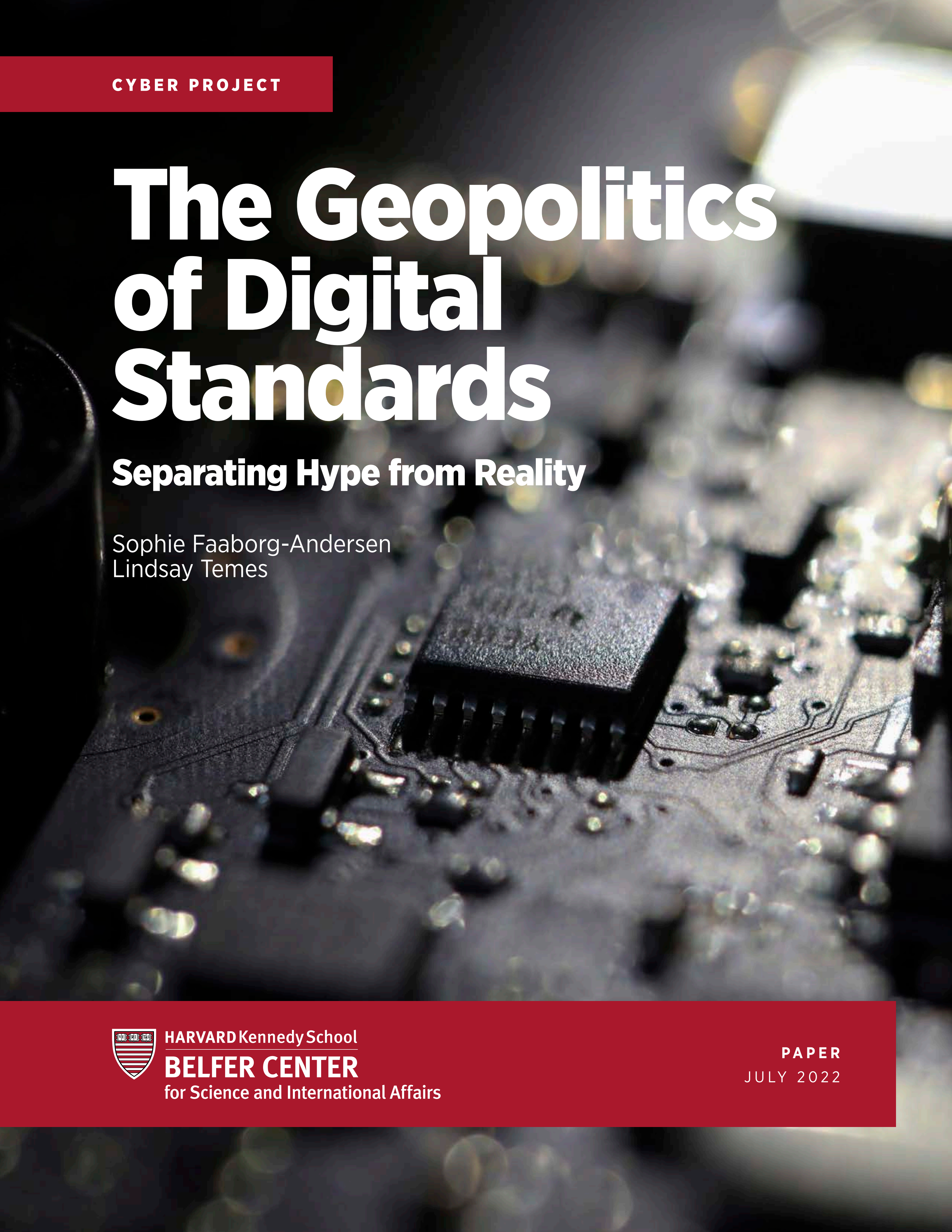
CYBER PROJECT



The Geopolitics of Digital Standards

Separating Hype from Reality

Sophie Faaborg-Andersen
Lindsay Temes

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JULY 2022

Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

http://www.belfercenter.org/cyberproject

Statements and views expressed in this report are solely those of the author(s) and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

CYBER PROJECT

The Geopolitics of Digital Standards

Separating Hype from Reality

Sophie Faaborg-Andersen
Lindsay Temes

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JULY 2022

About the Authors

Sophie Faaborg-Andersen is a Master of Public Policy candidate at Harvard Kennedy School and Young Leader Fellow at the Belfer Center for Science and International Affairs focusing on issues at the intersection of technology and national security. Sophie concurrently works as an analyst at The MITRE Corporation.

Lindsay Temes is a 2022 graduate of Harvard Kennedy School and an MBA candidate at MIT Sloan School of Management. Before graduate school, Lindsay served on active-duty with the United States Air Force and continues her service in the Air Force Reserve.

About the Cyber Project

Forty years ago, an interdisciplinary group of Harvard scholars—professors, researchers and practitioners—came together to tackle the greatest threat of the Cold War: the fear of a nuclear exchange between the Soviet Union and the United States. Today, the Belfer Center's Cyber Project seeks to recreate that interdisciplinary approach to tackle a new threat: the risk of conflict in cyberspace.

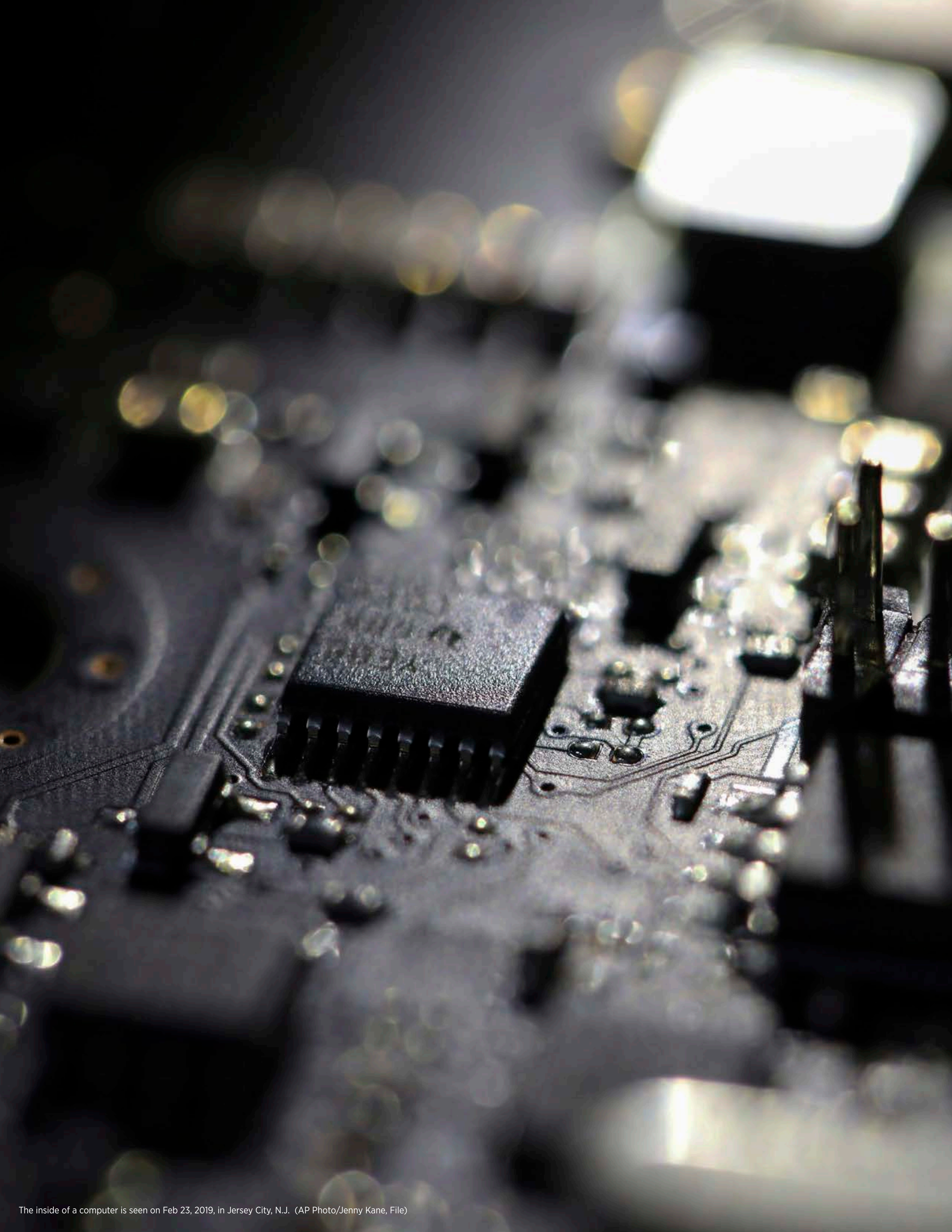
The problems that confront today's leaders are substantial and diverse: how to protect a nation's most critical infrastructure from cyber attacks; how to organize, train, and equip a military force to prevail in the event of future conflict in cyberspace; how to deter nation-state and terrorist adversaries from conducting attacks in cyberspace; how to control escalation in the event of a conflict in cyberspace; and how to leverage legal and policy instruments to reduce the national attack surface without stifling innovation.

The Cyber Project provides rigorous and policy-relevant study of these and related questions.

Acknowledgments

We would like to thank the following external reviewers, all of whose comments substantially improved the report: Lauren Zabierek, James Waldo, Calvin Nobles, Julia Voo, Samuel Visner and Winnona DeSombre.

Table of Contents



The inside of a computer is seen on Feb 23, 2019, in Jersey City, N.J. (AP Photo/Jenny Kane, File)

Executive Summary

Digital standards are the established norms that guide the development of digital technologies to ensure interoperability across products—international digital trade, commerce, and communication would not function seamlessly without them. These standards are in many ways as important as the software and hardware they underpin, from industrial control systems that allow utility operators to connect generation with distribution to the infrastructure that makes the internet work. In addition to providing product frameworks, digital standards help ensure transparent and safe applications of technologies and enable coordinated interoperability across manufacturers.

Long the domain of engineers and developers, digital standards have increasingly become the subject of strategic policy debate. In addition to lowering barriers to trade and costs to companies and consumers, standards define the normative evolution of the internet and digital world.[1] As digital technologies are increasingly embedded in all aspects of society, these technical specifications are difficult to separate from core values and principles. The technical, economic, and social implications of digital standards represent a strategic mode of extending geopolitical reach across domains, placing them at the core of emerging technology governance structures.

China's emergence as a peer technology competitor and increased presence in global standard-setting bodies has raised concerns among policymakers on both sides of the Atlantic. Many of these concerns are legitimate, especially in the context of divergent worldviews about the values that should guide the development and use of the global internet. Indeed China's state-led model of standards-setting and overall approach to digital governance architecture stands in stark contrast to the traditionally market-led and more open models adopted by the United States and European Union. The United States' current approach, characterized by market-led

[1] Lozada, Patrick, Tim Rühlig, and Helen Toner. "The Chinese Involvement in International Technical Standards: A DigiChina Forum." The Stanford Cyber Policy Center, 6 Dec. 2021. https://digichina.stanford.edu/work/chinese-involvement-in-international-technical-standards-a-digichina-forum/.

development of digital standards, is not sufficiently robust to confront the proliferation of a new brand of digital authoritarianism that could jeopardize the open nature of the global internet that exists today.

Yet the world of digital standards is vast, with equally complex implications when Chinese and other national or commercial players are involved. A new approach should prioritize U.S. involvement based on the extent to which digital standards-setting activities inhibit or advance global security, commercial, and human rights interests. **The United States should reverse its current hands-off approach to digital standards development and focus on what specific standards-setting activities are likely to impact U.S. strategic interests in the immediate, medium, and long term**. Toward the goal of developing a technically informed strategy for digital standards, policymakers must:

1. **Increase technical literacy within the policymaking community** to distinguish and prioritize standards across infrastructure, protocol, and application layers of the internet.
2. **Facilitate greater public and private sector participation in multi-stakeholder standards bodies** through federally funded training and stipends.
3. **Develop a clear picture of which digital standards that oppose U.S. strategic interests and values are being adopted by global markets** by filling existing data gaps regarding digital standards implementation across technology sectors and geographies.

This brief outlines what digital standards are and how the United States, European Union, and China approach standards development. It examines the implications of China's efforts to advance a new model of cyber sovereignty through its "New IP" proposal to illustrate that overhauls of existing infrastructure-level standards are unlikely, but foreshadow the changing nature of standards from a historically apolitical domain to one of geopolitical importance. Finally, it offers considerations for the development of a long-term strategy that focuses on technology areas of strategic interest to the U.S. at the application layer through targeted regulations that promote a free, open, and democratic internet while maintaining a clear and technically informed understanding of what is likely to change (and what is not) at the infrastructure level.

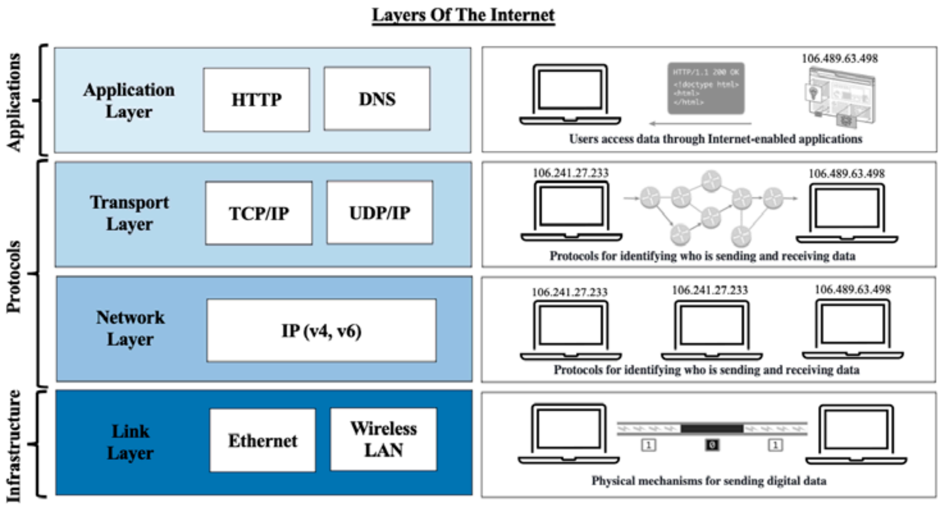
Digital Standards Today

What Are Standards and Why Do They Matter?

A growing literature describes the ways in which state censorship and powerful commercial interests are pulling the global network into distinct "internets" characterized by divergent worldviews with respect to privacy, cybersecurity, and state control. Despite increased attention to this "balkanization" of the internet, there is little consensus about which parts of the internet are fragmenting and to what degree these processes should be of concern.

The internet can be broadly thought of as consisting of three layers—**infrastructure**, **protocols**, and **applications**. Digital standards, including technical, web, and mobile standards, must be thought of in the context of which layer of the internet they support. Infrastructure is the physical hardware used to connect computers and users and forms the foundation for connectivity. This includes both global infrastructure in the form of undersea cables that transmit data through light traveling along silicon tubes as well as private infrastructure such as domain name servers (DNS) that provide low-level functionality required for computers to communicate. But the internet also includes protocols that sit on top of the physical infrastructure layer to connect users via their Internet Service Providers (ISPs). These protocols are an agreed upon set of steps that computers follow in order to communicate with each other. The top layer is the application layer, composed of services such as Facebook and Google that run on the previous two layers of the internet and allow users to send and receive data.

Figure 1. A Simplified Model of the Layers of the Internet[2]



Because digital standards function in distinct ways and with unique dependencies at each layer, it is important not to confuse these different layers when talking about setting standards to "govern the internet." **Technical standards** guide the development and deployment of infrastructure that powers the internet by allowing interoperability between hardware—including copper and fiber optic cables that run underground and along the ocean floor—and software from different sources. One of the most common technical standards is the Transmission Control Protocol and Internet Protocol (TCP/IP), which is the accepted blueprint for how data travels along hardware routes and is interpreted by receiving devices. In its most basic form, TCP/IP is a set of protocols that governs how data is broken down into packets, which are routed through a network and then reconstituted such that they are readable to the receiving user. **Web standards** are the technical specifications governing the World Wide Web ensuring content is accessible across devices on a network. These standards include commonly used languages for sharing structured information, such as HyperText Markup Language (HTML) and Extensible Markup Language (XML). Lastly, **mobile standards**, such as 5G, guide the development of mobile communication networks and their integration with mobile operators.

[2] Diagram inspired by Khan Academy. This diagram and analysis presents a subsection of the standard OSI model of the internet stack, which identifies seven layers: physical, data link, network, transport, session, presentation, and application layers.

How and Where Are Standards Set?

Technical standards are developed at the domestic and international levels with varying approaches adopted by different countries. While digital standards are commonly accepted benchmarks, they are generally voluntary and consensus-driven. There is no formalized global standards enforcement mechanism. However, standards serve as a basis for regulation in the United States and in other nations, such as China, as a regulatory tool where some standards are compulsory. Today, digital technical standards are established by a variety of **standards development organizations (SDOs)** that are either multilateral (composed of states) or multi-stakeholder (composed of a mix of industry, government, civil society, and academic representatives).

The Internet Engineering Task Force (IETF) is the leading international internet standards body that develops voluntary internet standards, such as those that make up TCP/IP. Since its founding in 1986, the IETF has been instrumental in shaping the majority of the internet's key networking protocols. Made up of researchers, academics, and engineers, the IETF has no formal country-level representation and instead operates through a multi-stakeholder model based on "rough consensus"—rather than formal voting, each working group chair decides when proposals have reached a sufficient majority of support.[3] Web and mobile standards are set by industry-led groups, such as the **World Wide Web Consortium** (W3C), and country-led groups, including the **International Organization for Standardization** (ISO). Similarly, the **International Telecommunication Union** (ITU), a multi-national UN body composed of three units, is charged with developing standards in internet connectivity (ITU-T) and radio and spectrum systems (ITU-R) as well as policies to support developing countries (ITU-D).

[3] ten Oever, Niels, and Kathleen Moriarty. "The Tao of IETF." IETF, 8 Nov. 2018, https://www.ietf.org/about/participate/tao/.

U.S., EU, and China Standards Policies

What is the United States' Standards Policy?

Historically, the United States' approach to standards-setting has been decentralized, characterized by a preference for industry-led and multi-stakeholder participation. Unlike many countries, the United States' standards engagement is coordinated by a private entity—the American National Standards Institute (ANSI)—composed of companies, industry associations, and other smaller SDOs. ANSI plays a crucial role in engaging the private sector to ensure synergy across standards bodies and educating the public on the importance of standards. It also publishes the annual United States Standards Strategy, which emphasizes "consensus, openness, and transparency" in a sector-based approach to standardization.[4]

Due to the strength of the U.S. innovation ecosystem and widespread adoption of American technologies globally, American engineers and developers have led multi-stakeholder SDOs like W3C and IETF. Within technical standards, the U.S. has a lead in participation in the IETF by percentage of attendees (51.64%) followed by the EU (20.10%) and China (6.64%).[5] American engineers also contribute the greatest number of proposals (69.86%) followed by China (16.71%).[6] While IETF supporters argue that more American proposals are adopted because they are more technically sound, critics view this multi-stakeholder approach as an anarchic wielding of political and commercial interests. Further, the exclusion of non-Western nations through rough consensus favors incumbent, well-connected, and typically American engineers.

[4] 2020 United States Standards Strategy." ANSI, American National Standards Institute, 9 Dec. 2020, https://ansi.org/resource-center/publications-subscriptions/usss.

[5] Number of Attendees for IETF 88 per Country." IETF Datatracker, Internet Engineering Task Force, https://datatracker.ietf.org/stats/meeting/88/country/.

[6] Arkko, Jari. Distribution of RFCs According to the Countries of Their Authors, 7 June 2022, https://www.arkko.com/tools/recrfcstats/d-countrydistr.html.

What is the European Union's Standards Policy?

In February 2022, the EU published a new standards strategy prioritizing a digital EU single market that ensures the development of future services that reinforce democratic values.[7] However, in contrast to the United States' private sector-led approach to standardization, the European Union has maintained a public-private partnership between the standards community consisting of private companies, non-profit organizations, and the European Commission. Historically, this partnership was defined as a bottom-up, industry-led approach to standards-setting with a reinforcing regulatory framework enforced by the Commission.[8]

While the private sector still develops standards in the EU, only one standards body is licensed within a specific sector in each country, and national standards that contradict accepted European standards are invalidated.[9] The Commission can request the development of standards to support regulation. However, these standards are not compulsory if implemented and still allow the market to determine ultimate adoption. This is in contrast to the U.S., where numerous competing standards bodies issue standards in the same sector, and adoption is determined purely by the market.

What Is China's Standards Policy?

China's digital strategy is broadly informed by the concept of cyber sovereignty—the idea that the government of a sovereign state should have the right to exercise control over the internet within its borders. To that end, China has invested heavily in digital standards over the past decade in an approach characterized by strategic alignment of technology investment,

[7] European Commission. "Factsheet - Standardisation: Supporting Europe's assertive global role." 2 Feb. 2022. https://ec.europa.eu/docsroom/documents/48602.

[8] Rühlig, Tim. "The Rise of Tech Standards Foreign Policy." February 3rd, 2022. https://dgap.org/en/research/publications/rise-tech-standards-foreign-policy.

[9] European Commission. "New approach to enable global leadership of EU standards." 2 Feb. 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661.

state-directed participation in SDOs, and a mass increase in the number of standards proposed by Chinese stakeholders.

The recently released China Standards 2035 strategy document—which sets the PRC's standards agenda for the next decade—calls for aligning standards within countries participating in China's state-subsidized regional development strategy known as the BRI and strengthening standardization dialogue between the BRICS (Brazil, Russia, India, China, and South Africa) countries.[10] In addition to providing economic benefits to Chinese companies whose intellectual property is baked into accepted standards, alignment across regional initiatives could result in Chinese technology becoming the de facto standard in countries undertaking BRI projects. This form of technology lock-in has the potential to enhance support for Chinese-backed proposals within relevant multi-lateral SDOs.[11]

China Standards 2035 also calls for a greater role for Chinese industry in supporting the development of state-led standards. Chinese companies are both coerced and incentivized to support Chinese proposals in industry-led bodies, even when technologically inferior.[12] Anecdotal evidence from standards industry participants and formalized subsidy programs describe financial incentives offered by the Chinese government to companies that propose standards adopted by SDOs and bonuses paid to representatives who secure leadership positions across working groups.[13, 14]

These incentives, coupled with China's rising technology prowess, have resulted in a significant increase in Chinese participation in standards-setting activities. At home, the Chinese state has issued over 300 national standards

[10] The Chinese Communist Party Central Committee and the State Council Publish the 'National Standardization Development Outline.'" [中共中央 国务院印发《国家标准化发展纲要》, 8 Nov. 2021. Center for Security and Emerging Technology. (Original work published 10 Oct. 2021, Xinhua News Agency). https://cset.georgetown.edu/publication/the-chinese-communist-party-central-committee-and-the-state-council-publish-the-national-standardization-development-outline/.

[11] McGeachy, Hilary. "US-China Technology Competition: Impacting a Rules Based Order https://www.ussc.edu.au/analysis/us-china-technology-competition-impacting-a-rules-based-order.

[12] Hersey, Frank. "Lenovo Founder in Public Backlash for 'Unpatriotic 5G Standards Vote.'" TechNode, 7 June 2020, https://technode.com/2018/05/16/lenovo-huawei-5g/.

[13] Bruer, Alexandra, and Doug Brake. Mapping the International 5G Standards Landscape and How It Impacts U.S. Strategy and Policy. Information Technology and Innovation Foundation, 8 Nov. 2021, https://itif.org/publications/2021/11/08/mapping-international-5g-standards-landscape-and-how-it-impacts-us-strategy/.

[14] McGeachy, Hilary. US-China Technology Competition: Impacting A Rules-Based Order. United States Studies Centre, 2 May 2019, https://www.ussc.edu.au/analysis/us-china-technology-competition-impacting-a-rules-based-order.

related to cybersecurity over the past several years.[15] Abroad, these strategies have resulted in rising Chinese leadership positions across SDOs, including the ITU, where China chaired twice as many standards focus groups as the United States in 2018.[16] A common criticism of China's engagement in standards bodies is the tendency to circumvent international standards bodies such as the IETF that might challenge technical shortcomings of proposals in favor of UN bodies such as the ITU, where China has more political influence.[17]

China's New IP

While China has and continues to expend significant resources on shaping global standards in emerging technology spaces such as 5G and AI, it views internet infrastructure standards as a core element of its digital foreign policy.[18] Policymakers are increasingly paying attention to China's role in standards bodies following efforts by Huawei and other Chinese stakeholders to standardize an alternative internet protocol (IP), known as New IP. Introduced to the ITU in 2019, New IP proposes a fundamental restructuring of the internet. While details on exactly how the IP would work are largely unpublicized, the concept involves replacing the current model of an open internet running the same standards and protocols in every country with a new approach wherein each country creates its own version of the internet subject to state-defined controls. These controls would require individuals to register to use the internet.

The United States and other proponents of the current decentralized internet model have voiced concerns surrounding New IP's potential to provide

[15] Sacks, Samm. "New China Data Privacy Standard Looks More Far-Reaching than GDPR." Critical Questions, Center for Strategic and International Studies, 29 Jan. 2018, https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.

[16] Montgomery, Mark, and Natalie Thompson. "What the U.S. Competition and Innovation Act Gets Right About Standards." Lawfare, The Brookings Institution, 13 Aug. 2021, https://www.lawfareblog.com/what-us-competition-and-innovation-act-gets-right-about-standards.

[17] Montgomery, Mark, and Theo Lebryk. China's Dystopian "New IP" Plan Shows Need for Renewed US Commitment to Internet Governance. Just Security, 18 May 2021, https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/.

[18] Murgia, Madhumita, and Anna Gross. Inside China's Controversial Mission to Reinvent the Internet. Financial Times, 27 Mar. 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.

state control and surveillance, enabling shutting off individual access to the internet and degrading privacy and free speech. Chinese and other stakeholders, such as those from Saudi Arabia, Russia, and Iran view the current internet infrastructure as lawless, with regulation controlled by private and largely American companies.[19] Huawei claims that it is focused on technological requirements for the evolving digital world and maintains that New IP's top-down reorientation would address speed and quality concerns with the current TCP/IP standard by offering higher data rates and shorter communication delays.[20]

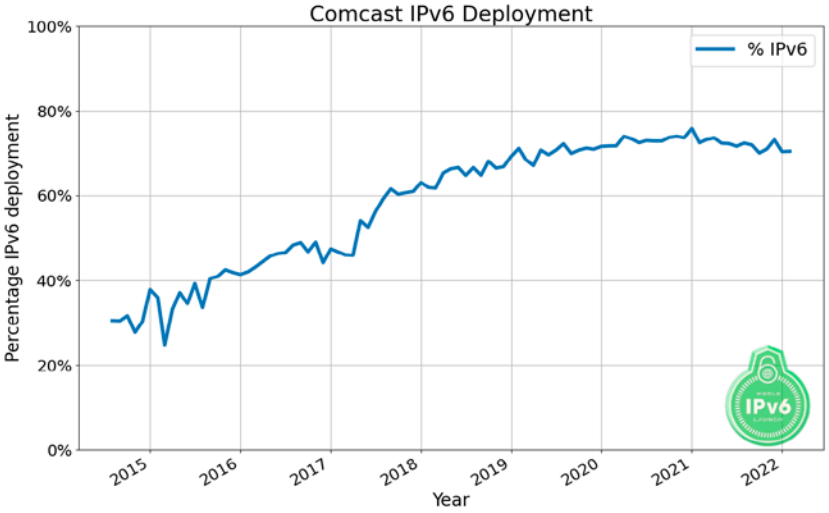
How Likely Is a New IP Protocol?

While discussions of changes to technical infrastructure such as New IP are concerning, **such changes are unlikely to materialize in the immediate to near term**. A new IP protocol would be prohibitively costly, requiring all existing IP-based infrastructure to be replaced or run in parallel to the new IP. History offers compelling nuance to this discussion. In 1998, there was a push by the IETF to update the existing internet protocol—known as Internet Protocol Version 4 (IPv4)—to handle the growth of the internet and to meet security needs. The resulting Internet Protocol Version 6 (IPv6) was the output of technical engineers collaborating to improve the existing TCP/IP infrastructure. Despite carrier networks and ISPs beginning to deploy IPv6 on their networks, the transition to IPv6 is only approximately halfway complete after more than twenty years. This example serves as a reminder that changes at the infrastructure level, even when layered on top of existing and well-developed capabilities, are slow.

[19] Murgia, Madhumita, and Anna Gross. Inside China's Controversial Mission to Reinvent the Internet. Financial Times, 27 Mar. 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.

[20] Jiang, Sheng. "New IP Networking for Network 2030," 2019. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf.

Figure 2. Adoption of IPv6 Protocol by Comcast, the Largest ISP in the United States (2015–2022)[21]



While the United States, United Kingdom, and European Union have advocated for greater regulatory authority in the technology sector, New IP represents a radical overhaul of existing underlying architecture.[22, 23] It would be exceptionally difficult to change the underlying protocols of the internet. With billions of devices running on the current IP, it would not be likely that all or even most markets currently undergirded by TCP/IP—essentially every market that touches any internet-enabled infrastructure—would adopt a new protocol. The change would require users to implement a new infrastructure that is both incompatible with current technologies, making communications more expensive and more restrictive. Because standards depend on adoption and implementation, it is unlikely that mandates, even by some governments, would be universally accepted.

The fact that infrastructure-level digital standards are unlikely to change in the immediate to short-term does not mean that standards bodies are obsolete. The policymaking community can and should pay greater attention to iterative changes at the infrastructure level that push the

[21] Measurements: World IPv6 Launch." The Internet Society. https://www.worldipv6launch.org/measurements/.

[22] McKinnon, John. "Lawmakers Want Biden to Play Bigger Role Pushing Tech Legislation." The Wall Street Journal, Dow Jones &amp; Company, 27 Dec. 2021, https://www.wsj.com/articles/lawmakers-want-biden-to-play-bigger-role-pushing-tech-legislation-11640514605.

[23] Satariano, Adam. E.U. Takes Aim at Big Tech's Power with Landmark Digital Act. The New York Times, 24 Mar. 2022, https://www.nytimes.com/2022/03/24/technology/eu-regulation-apple-meta-google.html.

architecture of the internet toward state control while recognizing that a complete overhaul of TCP/IP is unlikely. If China strategically advances its own standards for critical infrastructure in package deals as part of the Belt and Road Initiative, countries will have to contend with dependency on China as the result of technological lock-in. There are also legitimate questions at the infrastructure level surrounding network neutrality, the idea that ISPs should treat all internet communications equally and not discriminate based on user content or location.

To What Should Policymakers Pay Attention When Shaping Recommendations Policy?

Digital standards are a global public good. The U.S. should not seek to supplant the private sector's leadership in standards-setting for emerging technologies nor exclude proposals from China de facto; rather, the U.S. should consider the following recommendations toward a nuanced and technically informed strategy for maintaining digital standards in line with democratic values.

Preserve Multi-Stakeholder Oversight of Infrastructure-Level Standardization

To productively engage across all SDOs, U.S. government leaders should be mindful of concerns raised by private sector stakeholders about which standards venues are appropriate for which activities. **Policymakers should distinguish and prioritize standards across infrastructure, protocol, and application layers, each requiring a unique governance approach**. For example, numerous civil society groups have warned against mission creep in the ITU's standardization activities.[24, 25] While the United States should maintain a seat at the ITU table, it should seek to preserve multi-stakeholder oversight of infrastructure level standards through bodies such as the IETF.

Most debates around the impact of standards on global security, commercial and human rights interests occur at the application level. They are ultimately normative policy questions rather than technical standards questions. A long-term vision should focus on technology areas of strategic interest to the U.S. at the application layer through targeted regulations that maintain a free, open, and democratic internet while maintaining a clear and technically informed understanding of what is likely to change (and what is not) at the infrastructure level.

Governing application-level standards could occur in several ways, such as through regulations that curb authoritarian tendencies in digital governance regimes. Congress could grant the Federal Trade Commission (FTC) rulemaking authority to regulate the information social media companies acquire about their users and how that information is used, including what kind of algorithms can be developed using aggregated user data. Another method would be implementing a variation of the Fairness Doctrine introduced by the Federal Communications Commission (FCC) in 1949, which mandated holders of broadcast licenses to give equal time to opposing viewpoints.[26] Policymakers could decide to pass a law that requires a similar balance of perspectives within social media content. **However, these decisions should be considered and implemented at a policy level, instead of through standards bodies**.

[24] ITI Response to NTIA Request for Input on WTSA-2020 (Docket No. 200504-0126)." The Information Technology Industry Council, National Telecommunications and Information Administration, 8 June 2020, https://www.ntia.doc.gov/files/ntia/publications/iti-06082020.pdf.

[25] Knodel, Mallory, and Heather West. Input on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly . Center for Democracy and Technology, Mozilla, Corp., 8 June 2020, https://www.ntia.doc.gov/files/ntia/publications/cdt-mozilla-06082020.pdf.

[26] Waldo, James. Zoom Interview. 25 Feb. 2022.

Increase Equitable Public and Private Sector Participation in Standards Bodies

Any U.S. Government approach to digital standards should recognize that China's role as a leader and challenger in some areas of technology is unlikely to change. The Chinese Communist Party and other authoritarian governments have long favored engagement in standards-setting through multilateral international institutions such as the ITU over multi-stakeholder bodies, whose industry and civil society representation dilute tendencies toward state-controlled governance structures.[27] Standards development is and will continue to be based on consensus, a process with significant public visibility. **Therefore, it is important that the U.S. increases its participation in multi-stakeholder standards bodies and organizations.** The U.S. should encourage and support industry-led processes in developing standards fit for market adoption.

Training and enabling the best technical talent should be a cornerstone of any U.S. standards approach. The federal government could support this effort by increasing funding for training new engineers and providing stipends for participation in volunteer organizations like the IETF, many of which have pricey membership fees and associated travel costs. Section 2520 of the bipartisan U.S. Innovation and Competition Act of 2021, which authorizes the Department of Commerce to issue grants to private sector organizations to participate in standards bodies, is a welcome step in this direction.[28]

American leaders should also work toward addressing the real and perceived inequities in the United States' multi-stakeholder approach to digital standards development by facilitating joint research opportunities for students from historically underrepresented countries at standards organizations. Concurrently, the U.S. could lead an effort to lobby international

[27] Eichensehr, Kristen. "The Cyber-Law of Nations." Social Science Research Network. 9 Jan. 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683.

[28] Montgomery, Mark and Natalie Thompson. "What the U.S. Competition and Innovation Act Gets Right About Standards." The Lawfare Blog. 13 Aug. 2021. https://www.lawfareblog.com/what-us-competition-and-innovation-act-gets-right-about-standards.

companies receiving royalties for intellectual property embedded in digital standards to accept reduced payments from developing nations.[29]

Fill Data Gaps

Much of the current interest in standards in the United States at the policy level is based on the observation that China has markedly increased its participation in standards bodies over the past decade. This is unsurprising given China's role as a serious player in the development of emerging technologies and its sizable market power. Indeed the number of contributions proposed by Chinese representatives has increased steadily since 2000, while the share of U.S. authors has decreased.[30]

One criticism often raised in SDOs is that China submits a large number of proposals, often of low quality diverting "time and resources away from the consideration of serious proposals."[31] Instead of looking at the quantity of standards proposed, a more insightful metric would be to consider which standards are implemented worldwide and for what technologies. **No single country or party can determine a standard unilaterally—technical standards are not effective if they do not support commercial interests and will not be adopted by the market.** In partnership with SDOs, industry, and other governments, the U.S. could spearhead an effort to build a live database including information on which standards are proposed, passed, adopted, and implemented across strategic technology areas. Filling this data gap would help policymakers understand what technical standards proposed by China pose a legitimate risk to U.S. interests through their proliferation in global markets and allow for more nuance in corresponding national strategies.

[29] Hill, Jonah Force. "A Balkanized Internet?: The Uncertain Future of Global Internet Standards." Georgetown Journal of International Affairs, Georgetown University Press, 2012, https://www.jstor.org/stable/43134338.

[30] Teleanu, Sorina. The Geopolitics of Digital Standards: China's Role in Standard-Setting Organisations. DiploFoundation/Geneva Internet Platform and Multilateral Dialogue Konrad Adenauer Foundation Geneva, Dec. 2021, https://www.diplomacy.edu/wp-content/uploads/2021/12/Geopolitics-of-digital-standards-Dec-2021.pdf.

[31] China in International Standards-setting: USCBC Recommendations for Constructive Participation. US-China Business Council, Feb. 2020, https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf.

Conclusion

Standards are omnipresent and shape our daily lives in ways seen—like the ability to access a website regardless of the device one uses—and unseen—such as the internet protocol that routes traffic across a network to that website. To effectively compete in an era of renewed strategic competition that is increasingly playing out in digital spheres, U.S. policymakers must separate hype from reality through a realistic appraisal of the impacts that technical, web, and mobile standards are likely to have across global security, commercial, and human rights interests. The current laissez-faire approach to standards emerged from a period of uncontested U.S. dominance in technology development and adoption is no longer sufficient. U.S. policymakers should take a proactive role in supporting the proliferation of quality digital standards through a multi-stakeholder model while remaining clear-eyed about the prospects of what changes are likely to materialize and on what timescale.

A long-term strategy should focus on guiding the development of strategic technologies at the application layer through regulatory policy frameworks. At the infrastructure level, U.S. policymakers can empower participation in multi-stakeholder SDOs that advance a free, open, and democratic internet by lowering barriers to entry for civil society and smaller private companies. The costs of not adapting our approach to meet the demands of today's digital environment are too great. We risk an alternative where individual SDOs operate in silos that are at best not mutually reinforcing and at worst counteracting.

Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

http://www.belfercenter.org/cyberproject