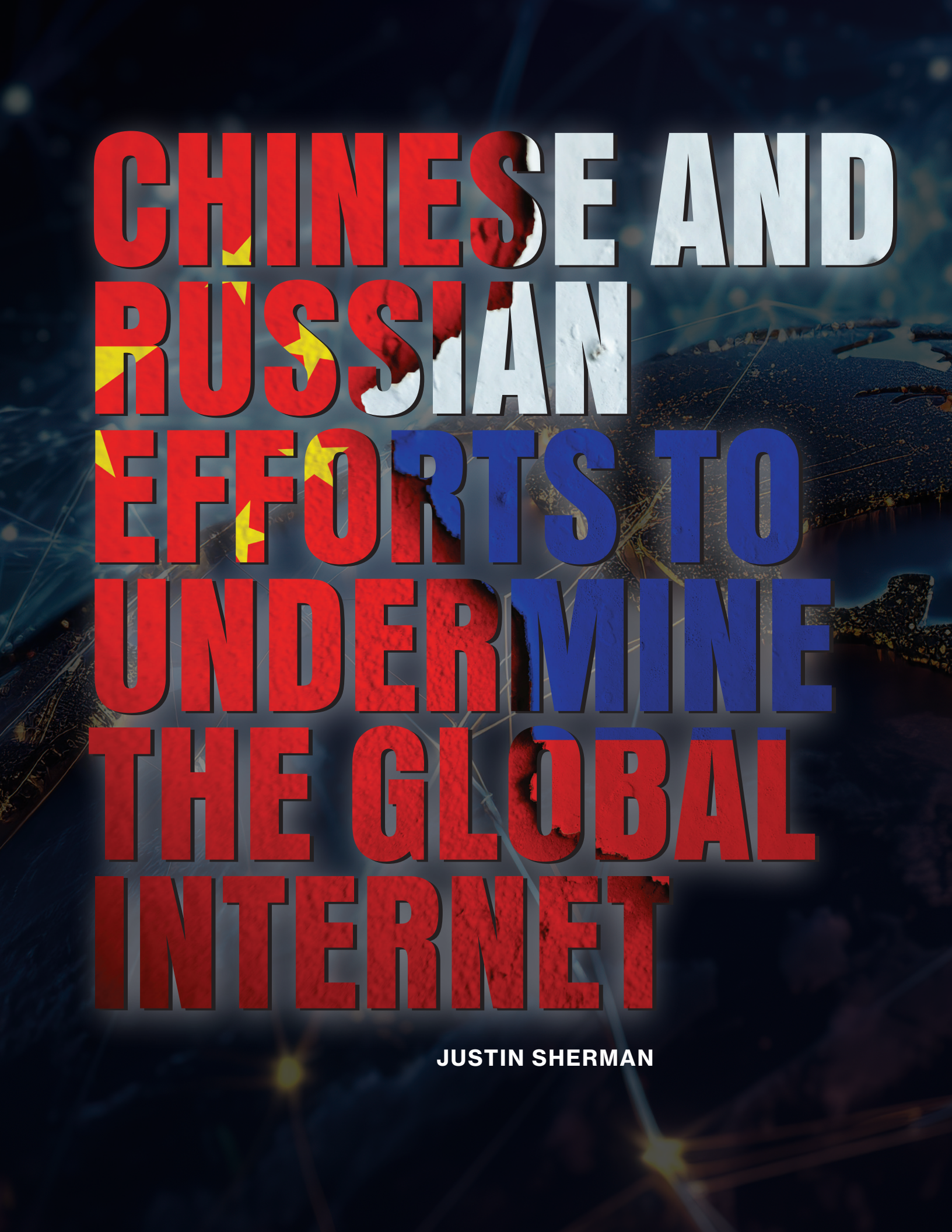

CHINESE AND
RUSSIAN
EFFORTS TO
UNDERMINE
THE GLOBAL
INTERNET
JUSTIN SHERMAN

THE GLOBAL INTERNET IS NOT A GIVEN. Many forces are shaping its future and threatening to make it more concentrated, less open, and more insecure, from giant companies with enormous market power, to governments that have failed to protect and promote privacy, to cybersecurity threat actors looking to steal data and scam individuals. Among those forces reshaping the internet as we know it are the Chinese and Russian governments. Internet optimists in democracies heralded the web as an enabler of freedom, a liberalizing force, a way for people to realize democracy while living under autocratic regimes. The Chinese and Russian governments took a very different view, perceiving the internet as a considerable threat to regime security—though their perceptions differ.

On top of cracking down on the internet at home, Beijing and Moscow have long worked to undermine narratives that support a global internet on the international level; grow their influence in bodies that develop internet standards; move internet governance activities to the United Nations, where initiatives are government-controlled; and legitimize their domestic internet control internationally, among other things. In some places, this activity is greatly aligned. For example, the Chinese and Russian governments have co-signed numerous UN cyber norms proposals over the years that seek to include regime-critical speech and journalism under the banner of "cybercrime."[1] In other areas, their activities diverge. Chinese companies and government organizations are far more active in technology and internet standards-setting bodies than their Russian counterparts. And recently, Russia's candidate to lead the International Telecommunication Union (ITU), the UN's tech agency, was overwhelmingly defeated in favor of the U.S. candidate. A U.S. candidate helps to combat both Chinese and Russian efforts to promote state internet control, but the very low level of support for the Russian candidate indicates that Moscow's internet activities in international bodies are likely to be far more constrained in the coming months than those of Beijing.

For those in the U.S. government looking to combat efforts to undermine the global internet—as well as for those in allied and partner countries—several points are critical. While Russia lost the ITU election in 2022, Chinese government efforts to undermine the global internet through formal processes, such as the UN, have been more successful. U.S. policymakers should keep capitalizing on the U.S.

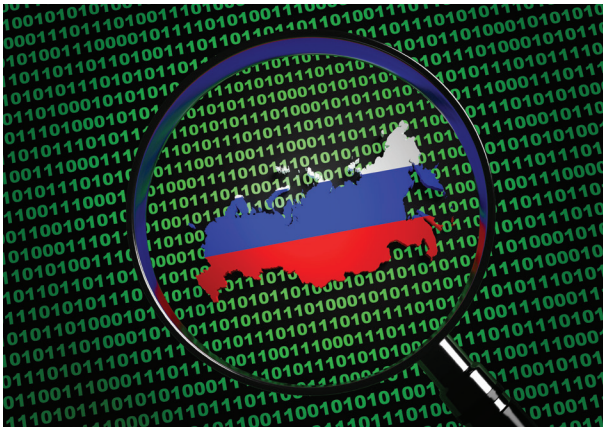
victory in the ITU to build the necessary blocs to continue supporting relatively open and global internet proposals in the coming years.

The Chinese and Russian governments took a very different view, perceiving the internet as a considerable threat to regime security.

The U.S. must also continue watching and combating Russian government efforts to undermine the global internet. While its ability to do so at the ITU is diminished, Moscow has many other means available to exert influence on the internet's future. In order to counter these efforts, the U.S. government must shift its tech-focused spending towards diplomacy, rather than continuing to concentrate this spending so much in military and defense. And the U.S. needs to get its own house in order—ensuring democratic values are being upheld and protected vis-à-vis technology and the internet at home, so they can be promoted more effectively on the international stage.

DIVERGENT VIEWS OF THE INTERNET

While many policymakers in democratic countries viewed the internet as a liberalizing force, a means of bringing democracy and freedom to the world,[2] several authoritarian



countries had a different perspective—seeing the internet as an opportunity for the country but also as a serious threat to regime security. In the 1990s, the Chinese government nationalized control of its four major internet backbones.[3] By 2000, the Chinese Ministry of Public Security had initiated the Golden Shield Project, an internet-focused policing system that evolved into the notorious "Great Firewall" used to censor online content and control the flow of internet data in the country.[4] Foreign companies like Google and Microsoft were soon complying with state censorship demands to stay in the market, and by the end of the decade, internet control mechanisms were in full swing.[5]

The Russian government set up an internet surveillance system in the 1990s but did not invest in the same way as China.[6] That is, until a series of events unfolded in the late 2000s and early 2010s: bloggers spreading information that countered Kremlin narratives in the 2008 Russo-Georgian War, individuals mobilizing with the internet's help in the Arab Spring in 2010–2013, the 2014 Euromaidan in Ukraine, and other events drove what I call the Kremlin's "internet awakening." Russian officials began devoting high-level attention to the internet as a security threat.[7] All told, the U.S. State Department's support of "internet freedom" and praise for the internet's role—including the role of blogs and social media—in the Arab Spring contrasted with very different, and concerned, reactions elsewhere.

Beijing and Moscow's prevailing term was (and is) cyber "sovereignty." Underpinning this perspective in China is an

emphasis on the importance of "sovereignty" broadly and the importance of multilateralism, where governments are the driver of decision-making, over multistakeholderism (the current global internet governance approach), where academics, members of civil society, companies, and others have a voice alongside governments.[8] The Russian government's perspective draws on the Russian concept of "information security," its belief in the importance of "sovereignty" to security, and its officials' paranoia about "color revolutions" in other countries like Ukraine;[9] Putin believes these events are the result of foreign interference and could occur in Russia. Although there are many general similarities between the two, Chinese and Russian officials do not view the global internet in exactly the same way.

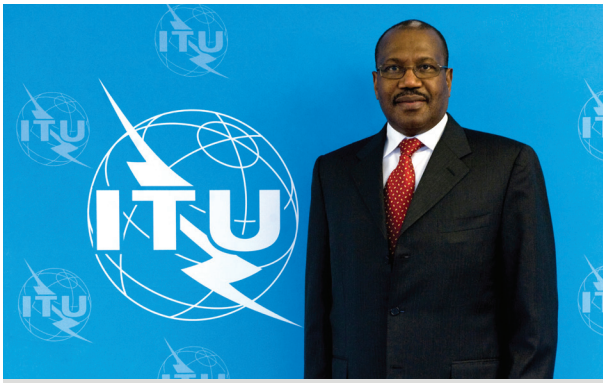
EFFORTS TO UNDERMINE THE GLOBAL INTERNET

Over the past several decades, the Chinese and Russian governments have worked in the UN and other international fora to undermine narratives that support a global internet; grow their influence in bodies that develop internet standards; move internet governance activities to the United Nations, where initiatives are government-controlled; and legitimize their domestic internet control internationally, among other things. While some of these activities are similar or more clearly aligned—such as joint Chinese-Russian proposals to the UN General Assembly that seek to promote state internet control and legitimize "cyber sovereignty" as a concept—others differ, such as Chinese and Russian activity on internet standards.

Both Moscow and Beijing have consistently advocated for internet governance decisions to move away from a multi-stakeholder model, where groups like the Internet Corporation for Assigned Names and Numbers (ICANN) and the nonprofit Internet Engineering Task Force (IETF) bring in a range of voices and perspectives, in favor of internet decision-making at the UN, a government-controlled body. At the 2003 World Summit on the Information Society, governments asked the UN secretary-general to establish a working group for future proposals—titled the Working Group on Internet Governance (WGIG). After four meetings in 2004–2005, the WGIG produced a report aiming to define internet governance, identify public policy issues around it, and develop a common understanding of governments, international organizations and forums, the private sector, and civil society in internet governance.[10] The report ultimately suggested that the UN or another multilateral, state-controlled body could take on a more assertive role in internet governance instead of multi-stakeholder nonprofits, even though it did not formally advance an agreement to make that happen. Beijing supported the conclusions and submitted formal comments declaring that governments and the UN were "the most authoritative delegates of the public interests."[11]

Beijing and Moscow's prevailing term was, and is, cyber "sovereignty."

In December 2012, China, Russia, Saudi Arabia, Algeria, Sudan, Egypt, and the United Arab Emirates introduced a proposal at the ITU to have it take over other internet organizations' authorities and functions, aiming to modify international telecommunications regulations agreed upon and in place since 1988.[12] The leaked proposal included a proposition for governments to control internet naming, numbering, addressing, and resource identification within their territories[13]—functions that multi-stakeholder nonprofits presently managed on behalf of the globe, irrespective (generally speaking) of state borders. It also said, "member states shall have the sovereign right to establish and implement public policy, including international policy,



Dr Hamadoun I. Touré, ITU Secretary-General | ITU Pictures from Geneva, Switzerland | CC BY 2.0 DEED

on matters of Internet governance, and to regulate the national Internet segment, as well as the activities within their territory of operating agencies providing Internet access or carrying Internet traffic."[14] After behind-the-scenes pushback from the U.S. and many others, the proposal was withdrawn.[15] It could have pushed to rip internet governance processes from the control of nonprofits that give voice to civil society, the private sector, and others—putting it firmly under governments' control.

Chinese and Russian activities don't end there. From 2007 to 2014, the Russian government appeared to maintain a close relationship with Hamadoun Touré, the ITU's then-secretary general. Most prominently, Putin met with Touré in June 2011 and was quoted as saying that Russia intended to continue a conversation about "establishing international control over the internet using the monitoring and supervisory capabilities of the International Telecommunication Union."[16] China and Russia have cosponsored several resolutions proposed to the UN General Assembly over the years, which nominally promote international cooperation on the responsible use of technologies, but in reality advance the normalization of state internet control under the guise of fighting "cybercrime" and "cyberterrorism" (which for Moscow and Beijing includes the likes of journalism, online mobilization, and anti-regime speech). More recently, Russia had a proposal passed in the UN to create a new cybercrime treaty—both to normalize state control of the internet and to undermine and replace the Budapest Convention on Cybercrime.[17]

Chinese government organizations and companies are far more active in technology and internet standards-setting bodies than their Russian counterparts. Chinese companies and government organizations are considerably active in the nonprofit IETF, the nongovernmental International Organization for Standardization (ISO), and the 3rd Generation Partnership Project (3GPP)—a collection of standards organizations. This was not always the case. From 1987 to 2001, for example, China co-authored only one of the 2,206 Requests for Comment that contribute to developing new internet protocols at the IETF.[18] Today, activity is pronounced: In August 2018, an official from China's Ministry of Industry and Information Technology stated that Chinese members submitted 12,774 contributions to ITU telecommunications study groups between 1998 and 2017, adding that in 2015, 2016, and 2017, Chinese members have made from 1,100–1,220 new ITU standards submissions each year.[19] A *Financial Times* analysis found that Chinese firms made every single ITU submission on surveillance technology between 2016 and 2019.[20]

The Chinese State Council's October 2021 national strategy for technical standards aims, among other things, to improve Chinese private sector competitiveness and increase alignment internationally with Chinese standards.[21] It calls for the alignment of advanced standards with Belt and Road Initiative (BRI) participant countries, BRIC countries, and Asia-Pacific Economic Cooperation forum member countries.[22] Of course, increasing the number of documents submitted into standards development processes does not guarantee those documents are accepted (or even if accepted, have importance in the world marketplace). There are also other reasons that Chinese companies may be incentivized to submit standards proposals beyond promoting or increasing the competitiveness of their products and services.

Putin met with Touré in June 2011 and was quoted as saying that Russia intended to continue a conversation about "establishing international control over the internet using the monitoring and supervisory capabilities of the International Telecommunication Union.

U.S. policymakers need to think about how they can capitalize on Doreen Bogdan-Martin's victory to build the necessary blocs to continue supporting relatively open-and-global internet proposals.

ITU Telecom World 2016—ITU SG Exhibition tour | ITU Pictures from Geneva, Switzerland | CC BY 2.0 DEED

As Naomi Wilson writes, "to encourage participation in standards bodies, the Chinese government provides monetary incentives for contributions," and "these incentives are also based on quantity, not quality."[23] Nonetheless, threaded throughout these initiatives is an emphasis on state-driven standards—and an effort to move internet standards-setting away from the nonprofit, multi-stakeholder bodies and towards the ITU, as it is government-controlled.

Most notably, Chinese telecom giant Huawei has advocated for "NEW IP," a new proposed approach to the Internet Protocol (IP) essential to the internet's function (e.g., forming the "IP" in "IP address"). The company initially presented this idea to ITU delegates in September 2019 and February 2020.[24] It was also backed by China's Ministry of Industry and Information Technology and the state-owned telecoms China Mobile, China Unicom, and China Telecom.[25] The proposal duplicated and essentially circumvented work already ongoing and historically within the purview of non-UN bodies,[26] and that was exactly the point. Beijing wants more government-led internet standards development, where it can use political leverage to outmaneuver other countries as opposed to relying on more technical arguments made in multi-stakeholder fora—such as at the ITU. Now, Huawei has repackaged its "NEW IP" proposal as "IPv6+" and has continued to push it internationally.[27]

LOOKING AHEAD – AND BUILDING A RESPONSE

In September 2022, the U.S. defeated Russia in an election for the next secretary-general of the ITU—the country representative elected, in a one-vote-per-country model, to lead the UN's tech agency for the next four years. After months of uncertainty, and an extensive international diplomatic campaign, U.S. candidate Doreen Bogdan-Martin beat Russian candidate Rashid Ismailov, by 139 votes to 25.[28] It was a stunning victory. It also, following several Russian successes in promoting "cyber sovereignty" proposals at the UN, underscored that the Putin regime's illegal war on Ukraine had at least partially undermined Russian legitimacy at the UN—enough so that the U.S. and its allies and partners were able to build a winning voting bloc. Moscow's ability to successfully advance internet control measures at the UN and in at least some other international bodies, by this indication, may be constrained in the years to come.

However, it would be a step too far to assume the same constraints would apply to Beijing. The Chinese government is in a very different position on the international stage

WSIS 2016—Doreen Bogdan-Martin, Chief of Strategic Planning and Membership Department | ITU Pictures from Geneva, Switzerland | CC BY 2.0 DEED

International Telecommunication Union (ITU) headquarters campus buildings | Bastiaan Quast CC BY-SA 4.0 DEED

than its Russian counterpart, given that it is not waging an illegal war on Ukraine, among many other reasons. China is the second-most populous country on the planet; Russia is the ninth. China has a massive and growing domestic technology sector that is internationally competitive; while Russia's tech sector pales in comparison in its size, capability, and market reach. The list goes on, but the point is that an ITU secretary-general election between an American and a Chinese candidate may have played out very differently—and the hypothetical result is very unclear. For the foreseeable future, at least right now, the Chinese government looks to maintain (if not increase) its influence on international technology issues, including matters of the global internet, even as Moscow may be losing some of its influence in traditional international processes (such as ITU votes).

The U.S. should breathe a sigh of relief now that Bogdan-Martin has won the ITU election, indeed due in part to the tireless efforts of many U.S. diplomats and their counterparts abroad. But the work does not stop here, and the Chinese government is certainly going to continue to attempt to undermine the global internet in the coming decades, including by marshaling support for new proposals and resolutions in the UN. It is also looking to do so via new mechanisms, such as turning its annual World Internet Conference event in China into an organization whose members include the governments of North Korea, Cambodia, and Syria, and many others.[29] U.S. policymakers need to already begin thinking now about how they can capitalize on Doreen Bogdan-Martin's victory to build the necessary blocs to continue supporting relatively open-and-global internet proposals. For example, the U.S. should focus much more on engaging, giving voice to, and empowering lower-resourced countries and countries in the Global South who are often shut out of international tech conversations. India, Brazil, and others cannot and should not be sidelined in these internet-focused activities.

The U.S. must continue combating Russian efforts to undermine the global internet.

The U.S. must continue monitoring and combating Russian government efforts to undermine the global internet as well. If the ITU election is any indication, Moscow's ability to do so through formal channels, like UN General Assembly and ITU proposal processes, may be limited in the coming years.

The Kremlin nonetheless has many available means to try to undermine the relatively global internet, including by quietly marshaling support for Beijing-led initiatives, hardening its domestic tech sector against sanctions and foreign entanglements, pushing for more internet isolation at home, and continuing to serve as a legalistic model of internet repression for former Soviet republics and other countries in Russia's "near abroad." Beijing's activities to undermine the global internet will demand a concerted response from the U.S. and its allies and partners, but the U.S. cannot take its eye off the ball with Russian efforts, either. In both cases, scaling up the amount of money spent on tech-focused diplomacy—both via executive branch budget requests and resulting Congressional allocations—will be essential.

Lastly, as mentioned above, the U.S. needs to look inward. If U.S. policymakers are going to talk a big game about "techno-democracy," as the Biden administration has done vocally and consistently, they need to work to ensure democratic values are being upheld and protected vis-à-vis technology and the internet at home. The U.S. currently lacks a comprehensive federal privacy model to protect citizens against data abuses, and policy conversations about corporate power and anti-competitiveness in tech focus heavily on the content sent over the internet, without also considering the risks of concentrating internet infrastructure in the hands of just a few companies—such as the dominant cloud "hyperscalers" Amazon, Google, and Microsoft. Meanwhile, U.S. government messaging on the internet contains many confusing and mixed signals, talking vaguely of openness and security and trusted data flows, and executive branch efforts to promote "techno-democracy" have focused largely on wealthy, Western countries—cutting many low-resourced countries out of the conversation. Even conversations about apps like TikTok and WeChat, often framed entirely through a national security lens, at some point must also consider questions of internet openness, market competitiveness, online connectivity, and more.

Today's internet ecosystem is not a given. The more that the Chinese and Russian government pursue efforts to undermine the relatively global internet as it currently stands, the more the U.S. and its allies and partners will have to articulate a positive vision for the internet, invest more in diplomacy to promote it, and work to support the many other countries, companies, civil society groups, and individuals in shaping an open and global future for the internet.

ABOUT THE AUTHOR

Justin Sherman is the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm; a senior fellow at Duke University's Sanford School of Public Policy; and a nonresident fellow at the Atlantic Council.

The more that the Chinese and Russian government pursue efforts to undermine the relatively global internet as it currently stands, the more the U.S. and its allies and partners will have to articulate a positive vision for the internet.

ENDNOTES

1 Much of this UN discussion and other components of this article draw on two previously published whitepapers: Justin Sherman, "*Russia's War for Control of Global Internet Governance*," Social Science Research Network, June 9, 2022; and Justin Sherman, "*China's War for Control of Global Internet Governance*," Social Science Research Network, August 1, 2022.

2 See Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012); and

Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011). It is also worth noting this is somewhat of a generalization of part of the policy community and some pundits in the media ecosystem. Certainly, many people in the United States and other democratic countries did not have the same view of the internet due to their lived experiences, such as heavily policed communities also facing heightened state surveillance online or women, Black individuals, and LGBTQIA+ people experiencing hate speech and harassment on the internet.

3 Zixiang (Alex) Tan, William Foster, and Seymour Goodman, "China's State-Controlled Internet Infrastructure," *Communications of the ACM* 42, no. 6 (June 1999):

44-52; Xing Li, Jianping Wu, and Youneng Liang, "China Education and Research Network: A Continuous Report," INET 96, Internet Society, 1996; "Introduction of CSTNET," *CSTCloud.net*,, https://www.cstcloud.net/cstnet.htm (accessed June 14, 2022);

Kathleen Ohlson, "China Internet market on the rise," *CNN*, September 4, 1998, http://www.cnn.com/TECH/computing/9809/04/chinet.idg/ (accessed February 24, 2023); and

"Jitong Network Communications Company Limited," *cs.wisc.edu*, September 5, 2001, https://pages.cs.wisc.edu/~anhai/wisc-si-archive/data/company_profiles/standard/instances/company_index/Telecommunications/Diversified_Telecom_Service_Providers/instances/http:%5E%5Ewww.thestandard.com%5Ecompanies%5Edossier%5Eo,1922,280995,00.html (accessed February 24, 2023).

4 Ping Punyakumpol, "The Great Firewall of China: Background," *cs.stanford.edu*, June 1, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html (accessed February 24, 2023).

5 "Timeline: China's net censorship," June 29, 2010, *BBC*, https://www.bbc.com/news/10449139 (accessed February 24, 2023); and

Sonali Chandel, Zang Jingji, Yu Yunnan, Sun Jingyao, and Zhang Zhipeng, "The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall," *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, October 17-19, 2019.

6 Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's back door onto the internet—extract," *The Guardian*, September 8, 2015, https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet (accessed February 24, 2023).

7 Justin Sherman, *Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior* (Washington, D.C.: Atlantic Council, July 2021); and Sherman, "Russia's War for Control of Global Internet Governance."

See also Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: PublicAffairs, 2015).

8 Sherman, *China's War for Control of Global Internet Governance*, 6-10.

9 Sherman, *Russia's War for Control of Global Internet Governance*, 5-7.

10 Châteu de Bossey, *Report of the Working Group on Internet Governance* (Geneva: UN Working Group on Internet Governance, June 2005), 3-4; and United Nations, Press Release, November 11, 2004, "United Nations Establishes Working Group on Internet Governance."

11 China's Comments to WGIG on Draft Working Papers: Identifying Issues for Internet Governance. February 11, 2005. 1.

12 International Telecommunication Union. *Final Acts of the World Administrative Telegraph and Telephone Conference* (Melbourne, 1988). Geneva: International Telecommunication Union, 1988. https://www.itu.int/osg/csd/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf.

13 Chris Welch, "Russia, China, and other nations draft proposal to Give ITU greater influence over the internet," *The Verge*, December 9, 2012, https://www.theverge.com/2012/12/9/3747402/countries-propose-greater-itu-influence (accessed February 24, 2023).

14 Violet Blue, "WCIT-12 leak shows Russia, China, others seek to define government-controlled internet,'" *ZDNet*, December 8, 2012, https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/ (accessed February 24, 2023).

15 International Telecommunication Union. Tweet. December 10, 2012. https://twitter.com/ITU/status/278079049983721472 (accessed February 24, 2023);

Blue, "WCIT-12 leak"; Mike Masnick, "ITU Boss In Denial: Claims Success, Misrepresents Final Treaty, as US, UK, Canada And Many More Refuse To Sign," *TechDirt*, December 14, 2012, https://www.techdirt.com/2012/12/14/itu-boss-denial-claims-success-misrepresents-final-treaty-as-us-uk-canada-many-more-refuse-to-sign/ (accessed February 24, 2023).

16 Leo Kelion, "US Resists control of internet passing to UN agency," *BBC*, August 3, 2012, https://www.bbc.com/news/technology-19106420 (accessed February 24, 2023).

17 Justin Sherman, "Putin Is Crushing Biden's Room to Negotiate on Ransomware," *WIRED*, August 6, 2021, https://www.wired.com/story/opinion-putin-is-crushing-bidens-room-to-negotiate-on-ransomware/ (accessed February 24, 2023).

18 Shen, "China and global internet governance," 6.

19 Fang Li, "China's Participation in ITU-T Standardization Activities and Experience Sharing on BSG," *ITU.int*, August 27, 2018, 5.

20 Anna Gross and Madhumita Murgia, "China shows its dominance in surveillance technology," *Financial Times*, December 26, 2019, https://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96 (accessed February 24, 2023).

21 Matt Sheehan, Marjory Blumenthal, and Michael R. Nelson, "Three Takeaways From China's New Standards Strategy," *Carnegie Endowment for International Peace*, October 28, 2021, https://carnegieendowment.org/2021/10/28/three-takeaways-from-china-s-new-standards-strategy-pub-85678 (accessed February 24, 2023).

22 Ibid.

23 Naomi Wilson, "China Standards 2035 and the Plan for World Domination—Don't Believe China's Hype," *Council on Foreign Relations*, June 3, 2020, https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype (accessed February 24, 2023).

24 Madhumita Murgia and Anna Gross, "Inside China's controversial mission to reinvent the internet," *Financial Times*, March 27, 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f (accessed February 24, 2023).

25 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/ (accessed February 24, 2023).

26 Hascall Sharp and Olaf Kolkman, "Discussion Paper: An analysis of the 'New IP' Proposal to the ITU-T," *Internet Society*, April 24, 2020, https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/ (accessed February 24, 2023).

27 Luca Bertuzzi, "China rebrands proposal on internet governance, targeting developing C=countries," *Euractiv*, June 6, 2022, https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/ (accessed February 24, 2023).

28 Tom Gerken, "UN Elects first female tech agency secretary-general," *BBC*, September 29, 2022, https://www.bbc.com/news/technology-63074895 (accessed February 24, 2023).

29 Phelim Kine, "China launches new bid for internet dominance," *Politico*, July 21, 2022, https://www.politico.com/newsletters/politico-china-watcher/2022/07/21/china-launches-new-bid-for-internet-dominance-00047037 (accessed February 24, 2023).