction Plan, *supra* note 262.

[264] *See* Shoushou Ren et al., *Deterministic Network Forwarding Technology*, 1 COMM. HUAWEI RSCH. 184, 193-92 (June 2022), https://www-file.huawei.com/-/media/corp2020/pdf/publications/huawei-research/2022/huawei-research-issue1-en.pdf (highlighting results of experimental verification conducted on national large-scale testbed); *see also* Yan Shen 闫屾 & Li Zhong 李忠, *Huawei New IP Jishu Shiyan* (华为 New IP 技术试验) [*Huawei New IP Technology Trial*], CENI (last visited Feb. 26, 2023), https://ceni.org.cn/406.html.

[265] *See* Hong, *supra* note 258, at 155-56.

[266] "*Internet Plus" to fuel innovation, development China unveils Internet Plus action plan to fuel growth*, XINHUA (June 4, 2015), http://english.www.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm.

manufacturing and IIoT are so prominently featured throughout the New IP proposal.[267] The Internet Plus initiative is an important component of the "Made in China 2025" plan, a long-term strategy to radically transform China's manufacturing base and move up the global value chain.[268] Made in China 2025 aims evolve Chinese manufacturing from a cheap, quantity-based model to an "intelligentized," one based on high quality.[269] China believes this can be achieved, in part, by leveraging technologies like IoT, advanced robotics, cloud computing, and big data analytics to improve manufacturing speed, quality, and efficiency.[270] The industrial Internet is the common thread connecting all of these technologies together.

Though certainly not lacking in buzzwords, China has taken concrete steps to advance this agenda. A recent National Informatization Plan published by the CAC, for instance, sets a goal of increasing "Enterprise Industrial Equipment Cloud Usage" from 13% to 30% by the end of 2025.[271] The type of fully autonomous manufacturing scenario depicted in the New IP proposals, where connected machinery is monitored and controlled by software running in a remote data center, is not all that far-fetched.[272] There are obvious risks associated with connecting Industrial Control Systems (ICS) to the public Internet, let alone moving them to the cloud. It would place a lot of pressure on networks to meet performance demands with little margin for error. From a security standpoint, it also expands the attack surfaces of these systems, introducing new pathways that malicious actors could potentially infiltrate. High-profile incidents like the Stuxnet worm and Colonial Pipeline hack illustrate the type of real-world impact that cyberattacks directed at Operational Technology can have.[273]

China seems to recognize these different risks to some extent. In 2017, the State Council issued a guiding opinion on *Deepening the Internet Plus Advanced Manufacturing*, in which it called for the acceleration of research and development into new capabilities that help meet the need for secure, low-latency, and highly reliable industrial networks.[274] Among the specific areas into which it directs intensified research efforts are Deterministic Networking, "heterogeneous

---

[267] Internet Plus is even explicitly referenced in initial New IP contribution that Huawei submitted to the ITU-T. *See* TSAG-C83, *supra* note 6 ("The combination of datamation and manufacturing industries, or 'Internet+', will bring a great deal of benefit to human society.").

[268] *See* Scott Kennedy, *Made in China 2025*, CTR. STRATEGIC & INT'L STUD. (June 1, 2015), https://www.csis.org/analysis/made-china-2025 (summarizing Made in China 2025); Jost Wübbeke et al., *Made in China 2025: The making of a high-tech superpower and consequences for industrial countries*, 20 (MERICS Papers on China, No. 2, Dec. 2016), https://merics.org/sites/default/files/2020-04/Made%20in%20China%202025.pdf (explaining the relationship between Internet Plus and Made in China 2025).

[269] *See* Zhongguo Zhizao 2025 (中国制造2025) [*Made in China 2025*] (issued by State Council July 7, 2015), *translated in* CTR. SEC. & EMERGING TECH. 5 (Mar. 8, 2022), https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf.

[270] *See id*. at 11-14 (outlining tasks for promoting the "deep integration of informatization and industrialization," one of the key points of the plan).

[271] Rogier Creemers et al., *Translation: 14th Five-Year Plan for National Informatization*, STAN. DIGICHINA (Jan. 24, 2022), https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

[272] *See, e.g.*, TSAG Tutorial, *supra* note 113, at 7; Li, *Market Opportunities*, *supra* note 114, at 8.

[273] *See generally* David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM, Mar. 2013, at 48; Andy Greenberg, *The Colonial Pipeline Hack Is a New Extreme for Ransomware*, WIRED (May 8, 2021), https://www.wired.com/story/colonial-pipeline-ransomware-attack/.

[274] *See* Guowuyuan Guanyu Shenhua Hulianwang+ Zianjin Zhizao Ye Fazhan Gongye Hulianwang De Zhidao Yijian (国务院关于深化"互联网+先进制造业"发展工业互联网的指导意见) [*Guiding Opinions of the State Council on Deepening the "Internet Plus Advanced Manufacturing" and Developing the Industrial Internet*] (promulgated by State Council Nov. 19, 2017, effective Nov. 19, 2017), § III, CLI.2.305507 (EN) (PKULaw).

identifier interoperability," and—most emphatically—measures for providing strong "security guarantees," all of which happen to be major elements of the New IP proposal.[275] Thus, while much of what China envisions here is extremely ambitious—often to the point of being overzealous—there is little doubt these aspirations have informed the type of future Internet capabilities reflected in New IP.

B. The Role of China's Oft-Forgotten "Private" Sector

Given the extent to which discussions of New IP have revolved around the Chinese government, it becomes easy to forget that it was in fact Huawei that conceived and led the initiative. This tendency to overlook the role and interests of the Chinese firms participating in SDOs also manifests itself in the wider debate over China's growing engagement in ICT standards development. Of course, we would be remiss not to acknowledge the legitimate questions surrounding the level of independence these firms enjoy from the party-state and whether it is fair to consider them as belonging to the private sector.[276] Huawei and its mysterious ownership structure are certainly no exception.[277] Yet, as long as Chinese firms like Huawei have a profit motive, there is strong reason to believe they are more than mere agents of the party-state and are responsive to the myriad of economic incentives they face in the standard-setting arena.[278]

There are indeed many economic interests at stake in the outcome of the standardization process. As Janet Abbate explains, these "technical decisions can have far-reaching economic and social consequences, altering the balance of power between competing businesses or nations."[279] Firms that are successful in shaping a standard are often able to translate this into a significant competitive advantage.[280] There is also a prestige factor, as having a standard endorsed by an SDO can signal a firms' market leadership and/or capacity to innovate. A popular saying among Chinese policymakers states that "third-tier companies make products, second-tier companies make technology, and first-tier companies make standards."[281] The CCP has strong aspirations for China to be a country of first-tier companies and has shown a willingness to provide domestic firms with the financial support and incentives necessary to achieve this. Hence, Chinese firms are not only subject to the same commercial incentives that have historically driven the engagement of their Western counterparts, but additional carrots dangled by the party-state provide all the more reasons to pursue influence over shaping technical standards.

Beyond the firm-specific economic interests at play, the different groups of industry actors involved in the Internet standard-setting process—network operators, hardware vendors, application providers, etc.—have their own collective interests.[282] The ongoing conflict between the various groups vying to maximize their interests and move up the network value-chain has

---

[275] *See id.*

[276] *See* Erie & Streinz, *supra* note 64, at 53-61 (examining the relationship between Chinese MNCs, SOEs, and the party-state).

[277] *See also* Raymond Zhong, *Who Owns Huawei? The Company Tried to Explain. It Got Complicated*., N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html.

[278] *See* Erie & Streinz, *supra* note 64, at 55.

[279] ABBATE, *supra* note 74, at 179.

[280] *See* Stanley M. Besen & Joseph Farrell, *Choosing How to Compete: Strategies and Tactics in Standardization*, J. ECON. PERSP., Spr. 1994, at 117, 124-25 (explaining that firms will often prefer different standard candidates despite having an interest in compatibility because it would give them an advantage over rivals).

[281] Seaman, *supra* note 54, at 14; Neaher et al., *supra* note 71, at 6; Russel & Berger, *supra* note 54, at 12.

[282] *See* David D. Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, 13 IEEE/ACM TRANSACTIONS NETWORKING 462 (2005).

come be known as "the tussle."[283] This tussle can be seen playing out in the case of New IP. Huawei's proposal was interested in shifting the Internet architecture towards a more intelligent network core, thereby securing a greater opportunity for equipment vendors to add and capture value at a time when their role has been steadily diminishing.

Though Huawei is perhaps best known for its wireless access network equipment, it is also one of the world's leading vendors of core routers, switches, and other specialized appliances (i.e., "middleboxes"). It is important to understand that New IP was proposed against a backdrop in which network hardware has grown increasingly commoditized. This trend is largely due to the emergence of technologies like virtualization, which enable different network tasks traditionally bound to specialized hardware to instead be performed at the software-level on cheaper general-purpose hardware or more centrally in the cloud.[284] Insofar as the TCP/IP model even afforded opportunities for hardware vendors like Huawei to add value to the network, these opportunities have been slowly eroding away along with their margins. This has led major vendors scrambling for new potential revenue streams.[285]

Through New IP, Huawei is counteracting this trend by adding greater complexity to the network, shifting many of the functions for meeting application-specific needs from the endpoints to the core.[286] Huawei frequently draws on the analogy of private courier services, which have been upgraded with a number of enhancements for package delivery that were not available with traditional postal services.[287] This includes the ability to customize the speed or method of delivery as well as to track and receive confirmation of delivery as a means of verifying that special requirements were met.[288] Recognizing that customers have been willing to pay more for value-added services in the package delivery context, Huawei hails New IP as the long-awaited introduction of these enhancements to network services.[289]

While Huawei views New IP as the network equivalent of FedEx, others have instead made comparisons to older "virtual circuit" technologies like Asynchronous Transfer Mode (ATM), which emerged as a potential challenger to the TCP/IP stack in the 1990s.[290] ATM networks are

---

[283] *Id*.

[284] *See generally What is Software-Defined Networking (SDN)?*, VMWARE (last visited, Feb. 26, 2023), https://www.vmware.com/topics/glossary/content/software-defined-networking.html; *VNF and CNF, what's the difference?*, REDHAT (last updated July 28, 2022), https://www.redhat.com/en/topics/cloud-native-apps/vnf-and-cnf-whats-the-difference.

[285] *See, e.g.*, Himanshu Agarwal et al., *Hardware's business-model shift: Finding a new path forward*, MCKINSEY (Mar. 3, 2021), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/hardwares-business-model-shift-finding-a-new-path-forward (noting that Cisco has responded to the trend of hardware commoditization by expanding its portfolio into the software space).

[286] See Geoff Huston, New IP and emerging communications technologies, APNIC (May 25, 2020), https://blog.apnic.net/2020/05/25/new-ip-and-emerging-communications-technologies/ (placing New IP in the same category as other past initiatives that were motivated by vendors and operators' desire to add value and a refusal to "accept their role as a commodity utility").

[287] Li, *Market Opportunities*, *supra* note 114, at 24-25; Li et al., *New IP Data Packet Framework*, *supra* note 112, at 4.

[288] Li et al., *New IP Data Packet Framework*, *supra* note 112, at 4.

[289] *See* Richard Li et al., *Qualitative Communication for Emerging Network Applications with New IP*, *in* PROC. 17TH INT'L CONF. ON MOBILITY, SENSING & NETWORKING (MSN 2021) 628, 629-30 (2021), https://doi.org/10.1109/MSN53354.2021.00096 ("With New IP, the network services become customizable, trackable, assurable, and billable at the packet level.").

[290] *Id*. at 630; *see also* Alain Durand, New IP 28 (ICANN Off. Chief Tech. Officer, OCTO-017, October 27, 2020), https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf ("Better-than-best-effort networking appears to suggest a return to circuit-switched technology, harking back to ATM days."); Huston, supra note 286.

connection-oriented, meaning they establish a dedicated virtual path before any data is transmitted. The use of such virtual circuits, which can exist on a permanent basis or be set up on demand, allows for the reservation of dedicated resources that can provide QoS guarantees (not unlike *IntServ*).[291] ATM networks take an active role in flow and congestion control in order to ensure these guarantees can be met. The upshot of this approach is that much more sophisticated and hence expensive core network hardware is required to operate at scale. Cost was a major reason that the host-oriented model of TCP/IP over Ethernet largely prevailed over ATM.[292] Huawei seems to be betting that this time around, enhanced features will be more economically viable due to the combination of increased demand from emerging use cases and the massive strides made in hardware/software since the 1990s.

One factor that may be working in its favor is the expanding market for its products in developing countries, something being facilitated by China's DSR initiative.[293] DSR countries, a large share of which are located in the Global South, tend to lack well-developed digital infrastructure and jump at the opportunity to help modernize their economies. In Africa, for example, Huawei has been contracted by several governments to carry out the construction of national fiber optic backbone or wireless broadband networks, projects financed with concessional loans from Chinese state-owned development banks.[294] As a result, many African countries have become heavily reliant on Huawei equipment in both their fixed and wireless networks.

There are strong indications that Huawei intends to push similar "value-added" network features in DSR countries. In the Fall of 2022, it co-released a whitepaper with the African Telecommunications Union on IPv6 Development in Africa.[295] The whitepaper promotes something called "IPv6 enhanced," a collection of IPv6 feature extensions and network operation and management tools that help enable capabilities like deterministic QoS, low latency transmission, and ultra-high bandwidth.[296] A consequence of adopting more complex, vendor-specific network technologies—those in which networked applications become more tightly coupled to the network itself—is that it becomes increasingly challenging to migrate to alternatives in the future. It can thus lead to a type of path dependence or vendor lock-in, giving Huawei a much more durable hold on these markets in the future. As digital ecosystems within DSR countries begin to take shape around Huawei's network solutions, it may become very difficult for competing vendors to ever win them back.

---

[291] See claffy & Clark, *supra* note 118, at 222 (explaining that a main impetus behind *IntServ* was the ongoing development of ATM and concerns over TCP/IP's future were it unable to support similar functionality).

[292] Durand, *supra* note 290, at 28.

[293] *See* Erie & Streinz, *supra* note 64, at 50-53; Greene & Triolo, *supra* note 63 (maintaining that as DSR countries look to expand their digital infrastructure, Chinese tech companies "will enjoy significant state support" to help meet this demand).

[294] Alan Weissberger, China (led by Huawei) in bid to take over Africa's telecom networks, IEEE ComSoc: Tech. Blog (Aug. 14, 2021), https://techblog.comsoc.org/2021/08/14/china-led-by-huawei-in-bid-to-take-over-africas-telecom-networks/; see also Motolani Agbebi, China's Digital Silk Road and Africa's Technological Future, Council on Foreign Rels. (February 1, 2022), https://www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf3, (displaying a list of African telecom infrastructure construction projects Huawei has been involved in over the last decade).

[295] *ATU, African Union & Huawei Release Africa IPv6 Development White Paper*, HUAWEI (Nov. 14, 2022), https://blog.huawei.com/2022/11/14/atu-african-union-huawei-release-africa-ipv6-development-white-paper/.

[296] African Telecomm. Union & Huawei, Africa IPv6 Development White Paper 5-6 (2022), https://e.huawei.com/za/material/networking/6706d69e17564b10bb2ac87498e633b9; *see also infra* Section IV Part B for a more complete discussion on "IPv6 enhanced."

IV. CHINA'S RISE AND THE FUTURE OF THE GLOBAL INTERNET

The trojan horse narrative leads to a number of predictions about the consequences of failing to address the threat posed by China, ranging from an eventual ITU Internet takeover to the bifurcation of cyberspace into two separate Internets that reflect the new multipolar world order. Having made a case against the common understanding of what motivates China's desire to shape Internet standards, we now turn to another fascinating question: what might China's emergence in this sphere *really* hold in store for the global Internet? In this Part, we explore the future implications of this trend as it pertains to three areas: the ITU's involvement in Internet governance activities, China's role in shaping the Internet's technical architecture, and the possibility of a global "splinternet,"

A. Internet Governance Activities at the ITU

In the planning process leading up to the most recent World Telecommunication Standardization Assembly (WTSA-20), the event at which ITU-T study group activities for the next period are approved, several proposed study topics related to New IP failed to gain approval.[297] As we point out in Part III, ITU-T's adherence to consensus-based decision-making made this predictable. However, this outcome also reaffirms something that has been evident for some time: that the ITU's threat to Internet governance has been overstated. Despite claims that authoritarian states like Russia and China have made advances in the ITU,[298] the easy defeat of New IP provides a stark reminder of just how much of an uphill battle these countries face.

It is important to recognize this, as claims that the ITU is attempting to take over the Internet are hardly new and will likely resurface again in the future. This takeover narrative rears its head every few years when some major event transforms the ITU into a battleground for competing visions of governance with the fate of the Internet allegedly hanging in the balance. Previous iterations include: the ITU's bid to inherit responsibility for managing the Internet's namespace prior to the establishment of Internet Corporation for Assigned Names and Numbers (ICANN) in the late 1990s,[299] a renewed push to take control over these functions just a few years later at the World Summits on Information Society (WSIS),[300] the proposed revisions to the International Telecommunications Regulations (ITRs) at the World Conference on International Telecommunications (WCIT) convened in Dubai in 2012,[301] and the efforts to advance a number

[297] *See* SG13 December 2020 Meeting Report, *supra* note 177, at 4. Also note that WTSA-20 was postponed due to the COVID-19 pandemic and did not take place until March 2022. However, the planning process took place according to the originally scheduled timeline.

[298] *See, e.g.,* Freedom House, *supra* note 167, at 3 ("Diplomats from China and Russia have made inroads at institutions like the International Telecommunication Union (ITU), seeking to transform the United Nations agency into a global internet regulator that advances authoritarian interests"); THE NEW BIG BROTHER, *supra* note 10, at 44 (citing China's "ushering in of the proposed New IP" as evidence that its strategy to leverage its influence at multilateral institutions like the ITU has been successful).

[299] *See* Wolfgang Kleinwachter, *Beyond ICANN vs. ITU? How WSIS Tries to Enter the New Territory of Internet Governance*, 66 GAZETTE: INT'L J. COMM. STUD. 233, 235–240 (2004) (recalling early attempts by the ITU to assume control of managing the DNS).

[300] MUELLER, NETWORKS AND STATES, *supra* note 36, at 55-60 (providing a history of WSIS, the ITU-led multi-phase summit through which a number of participating states took aim at ICANN and its relationship with the U.S.).

[301] *See* Robert M. McDowell, *The U.N. Threat to Internet Freedom*, WALL ST. J. (Feb. 21, 2012), http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html (arguing revisions to the ITRs could result in giving the U.N. "unprecedented powers over the Internet").

of proposals related to the Distributed Object Architecture, an alternative system of Internet identifiers purported to be ideal for IoT and that would be administered by a body under the auspices of the ITU.[302]

The example that is particularly instructive here is that of the 2012 WCIT, which involved ITU member states contemplating updates to the treaty-level ITRs. Some of proposed revisions submitted by countries like Saudi Arabia and Russia led commentators to sound the alarm over what they perceived to be a government-led power grab. Vint Cerf, one of the Internet's founding fathers, testified before Congress that the outcome of WCIT risked "a fundamental shift in how the Internet is governed."[303] Likewise, then-FCC commissioner Robert McDowell penned a *Wall Street Journal* op-ed warning the WCIT threatened to give the U.N. "unprecedented powers over the Internet."[304] Fortunately, this never materialized, as less than half of all member states ultimately signed a watered-down version of the updated ITRs.[305]

Yet, even in the leadup to WCIT, many respected voices from the Internet governance and policy realm recognized the ITU's threat to Internet governance had been inflated.[306] They correctly pointed out that the ITU lacked the power to simply assume regulatory control over the global Internet through a majority vote. In reality, the ITU had no real power of its own. The power to regulate the Internet within a country's borders resides exclusive with national governments, and insofar as the ITU has any ability to dictate how this power is exercised, it is because governments have voluntarily agreed to be bound by treaty instruments like the ITRs. Those who objected to the new ITRs could simply choose not to sign and ratify them, which is precisely what ended up happening.[307] Far from a power grab, these voices instead characterized WCIT as an attempt by the ITU to remain relevant amid a changing technological landscape.

The ITU's fading relevance, especially in the standardization sector, is arguably one reason why authoritarian countries have repeatedly sought an expanded role for it within Internet governance. The organization is, in many ways, a vestige of an era in which public telecommunications networks existed as state-owned or regulated monopolies, making an intergovernmental body the most natural standardization venue. Yet, the technology environment has evolved, markets have liberalized; new venues have emerged; and the subject matter within ITU-T's expert remit (i.e., circuit-switched telephony) has been relegated to legacy status. Authoritarian countries have recognized that ITU-T is an organization in search of a purpose and

---

[302] *See* Robert M. McDowell & Gordon M. Goldstein, *The Authoritarian Internet Power Grab*, WALL ST. J. (Oct. 25, 2016), https://www.wsj.com/articles/the-authoritarian-internet-power-grab-1477436573 (arguing the DOA is a strategic attempt by countries like China to take "centralized control" over the IoT).

[303] *See, e.g.*, Violet Blue, *WCIT-12 leak shows Russia, China, others seek to define "government-controlled Internet,"* ZDNET (Dec. 8, 2012), https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/.

[304] *International Proposals to Regulate the Internet: Hearing Before the Subcomm. on Comm. and Tech., H. Comm. on Energy & Comm.*, 112th Cong. 80 (2012) (statement of Vinton Cerf), https://www.govinfo.gov/content/pkg/CHRG-112hhrg79558/html/CHRG-112hhrg79558.htm.

[305] *See* McDowell, *supra* note 301.

[306] *See, e.g.*, Jack Goldsmith, *WCIT-12: An Opinionated Primer and Hysteria-Debunker*, LAWFARE (Nov. 30, 2012), https://www.lawfareblog.com/wcit-12-opinionated-primer-and-hysteria-debunker; Milton Mueller, *ITU Phobia: Why WCIT was derailed*, INTERNET GOVERNANCE PROJECT (Dec. 18, 2012), https://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

[307] *See* Anthony Rutkowski, *Saying No to the ITRs*, CIRCLEID (Dec. 05, 2012), https://circleid.com/posts/20121205_saying_no_to_the_itrs (arguing there are no real adverse consequences of not acceding to the new ITRs).

have sought to take advantage of it.[308] However, what is crucial is that none of these attempts have succeeded, nor do these countries appear to have made any significant inroads in gaining international support for an expanded ITU mandate.

This is unlikely to change anytime soon, a fact further reinforced by two recent developments. The first is the 2022 "Declaration for the Future of the Internet," a statement issued by a U.S.-led partnership of sixty (mostly) democratic countries reaffirming their commitment to upholding a free and open global Internet and the multistakeholder model of governance.[309] The declaration itself does little more than endorse a set of aspirational principles that are entirely non-binding on signatories. At the very least, however, it does send a message that there exists a coalition that is willing to defend multistakeholderism, a reminder of the opposition that those interested in pushing Internet governance functions to the ITU that their efforts will likely face.[310]

The other major development was the election of a new ITU Secretary-General at the 2022 Plenipotentiary Conference. It was effectively a two-candidate race between Rashid Ismailov, a Russian telecom official and former Huawei executive, and the United States' Doreen Bogdan-Martin, a thirty-year veteran of the ITU who received strong backing from the Biden Administration.[311] The election earned coverage from several mainstream media outlets, where it was heralded as "the most important election in the history of the Internet"," and a clash between two competing visions that would determine the fate of the net's future.[312] Fortunately, this latest iteration of the ITU Internet takeover narrative, like those before it, never came to be. The American candidate prevailed in a landslide to become the first female Secretary General in the institution's long history.[313] Although it is not certain how much of an upper hand (if any) a Russian victory would have given countries seeking to use the ITU to expand state control over the Internet, the election of Bogdan-Martin makes any such takeover all the more difficult.

The purpose of calling attention to the exaggerated threat of the ITU is not to suggest that developments taking place within it can be safely ignored without consequence. Even post-New IP, there continues to be a steady inflow of proposed standardization work at ITU-T that, if fully developed and implemented, has the potential to be highly disruptive to the technical foundation of the Internet and the established systems for managing its critical resources. One such example is a Chinese-led work item in ITU-T Study Group 13 titled "Decentralized Trustworthy Network

---

[308] Anthony Rutkowski, *Privatizing the ITU-T: Back to the Future*, CIRCLEID (Aug. 17, 2012), https://circleid.com/posts/20120816_privatizing_the_itu_t_back_to_the_future ("The problem with an intergovernmental organization without a purpose is that it becomes a venue of mischief.").

[309] *See generally* WHITE HOUSE, A DECLARATION FOR THE FUTURE OF THE INTERNET (April 28, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf.

[310] Some have suggested that the intended target of the Declaration were the signatory countries who had been drifting away from the democratic vision of cyberspace, not those like Russia or China who reject it outright. Alex Engler, *The Declaration for the Future of the Internet Is for Wavering Democracies, Not China and Russia*, LAWFARE (May 6, 2022), https://www.lawfareblog.com/declaration-future-internet-wavering-democracies-not-china-and-russia. While this may be true, it does not change what is being signaled to countries like China and Russia.

[311] *Meet the Candidates*, ITU NEWS MAG., Sept. 2020, at 10, 11-18, *available at* https://www.itu.int/pub/S-GEN-NEWS-2022-4.

[312] *See, e.g.*, *Michael Morell, This obscure election will decide the fate of the open internet*, WASH. POST (Sept. 28, 2022), https://www.washingtonpost.com/opinions/2022/09/28/un-international-telecommunication-union-election/; *An election that could make the global internet safer for autocrats*, ECONOMIST (Sept. 20, 2022), https://www.economist.com/international/2022/09/20/an-election-that-could-make-the-global-internet-safer-for-autocrats.

[313] Press Release, Int'l Telecomm. Union [ITU], Member States Elect Doreen Bogdan-Martin as ITU (Sept. 29, 2022), https://www.itu.int/en/mediacentre/Pages/PR-2022-09-29-ITU-SG-elected-Doreen-Bogdan-Martin.aspx.

Infrastructure" (DNI).[314] It proposes a permissioned blockchain network that would support decentralized management of the Internet's global name and address spaces.[315] The blockchain network's nodes, which only organizations like regional and national Internet registries would be eligible to run, approve transactions (e.g., an address block assignment or domain name transfer) through some sort of consensus process and write it to a distributed, immutable ledger.[316] This blockchain-oriented solution would effectively displace the existing regime for managing these activities currently led by ICANN. A draft recommendation defining requirements and a high-level framework for DNI reached the "last call" stage of ITU-T's Alternative Approval Process in late 2021. This draft would have been approved were it not for substantive issues raised by UK delegates to ITU-T.[317] The draft must now go up for additional review at a future Study Group meeting, where it will struggle to gain final approval.

The DNI example illustrates the risks of neglecting ITU-T entirely. Although its approval would not have brought the dream of replacing ICANN with the blockchain much closer to reality, it would have still allowed a controversial idea to gain further legitimacy and momentum, increasing the likelihood that it become a source of unnecessary conflict in the future. Proposals like this should be expected to continue until there is a serious re-evaluation of certain ITU-T study groups, their mandates, and the need for their continuation. While a push to scale-back activities at ITU-T is something on which the United States' delegation should strongly consider taking the lead, they and other like-minded Member States need to remain vigilant for the time being.

Instead of encouraging disengagement from the ITU, the reason we highlight the exaggerated nature of its threat to Internet governance is to caution against it turning into a distraction. Myopically focusing on each new high-profile iteration of the recurring "ITU Internet takeover" cycle—growing to expect threats towards Internet values like openness and freedom to come from the actions of authoritarian challengers in Geneva—makes it very easy to overlook what is arguably a more formidable set of threats: the slow retreat from these values by liberal democracies. Indeed, many that have historically championed Internet freedom and openness have recently taken actions out of line with these values. A non-exhaustive list may include: the United States' flirtation with bans on popular Chinese apps,[318] the EU's ongoing development of a public DNS resolver service with built-in filtering of unlawful content,[319] and the UK's proposed Online

---

[314] Though DNI is concerned with the Internet's supporting infrastructure (i.e., the DNS, PKI, etc.), whereas New IP focuses on protocol innovation at the network layer, the two still appear to be loosely related. Huawei has been the driving force behind both initiatives and even identifies some of the same problems DNI is intended to address in its New IP submissions to the ITU-T. *See* TSAG Tutorial, *supra* note 113, at 10.

[315] Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Draft new Recommendation ITU-T Y.2086 (formerly Y.DNI-fr): "Framework and Requirements of Decentralized Trustworthy Network Infrastructure" - for consent*, at 9, SG13-TD613/WP3 (July 16, 2021), https://www.itu.int/md/T17-SG13-210716-TD-WP3-0613.

[316] *Id*. App. I.

[317] *Y.2086: Framework and Requirements of Decentralized Trustworthy Network Infrastructure*, ITU-T AAP (last accessed Feb. 26, 2023), https://www.itu.int/t/aap/recdetails/10055.

[318] *See* Paul Rosenzweig, *The WeChat and TikTok Bans Show the U.S. No Longer Stands for Internet Freedom*, SLATE: FUTURE TENSE (Sept. 28, 2020), https://slate.com/technology/2020/09/tiktok-wechat-icann-dns-internet-freedom.html; Bobby Allyn, *Trump Signs Executive Order That Will Effectively Ban Use of TikTok in the U.S.*, NPR (Aug. 6, 2020), https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s.

[319] *See* Markus Reuter, *EU will eigenen DNS-Server mit Filterlisten und Netzsperren* [*EU wants own DNS-Server with filter lists and blocking*], NETZPOLITIK.ORG (Jan. 24, 2022), https://netzpolitik.org/2022/dns4eu-eu-will-eigenen-dns-server-mit-filterlisten-und-netzsperren/; Geoff Huston, *Some Thoughts on DNS4EU – the European Commission's Intention to Support the Development of a New European DNS Resolver*, CIRCLEID,

Safety Bill that many warn would severely undermine online free expression.[320] Whereas the ITU is limited in its power to regulate the Internet, national governments are not. Thus, if one is truly concerned threats to the free and open Internet, they would be wise to broaden their sights beyond the ITU, as these developments are just as likely to come from Brussels, European capitals, or D.C. as Geneva.

B. Internet Evolution in China

As illustrated in Part IV, China has identified a number of future Internet capabilities it sees as necessary for supporting its long-term strategic objectives and has taken major steps to facilitate enterprise-driven innovation in these areas. Given their overall importance to its vision, China is not simply going to abandon the pursuit of these capabilities simply because Huawei's New IP proposal—one of many possible ways to achieve them—was unsuccessful. Some type of Internet architecture evolution, whether it be a clean slate design or merely a set of enhancements, will inevitably come out of China in the coming years. Although there are strong hints as to what this evolution may look like, it is still somewhat undetermined.

The most likely candidate at present is something called "IPv6+" (or "IPv6 enhanced"), which has been promoted by both China's CAC and MIIT as well as fully embraced by Huawei following the demise of New IP.[321] IPv6+ and New IP share many of the same functional goals (e.g., network determinism) which has led some to conclude IPv6+ is a simply a re-packaged version of New IP after the latter failed to catch on at the ITU.[322] Yet, there are significant differences between the two, the most notable being that IPv6+ is not actually a protocol itself. The name is rather misleading, as IPv6+ is just a buzzword the Chinese are using to denote a variety of IPv6-compatible technologies already being developed at places like the IETF.[323]

There is a growing amount of evidence suggesting that IPv6+ is indeed a large part of China's future Internet plans. As mentioned above, it is being actively pushed by major state and Party organs. In 2021, the CAC and MIIT jointly issued a notice on accelerating IPv6 deployment efforts which established the goal for China to become a driving force behind global IPv6+

---

https://circleid.com/posts/20220213-some-thoughts-on-dns4eu-new-european-dns-resolver; *Europe: Content moderation at infrastructure level must respect human rights*, ARTICLE 19 (Mar. 9, 2022), https://www.article19.org/resources/europe-content-moderation-at-infrastructure-level-must-respect-human-rights/ (highlighting some of the concerns presented by DNS4EU project proposal).

[320] *See also* Joe Mullin, *The UK Online Safety Bill Attacks Free Speech and Encryption*, ELECTRONIC FRONTIER FOUND. (Aug. 5, 2022), https://www.eff.org/deeplinks/2022/08/uks-online-safety-bill-attacks-free-speech-and-encryption; *UK: House of Lords must reject the Online Safety Bill*, ARTICLE 19 (Jan. 30, 2023), https://www.article19.org/resources/uk-house-of-lords-must-reject-the-online-safety-bill/.

[321] *See IPv6 Enhanced Paves the Way for IP on Everything*, HUAWEI (Apr. 26, 2022), https://www.huawei.com/en/news/2022/4/has-ipv6-ip-on-everything.

[322] See, e.g., Luca Bertuzzi, China rebrands proposal on internet governance, targeting developing countries, Euractiv (June 6, 2022), https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/.

[323] One of the major IPv6+ technologies is Segment Routing over IPv6 (SRv6), a type of source routing that allows the network to better steer traffic by selecting a pre-determined path and embedding it into the packet header. IPv6+ also includes DetNet, the architecture developed by the IETF Deterministic Networking Working Group for ensuring minimal packet loss and bounded latency. For a complete list of component technologies *see IPv6+*, IPV6PLUS.NET (last accessed Feb. 26, 2023), https://www.ipv6plus.net.

technology by the year 2025.[324] The same notice calls for strengthening domestic IPv6 research and standardization activities as well as increasing the participation of Chinese actors in the formulation of IPv6-related international standards.[325] Here, it identifies two particular standards bodies by name: the European Telecommunications Standards Institute (ETSI) and the IETF.[326] Not coincidentally, of the new Internet Drafts submitted to IETF working groups that are home to IPv6+ technologies, a large percentage feature authors affiliated with companies like Huawei, ZTE, and China Mobile.[327] In fact, Chinese participation in the IETF has been increasing in general.[328] In terms of total submissions, 2022 was the most active Chinese authors have ever been within the organization.[329] The progress made within the IETF was even emphasized in a recent whitepaper issued by China's State Council Information Office.[330] Chinese actors continue to inch towards matching the contribution level of those from the United States, something difficult to imagine just a decade ago.

Given that criticisms of the New IP proposal included its top-down design approach, potential redundancy, lack of interoperability, and the venue it was presented at, one might think IPv6+ would be a welcome development. However, it has not managed to avoid its own share of controversy. In 2020, Huawei successfully pushed for a new working group on "IPv6 enhanced innovation" to be established within ETSI, one of the two standards body explicitly referenced in China's IPv6 strategy. The working group, which aimed to promote and support implementation of IPv6+ technologies developed at the IETF, quickly became one of the largest within ETSI in terms of active participants.[331] Yet, despite the group's ostensible popularity, concerns about IPv6+'s connection to Huawei and New IP persisted. When the working group was set to expire and requested an extension, it encountered strong opposition and was not allowed to continue.[332] It was further reported that the European Commission (EC) "played a decisive role" in

[324] Zhongyang Wangluo Anquan He Xinxi Hua Weiyuanhui Bangongshi Guojia Fazhan He Gaige Weiyuanhui, Gongye He Xinxi Hua Bu Guanyu Jiakuai Tuijin Hulianwang Xieyi Di Liu Ban (IPv6) Guimo Bushu He Yingyong Gongzuo De Tongzhi (中央网络安全和信息化委员会办公室、国家发展和改革委员会、工业和信息化部关于加快推进互联网协议第六版(IPv6)规模部署和应用工作的通知) [Notice by the Office of the Central Cyberspace Affairs Commission, the National Development and Reform Commission, and the Ministry of Industry and Information Technology of Accelerating the Extensive Deployment and Application of Internet Protocol Version 6 (IPv6)] (issued July 7, 2021) CLI.4.5054538 (EN) (PKULaw).

[325] *Id*.

[326] *Id*.

[327] The examples are too numerous to list here. To see for oneself, the ipv6plus.net website, *supra* note 323, includes links to several related IETF Internet Drafts or RFCs for each IPv6+ feature listed. Virtually all of these were either authored or co-authored by individuals affiliated with Chinese entities.

[328] *See* Nanni, *supra* note 72, at 2358 (finding a general increase in participation by Chinese actors—particularly Huawei—in select IETF working groups examined).

[329] *Internet-Draft and RFC statistics*, IETF (last accessed Feb. 26, 2023), https://datatracker.ietf.org/stats/document/yearly/country/.

[330] *See* SCIO, Shared Future in Cyberspace, *supra* note 87, § III.

[331] *See* Will Liu, *ETSI ISG IPE: Off to a good start*, ETSI (May 19, 2021), https://www.etsi.org/newsroom/blogs/technologies/entry/etsi-isg-ipe-off-to-a-good-start (showing a graphical list of IPE working group participants); Latif Ladid, *ETSI IPv6 Enhanced innovation (ISG IPE) starts PoC activities at IPE#08*, ETSI (Sept. 30, 2022), https://www.etsi.org/newsroom/blogs/technologies/entry/etsi-ipv6-enhanced-innovation-isg-ipe-starts-poc-activities-at-ipe-08 (reporting it had surpassed 100 participants at last meeting).

[332] Luca Bertuzzi, *Controversial European working group on internet governance faces shutdown*, Euractiv (Dec. 1, 2022), https://www.euractiv.com/section/digital/news/controversial-european-working-group-on-internet-governance-faces-shutdown/.

coordinating this opposition.[333] This is significant, as it came just a few months after the EC released a new EU standardization strategy that was allegedly motivated by growing concerns over Chinese influence at international standards venues.[334]

Since all signs point towards continued growth in Chinese involvement in the IETF, politically motivated resistance to contributions from Huawei and other Chinese actors could have severe unintended consequences. It is understandable why the CCP's role in actively promoting this trend may make some given its less than stellar human rights record. We do not mean to suggest that stakeholders should disregard the political dimension of standard-setting or abdicate their responsibility for ensuring protocols are compatible with certain values like respect for human rights. Protocol designs with the objective or probable consequence of curbing civil liberties should obviously be resisted, even if only to avoid condoning or being complicit in the erosion of online freedoms. However, the New IP saga demonstrates that there is a tendency in the West to project fears of China's techno-authoritarianism and growing influence—fears which alone are not necessarily unfounded—onto Chinese technologies and standards when the evidence does not support it.

Adopting a combative response to the trend of increased Chinese engagement would have damaging effects on the legitimacy of venues like the IETF and would lend credence to the CCP's claims that incumbent multistakeholder Internet governance bodies exist only to serve Western interests. This is especially the case where opposition is promoted by policymakers. As former IETF Chair Alissa Cooper astutely observed in recent congressional testimony, such efforts could have the effect of "undermining the successful industry-led standardization system, fragmenting standards development into silos, and diminishing the influence of U.S. companies in global organizations."[335] So in short, Internet protocol evolution does appear to be coming to China, and the response of Western actors at venues like the IETF may greatly influence where and how that evolution takes shape.

C. The Prospect of a "Splinternet"

Those who pay attention to the ongoing discussions in the technology law and policy sphere have likely heard something by now about the worrying trend of Internet fragmentation. A recent report published by the Council on Foreign Relations, for example, declared that the "era of the global Internet is over" and that the global Internet is becoming irreversibly fragmented.[336] In a similar vein, former Google CEO Eric Schmidt predicted in 2018 that an emergent China would lead to the creation of "two distinct Internets": the existing Western-centric Internet and a Chinese-led alternative that will come to dominate Asia.[337] Indeed, one of the concerns

[333] *Id*.

[334] Jorge Valero & Alberto Nardelli, *EU Seeks to Counter China's Influence Over Global Standards*, BLOOMBERG (Feb. 1, 2022), https://www.bloomberg.com/news/articles/2022-02-01/eu-seeks-to-counter-china-s-influence-over-global-standards.

[335] *Setting the Standards: Strengthening U.S. Leadership in Technical Standards, Hearing Before the Subcomm. Rsch. & Techn. of the H. Comm. Sci., Space, & Tech.*, 117th Cong. (Mar. 17, 2022) (statement of Alissa Cooper), https://www.congress.gov/117/meeting/house/114508/witnesses/HHRG-117-SY15-Wstate-CooperA-20220317.pdf.

[336] COUNCIL ON FOREIGN RELS., CONFRONTING REALITY IN CYBERSPACE: FOREIGN POLICY FOR A FRAGMENTED INTERNET 7 (May 2022), https://www.cfr.org/report/confronting-reality-in-cyberspace.

[337] Lora Kolodny, *Former Google CEO predicts the internet will split in two — and one part will be led by China*, CNBC (Sept. 20, 2018), https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html.

surrounding New IP was its potential to precipitate this exact type of scenario.[338] Yet, the prospect of a true Chinese-led "splinternet," in which the country secedes from the global Internet to form an incompatible alternative, remains extraordinarily unlikely.

Given the inconsistent meanings attached to terms like "fragmentation" and "balkanization" as they frequently appear in the Internet context, it is crucial first to distinguish some important concepts. As Milton Mueller observes in his book *Will the Internet Fragment?*, if fragmentation is understood as the state of being separated into parts that are distinct from the whole, then the Internet has always been fragmented.[339] The Internet, as explained earlier in Part II, is a network of networks; it is a consists of thousands of independent autonomous systems—each with their own rules, policies, and configurations—interconnected through their ability to speak the same universal language at the network layer (IP) and the assistance of supporting global infrastructure like the DNS.[340]

A corporate network, for example, may be configured to block traffic to social media websites to ensure employees are being productive while on the clock. At a more macro level, data flows may rarely leave a country's national borders due to localization requirements and/or technical controls implemented at international gateways like China's. Similarly, Internet search results displayed to users in one country or geographic region may be hidden from users in another, such as those de-linked pursuant to EU's Right to Be Forgotten.[341]

In the scenarios above, the way the Internet is experienced by users—the content available to them and where they retrieve it from—varies significantly. However, the underlying architecture remains capable of universal interconnection; the only thing preventing the free flow of information is some entity, whether it be a government or private company, deciding to place a barrier in the way. This type of fragmentation is thus conceptually distinct from the type that involves the Internet breaking into separate parts that are *incapable* of interoperating due to technical incompatibilities. The latter type has occasionally been referred as *technical fragmentation* to better capture the distinction.[342]

Although the two types of fragmentation are frequently conflated, the distinction matters. This softer variety of fragmentation, perhaps more appropriately conceptualized as the Internet growing increasingly *federated*, is undoubtedly a growing trend that is undesirable in many cases. However, the impact of the harder, technical form of fragmentation is much more severe, and the

---

[338] *See, e.g.*, Hoffman et al., *Standardising the Splinternet*, *supra* note 13, at 23 (arguing "decentralised internet infrastructure," a group of Chinese technologies the authors lump New IP in with, could "enable countries to decouple or disconnect from the current global internet"); Lauren Dudley, *Part Three: Huawei's Role in the China-Russia Technological Partnership*, COUNCIL ON FOREIGN RELS.: NET POLITICS (Dec. 16, 2020), https://www.cfr.org/blog/part-three-huaweis-role-china-russia-technological-partnership (arguing New IP could further promote "the bifurcation of the global technological system"); Flavia Kenyon, *China's "splinternet" will create a state-controlled alternative cyberspace*, GUARDIAN (June 3, 2021), https://www.theguardian.com/global-development/2021/jun/03/chinas-splinternet-blockchain-state-control-of-cyberspace.

[339] MILTON MUELLER, WILL THE INTERNET FRAGMENT?: SOVEREIGNTY , GLOBALIZATION AND CYBERSPACE 21-22 (2017) [hereinafter MUELLER, WILL THE INTERNET FRAGMENT?].

[340] *Id.* at 24.

[341] *See generally* Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, (Sept. 24, 2019) (judgment) (limiting the territorial scope of the EU's right to be forgotten to within the EU's borders).

[342] WILLIAM DRAKE ET AL., INTERNET FRAGMENTATION: AN OVERVIEW 4 (World Econ. F., Future of the Internet Initiative White Paper, 2016), http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

forces preventing it from happening are also much stronger.[343] When commentators raise concerns over long-term potential for a Chinese-precipitated "splinternet," this is typically the type of fragmentation to which they are alluding, as the other type of fragmentation already exists to an extreme degree with China's Internet. Yet, there is strong reason to doubt China will attempt a hard break from the global Internet any time soon.

Even if China were to push domestic adoption of a new Internet protocol suite that, by default, was incompatible with TCP/IP, the incentive to develop a mechanism for bridging the protocols (e.g., a translation gateway) would be near-overwhelming.[344] This is because completely isolating itself from the global Internet would cause China a great deal of self-inflicted economic damage. It is not just the global Internet it would be decoupling itself from but also the entire digital economy that operates on top of it.[345] Despite the restrictiveness of its Internet, China has become increasingly integrated into the global digital economy. Chinese firms in digital markets such as cloud services, e-commerce, and social media have gradually expanded their global reach.[346] Look no further than ByteDance, the Beijing-based parent company of TikTok, which, albeit controversial, has amassed a user base of over 100 million in the United States alone.[347]

A hard break from the global Internet would also be completely antithetical to long-term strategic initiatives like DSR. At the center of these are promoting digital interconnectedness and expanding the international presence of its digital national champions.[348] Even with aid and generous financing, the Chinese would have a difficult time persuading countries to adopt digital infrastructure incapable of interoperating with most of the world. It is conceivable that, at some point in the distant future, DSR countries will have become so deeply integrated into China's digital ecosystems and dependent on Chinese infrastructure that they would have no choice but to join China in breaking away from the global Internet.[349] This would make a splinternet more economically tolerable for China, as the loss of positive network externalities from migrating to a separate, smaller Internet would not be as drastic. Until then, however, a hard break from the global Internet would be prohibitively costly for China and should remain so for the foreseeable future.

China's Great Firewall and restrictions on information flows already come at a significant economic opportunity cost, one that it has been willing to accept in exchange for greater domestic security, stability, and control. The tradeoff here represents a tension that has become one of the most important themes in Chinese technology and industrial policy.[350] While unfettered access to information via the Internet risks weakening the Party's grip over China, so too would completely

---

[343] MUELLER, WILL THE INTERNET FRAGMENT?, *supra* note 339, at 30.

[344] *Id*. at 62-63; *see also* Paul A. David & Julie Ann Bunn, *The Economics of Gateway Technologies and Network Evolution: Lessons from Electricity Supply Industry*, 3 INFO. ECON. & POL'Y 165, 197 (1988) (explaining that the economic significance of ex ante incompatibilities between network technologies can be mitigated through the use of gateway technologies).

[345] U.N. Conf. on Trade & Dev., *Digital Economy Report 2021*, 114 U.N. Doc. UNCTAD/DER/2021 (Sept. 29, 2021), https://unctad.org/system/files/official-document/der2021_en.pdf [hereinafter UNCTAD Report] (noting that Internet fragmentation and digital economy fragmentation would be "joint processes").

[346] *See* Longmei Zhang & Sally Chen, *China's Digital Economy: Opportunities and Risks* 4-6 (IMF Working Paper, No. 2019/016, 2019), https://www.imf.org/-/media/Files/Publications/WP/2019/wp1916.ashx.

[347] Alex Sherman, *TikTok reveals detailed user numbers for the first time*, CNBC (July 24, 2020), https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html.

[348] *See* Erie & Streinz, *supra* note 64, at 48; UNCTAD Report, *supra* note 345, at 112.

[349] Henry Farrell & Abe Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, 44 INT'L SEC. 42 45 (2019) (referring to the leverage possessed by states that are the "hubs" of asymmetric economic and technological networks as "weaponized interdependence").

[350] *See, e.g.*, Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 86, at 107.

walling the Country off from the rest of the digital world. It is widely recognized that the legitimacy of CCP rule rests largely on its continued ability to deliver economic growth.[351] Even though China has historically given greater weight to stability and security-related concerns, it still recognizes the need to delicately balance these with the goals of economic modernization and the development of its technology sector. President Xi Jinping has characterized these two sets of oft-conflicting priorities as "two wings of a bird."[352] There is thus little reason to believe China would abruptly change course and become willing to completely sacrifice one such wing in favor of the other. This is precisely what it would be doing by splintering from the global Internet in favor of an isolated, authoritarian alternative.

CONCLUSION

China is an authoritarian-leaning country with a substandard human rights record. It engages in widespread surveillance and censorship of its citizens in both the physical world and, as illustrated in Part III, the digital one. Its idealized version of the Internet technical architecture—were it possible to re-design it from scratch without costs or other constraints—likely looks different from what is currently in place. It may even reflect and reinforce values most would deem repressive.

However, this does not necessarily mean every technology or technical standard originating from China is aimed at advancing these values. The New IP proposal, though questionable in both its technical merits and practicality, was not necessarily a trojan horse intended to expand state control of the Internet or embed authoritarianism into its architecture. Parts of the proposal raise legitimate concerns, namely its intrinsic security features, but these do not appear to be an integral part of New IP and should not be mistaken for its true aim. Instead, China has spent the last decade heavily investing in and promoting innovation into the exact type of future network capabilities proposed by New IP in order to support its long-term industrial policy objectives. Likely recognizing that such capabilities strongly aligned with its business interests—particularly the capabilities demanded by future business-critical industrial use cases like deterministic QoS—Huawei simply seized the opportunity being dangled in front of it.

It is important to recognize that New IP may be only the beginning of China's push for evolution of the Internet's technical architecture. Contrary to some predictions, this trend is not a harbinger of an impending Chinese-led "splinternet." Quite the opposite, in fact, as China has been promoting increased involvement at traditional Internet standards bodies like the IETF. This should come as no surprise; it would be naïve to expect the country with the most Internet users and a rapidly growing ICT sector to sit idly by while others continue to shape such vital technologies.

The way stakeholders and policymakers respond to this trend will have significant implications for U.S. technological leadership in the business arena. Some have called for building coalitions to counter Chinese influence at places like the ITU as well as for an increased governmental role in coordinating U.S. contributions at international standards bodies to increase

[351] *See, e.g.*, G. John Ikenberry, The Rise of China and the Future of the West, 87 Foreign Affs. 32 (2008) ("State power today is ultimately based on sustained economic growth, and China is well aware that no major state can modernize without integrating into the globalized capitalist system."); Joseph Nye Jr., Power and Interdependence with China, Wash. Q., Jan. 2020, at 7, 12 ("The legitimacy of the Chinese Communist Party depends heavily upon economic growth, and Chinese economic growth increasingly depends upon the internet.").

[352] *Xi Jinping leads Internet security group*, XINHUA (Feb. 27, 2014), https://www.chinadaily.com.cn/china/2014-02/27/content_17311358.htm.

competitiveness relative to China.[353] These approaches are unlikely to succeed and may even harm the model of standards development that made the Internet a historic success. While important to keep a watchful eye on ITU-T, resources would be better spent in pushing to scale down the sector and the many study groups whose work is duplicative, receives little attention in the marketplace, and/or falls outside the ITU's expert remit.

Just as importantly, Chinese actors are going to be increasingly active at primarily industry-led venues such as the IETF, and not every proposal they bring to the table has an ulterior motive beyond the obvious commercial incentives. Instead of trying to orchestrate a unified front for combatting China's growing role, a more constructive response for policymakers would be to increase their focus on targeted investment and policies that promote U.S. participation at these venues and cultivate the type of innovation that naturally translates to standards competitiveness. This is the surest way to see that system by which Internet standards have historically been developed, and the United States' leadership thereof, are both preserved going forward.

[353] *See supra* note 18; *see also* Brett Schaefer & Danielle Pletka, *Countering China's Growing Influence at the International Telecommunication Union*, HERITAGE FOUND. (Mar. 7, 2022), https://www.heritage.org/global-politics/report/countering-chinas-growing-influence-the-international-telecommunication; *see also, e.g.*, U.S.-CHINA ECON. & SEC. REV. COMM'N, 2020 REPORT TO CONGRESS 537 (Dec. 2020), https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf.