Norm diffusion in cyber governance: China as an emerging norm entrepreneur?

XUECHEN CHEN AND XINCHUCHU GAO*

In the past decade, China has emerged as a technological and cyber power with immense potential to reshape cyber governance regionally and globally.[1] Hosting the world's largest internet user community[2] and comprising the second largest digital economy,[3] China has increasingly sought leadership in reshaping the global cyber-governance regime.[4] In this light, scholars have debated the extent of China's newfound emergence as a norm entrepreneur in global cyber governance and the nature of its attempts to diffuse its norms and approaches to cyber governance in the international arena.

The western-centric character of early scholarly discussions of cyber politics and governance from the mid-1990s and early 2000s is widely acknowledged. Discussion focused heavily on institutional innovation, the controversy surrounding the formation of the Internet Corporation for Assigned Names and Numbers (ICANN), and the hegemonic position of the United States in cyber governance,[5] while considering China's marginalized role within the wider global South. Only in the 2010s did an increasing body of research on China's visions, behaviours, policies and influence in cyberspace begin to emerge. Tracing the genealogy of the debates over China's approach to and role in cyber governance yields two distinct yet interrelated scholarly camps. For the first, China's authoritarian use of

* This article is part of a special section in the November 2024 issue of *International Affairs* on 'Cybersecurity and International Relations: developing thinking tools for digital world politics', guest-edited by Tobias Liebetrau and Linda Monsees. We would like to express our gratitude to Tobias Liebetrau and Linda Monsees for organizing this special section and the workshops. We would also like to thank Benjamin Farrand and Helena Carrapico for their constructive feedback on our first draft. In addition, we are grateful to the editorial team at *International Affairs* and the four anonymous reviewers for their professional and constructive engagement with the article. For this research project, the authors received funding from the British Academy/Leverhulme Small Research Grants SRG 2022 Round (SRG22\220227). The authors both contributed equally to the conceptualization, drafting and completion of this manuscript.

[1] Nigel Inkster, *China's cyber power* (Abingdon: Routledge, 2016).

[2] People's Republic of China, State Council Information Office, 'White paper: China's internet population reaches 1.05 billion', 7 Nov. 2022, http://english.scio.gov.cn/m/pressroom/2022-11/07/content_78506468.htm. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 6 Sept. 2024.)

[3] Xinhua, 'China's digital economy as a new growth engine to drive modernization', State Council Information Office, 28 April 2023, http://english.scio.gov.cn/chinavoices/2023-04/28/content_85259744.htm.

[4] Xinchuchu Gao, 'An attractive alternative? China's approach to cyber governance and its implications for the western model', *The International Spectator* 57: 3, 2022, pp. 15–30, https://doi.org/10.1080/03932729.2022.2074710.

[5] Milton L. Mueller and Farzaneh Badiei, 'Inventing internet governance: the historical trajectory of the phenomenon and the field', in Laura DeNardis et al., eds, *Researching internet governance: methods, frameworks, futures* (Cambridge, MA: MIT Press, 2020), pp. 59–83.

International Affairs **100**: 6 (2024) 2419–2440; DOI: 10.1093/ia/iiae237

cyber governance, with its socio-political implications, formed an important line of interrogation.[6] This camp primarily analyses China's practices in cyber governance as a particular means to strengthen its authoritarian regime and advance its political ambitions, centring on internet politics at the domestic level (e.g. internet censorship and state control over online expression and political opposition).[7]

The second group widened its focus beyond authoritarian internet control to unpack China's distinct normative positions;[8] legal, regulatory, institutional foundations; and policy mechanisms in governing cyberspace.[9] Unlike the 'digital authoritarianism' arguments, their analyses call for a more nuanced understanding of China's cyber-governance landscape, considering the pluralistic nature of China's vision and approach and the wide array of institutional actors shaping its discourses and policies on cyber governance.[10] Despite lacking consensus on how best to conceptualize China's cyber-governance model, this group widely agrees that China is actively developing a unique vision and approach to governing cyberspace that differs from western approaches and 'is embedded within the country's distinctive political, economic and technological context'.[11] Within this second camp, a growing number regard China as a nascent norm entrepreneur (i.e. an 'agent having strong notions about appropriate or desirable behaviour in their community'[12]), proactively seeking to externalize its own models of and approach to cyber governance beyond its borders. Specifically, extensive arguments have underscored China's promotion of global cyber or internet sovereignty norms[13] with the hope of contesting and reshaping the existing multi-stakeholder aspect of global cyber-norm design promoted by western actors such as the US and the European Union.[14] Others have labelled China's global regulatory outreach the 'Beijing effect' in examining China's mechanisms of exporting its cyber-governance models to developing countries.[15] This growing volume of research consid-

[6] See for example Min Jiang, 'Authoritarian deliberation on Chinese internet', *Electronic Journal of Communication* 20: 3&4, 2010, pp. 1–22, https://www.cios.org/EJCPUBLIC/020/2/020344.html; Jinghan Zeng, 'China's date with big data: will it strengthen or threaten authoritarian rule?', *International Affairs* 92: 6, 2016, pp. 1443–62. https://doi.org/10.1111/1468-2346.12750.

[7] Min Tang and Narisong Huhe, 'Parsing the effect of the internet on regime support in China', *Government and Opposition* 55: 1, 2020, pp. 130–46, https://doi.org/10.1017/gov.2017.39; Daniëlle Flonk, 'Emerging illiberal norms: Russia and China as promoters of internet content control', *International Affairs* 97: 6, 2021, pp. 1925–44, https://doi.org/10.1093/ia/iiab146.

[8] See for example Geoffrey Joseph Hoffman, 'Cybersecurity norm-building and signaling with China', in Dennis Broeders and Bibi van den Berg, eds, *Governing cyberspace: behavior, power and diplomacy* (Lanham, MD: Rowman & Littlefield, 2020), p. 187.

[9] See for example Rogier Creemers, 'Cybersecurity law and regulation in China: securing the smart state', *China Law and Society Review* 6: 2, 2023, pp. 111–45, https://doi.org/10.1163/25427466-06020001.

[10] Jinghan Zeng, Tim Stevens and Yaru Chen, 'China's solution to global cyber governance: unpacking the domestic discourse of "internet sovereignty"', *Politics & Policy* 45: 3, 2017, pp. 432–64, https://doi.org/10.1111/polp.12202.

[11] Rogier Creemers, 'The Chinese conception of cybersecurity: a conceptual, institutional and regulatory genealogy', *Journal of Contemporary China* 33: 146, 2024, pp. 173–88, https://doi.org/10.1080/10670564.2023.2196508.

[12] Martha Finnemore and Kathryn Sikkink, 'International norm dynamics and political change', *International Organization* 52: 4, 1998, pp. 887–917 at p. 896, https://doi.org/10.1162/002081898550789.

[13] Aleš Karmazin, 'China's promotion of cyber sovereignty beyond the West', in Šárka Kolmašová and Ricardo Reboredo, eds, *Norm diffusion beyond the West* (Cham, Switzerland: Springer Nature, 2023), pp. 61–76; Zeng et al., 'China's solution to global cyber governance'.

[14] Gao, 'An attractive alternative?'.

[15] Matthew S. Erie and Thomas Streinz, 'The Beijing effect: China's Digital Silk Road as transnational data

ering China as a nascent cyber-governance norm entrepreneur resonates well with the wider debate in International Relations (IR) scholarship concerning its potential shift from being a 'status quo power' to a 'revisionist power' aiming to reshape the existing global order either through incremental adjustments or by completely overthrowing it via new measures or initiatives.[16]

Despite surging research interest in China's norm entrepreneurship in cyberspace, three limitations and gaps are evident in the existing research. First, studies of China's cyber norms have primarily examined its promotion of a single cyber-governance norm, focusing almost exclusively on Beijing's conception and discursive construction of the norm of cyber sovereignty.[17] Although recent studies have explored China's adoption of additional cyber norms, such as the protection of the public core of the internet, these norms are essentially regarded as extending or rhetorically modifying the core norm of cyber sovereignty.[18] An exclusive focus on cyber sovereignty neglects the evolving nature of China's normative position on cyber governance and underestimates other core values embedded in its official discourses.

Second, while some scholars have rightly stated that China's cyber norms remain vague,[19] in-depth investigation of the elastic nature and multilayered structure characterizing China's cyber norms is lacking. Building on the norm diffusion literature's latest theoretical advancements, this article departs from this position by conceptualizing norms not as single entities, but as norm clusters—a looser collection of interlocking components comprising a specific set of problems, values and appropriate behaviours. Analysing China's cyber norms in such a way enables a more sophisticated examination of the heterogeneous components that constitute China's normative position on cyber governance.

Third, detailed examinations of China's diverse mechanisms employed to promote its cyber-governance norms remain relatively limited, while studies examining China's norm promotion mechanisms have not paid sufficient attention to Chinese firms' increasing role in shaping China's strategies to promote norms and standards externally and to the delicate relationship between its public and private stakeholders throughout the diffusion processes. Such gaps highlight the necessity of refining theoretically informed empirical analyses to further examine China's norm-diffusion process in the sphere of cyber governance. To mitigate these gaps, this article explores two questions: 1) What core norms has China sought to externalize in the domain of cyber governance, and how can we understand the elastic and multifaceted nature of China's cyber norms?; and 2) what

governance', *New York University Journal of International Law and Politics* 54: 1, 2021, pp. 1–92, https://www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf.

[16] David Shambaugh, 'China or America: which is the revisionist power?', *Survival* 43: 3, 2001, pp. 25–30, https://doi.org/10.1080/00396330112331343025.

[17] See for example Zeng et al., 'China's solution'; Jon R. Lindsay, 'The impact of China on cybersecurity: fiction and friction', *International Security* 39: 3, 2014, pp. 7–47, https://doi.org/10.1162/ISEC_a_00189.

[18] Courtney J. Fung, 'China's use of rhetorical adaptation in development of a global cyber order: a case study of the norm of the protection of the public core of the internet', *Journal of Cyber Policy* 7: 3, 2022, pp. 256–74, https://doi.org/10.1080/23738871.2023.2178946.

[19] Zeng et al., 'China's solution'.

mechanisms has China used to promote its norms and relevant policies in cyber governance beyond its territory?

To address the three problems identified in existing research, this study seeks to offer empirical, conceptual and policy contributions. First, through a systematic review of a wide range of primary materials, including official statements and policy papers as well as interview data collected during fieldwork in China in July 2023, this study transcends the narrow focus on the norm of cyber sovereignty by providing a more comprehensive mapping of China's cyber-norm cluster, encompassing a complex combination of different problems, core values and appropriate behaviours. Thus, this study highlights the need to broaden the scope of empirical research on China's cyber-governance norm entrepreneurship and to consider newly emerging ideas and concepts promoted by Beijing in this policy domain. Furthermore, this article advances our understanding of China's mechanisms for externally diffusing its cyber-governance norms. Departing from the existing research on China's use of a single norm-promotion mechanism,[20] our findings suggest that Beijing has relied on a combination of diffusion mechanisms in the form of socialization and positive incentives to externalize its cyber-governance norms regionally and globally.

Second, this study advances the conceptual debate on China's emerging cyber-governance norm entrepreneurship. Whereas previous studies essentially saw China's norms as single norms, this research develops a more sophisticated conceptual framework that helps disaggregate the tripartite structure of China's cyber norms and detect different norm-promotion strategies, adding nuances to the conceptual and theoretical discussion of China's emerging role as a norm shaper in global politics in general, and in cyber governance in particular. By operationalizing norm diffusion theory in the case-study of China's cyber governance, this article aligns well with the special section's objective to develop innovative thinking tools for digital world politics.[21] Third, the article sheds light on the burgeoning policy debates on how best to interpret the nature of China's distinctive vision and behaviour concerning cyber governance and the extent to which China can be regarded as a 'revisionist power' or a threat to the existing normative global cyber-governance structure dominated by liberal democratic principles and multi-stakeholder models. Our observations add nuance to the view—shared by many western policy analysts—that China's vision of cyber governance is largely driven by digital authoritarianism, with a growing capability to overturn the existing normative and institutional global cyber-governance frameworks. Our findings suggest that while China's normative cyber-governance underpinnings differ significantly from western-led liberal democratic values, China's ambition and capability to fundamentally alter global cyber governance remain modest. Notably, China's strong preference to promote its cyber norms through existing regional and international forums, and its intention to consolidate the United

[20] Flonk, 'Emerging illiberal norms'.

[21] See the introduction to this special section: Linda Monsees and Tobias Liebetrau, 'Cybersecurity and International Relations: developing thinking tools for digital world politics', *International Affairs* 100: 6, 2024, pp. 2303–14, https://doi.org/10.1093/ia/iiae232.

Nations' role in setting global cyber-governance rules and agendas, indicate that China has not yet achieved the status of a revisionist power in this policy domain.

Methodology

For this article, we adopted a case-study approach to examine the substance of China's norm cluster and norm-diffusion strategy in the sphere of cyber governance. While a case-study approach can be limited in scope, it enables a holistic evaluation of a specific process and its context, thereby serving as a critical tool for conceptual validity and exploring complex mechanisms at the core of the research.[22] The empirical analysis of China's cyber-norm cluster and norm-diffusion mechanisms was informed by a qualitative analysis of a wide range of primary and secondary data published between 2010 and 2023. This time-frame reflected the evolution of China's cyber norms and norm-promotion mechanisms since the introduction of its first landmark white paper on cyber governance. The qualitative analysis in this research involved a process designed to condense data into key themes and categories based on valid interpretations and inferences.[23] Our codes and categories concerning China's norm cluster and norm-diffusion mechanisms were developed both inductively and deductively, deriving from norm-diffusion theories, previous related studies on China's cyber-governance norm entrepreneurship and the data we collected through a comprehensive and systematic review of official documents published by Chinese authorities such as the State Council Information Office, the Ministry of Foreign Affairs and China's Permanent Mission to the United Nations, and China's statements and policy documents released at various regional and international organizations and institutions, such as the United Nations Open-ended Working Group, the Shanghai Cooperation Organization (SCO) and the BRICS grouping (which comprises Brazil, Russia, India, China and South Africa). In addition, the analysis draws on various secondary sources, including media reports, academic journal articles and policy analyses in both Chinese and English, which serve as complementary tools to triangulate evidence and increase the reliability of the empirical findings. Data triangulation is also facilitated by data from interviews with Chinese officials and scholarly experts working closely in the field of cyber governance, collected during fieldwork in China in July 2023.

The remainder of the article proceeds as follows. The first section delineates the theoretical framework, drawing from the literature on norm diffusion in IR scholarship. A norm cluster containing specific problems, values and behaviours that China has sought to promote in cyber governance is examined in the second section, taking into consideration the complex and evolving nature of China's cyber norms. The third section discusses the mechanisms China employs to diffuse its norms and approaches, while the final section provides a summary of the key arguments and research conclusions.

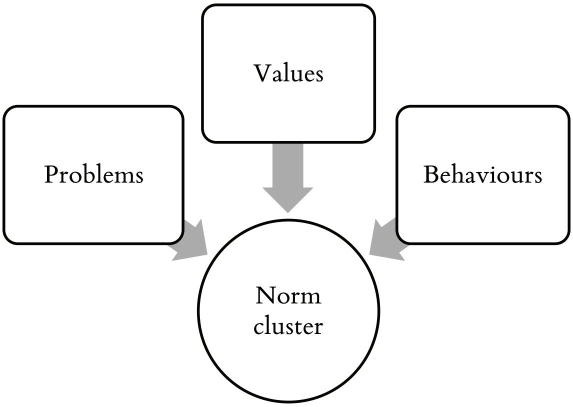
[22] Alexander L. George and Andrew Bennett, *Case studies and theory development in the social sciences* (Cambridge, MA: MIT Press, 2005).

[23] Matthew B. Miles and A. Michael Huberman, *Qualitative data analysis: an expanded sourcebook* (Thousand Oaks, CA: Sage, 1994).

Norm-diffusion literature as a nuanced framework for unpacking China's norm promotion in cyber governance

To develop a more nuanced understanding of China's cyber norms, we must first delve into the structure and nature of these norms. The literature on norm diffusion defines norms as 'shared understandings that make behavioural claims'[24] or as 'standards of appropriate behaviour'.[25] These multiple functions suggest that norms have both constitutive and constraining aspects.[26] Recent critical norm research and norm-diffusion theory argue that the interaction between the constitutive and constraining aspects generates a norm's tripartite conceptual structure, comprising problem, value and behaviour.[27] Thus, a norm first presupposes the existence of a problem—the issue to be addressed. Second, it contains a value that differentiates good from bad. Lastly, it involves behaviour—that is, an appropriate action to be taken to solve a given problem that is publicly justified by the actor.[28] In rejecting the linear, static conceptualization of norms and norm diffusion, this study adopts Winston's view that international norms can be better conceptualized as norm clusters—that is, a looser collection of interlocking components comprising a specific set of problems, values and behaviours, as demonstrated in figure 1.[29] Perceiving norms in this way enables a more comprehensive understanding of the evolving, multifaceted nature of China's cyber-governance norms.

Figure 1: The tripartite structure of norm clusters



Source: Authors' elaboration based on Winston, 'Norm structure, diffusion, and evolution'.

[24] Jeffrey T. Checkel, 'Norms, institutions, and national identity in contemporary Europe', *International Studies Quarterly* 43: 1, 1999, pp. 83–114 at p. 88, https://doi.org/10.1111/0020-8833.00112.

[25] Finnemore and Sikkink, 'International norm dynamics', p. 891.

[26] Antje Wiener, 'Enacting meaning-in-use: qualitative research on norms and International Relations', *Review of International Studies* 35: 1, 2009, pp. 175–93, https://doi.org/10.1017/S0260210509008377.

[27] Carla Winston, 'Norm structure, diffusion, and evolution: a conceptual approach', *European Journal of International Relations* 24: 3, 2018, pp. 38–661, https://doi.org/10.1177/1354066117720794.

[28] Winston, 'Norm structure, diffusion, and evolution'.

[29] Winston, 'Norm structure, diffusion, and evolution'.

Furthermore, norm-diffusion theory offers a more nuanced insight into how China's cyber-governance norms and regulations traverse borders. Diffusion theory helps address the current lack of consensus on how to theorize China's norm-diffusion mechanisms in its approaches to cyber governance by identifying different categories of diffusion mechanisms devised by the norm sender.[30] The first category of diffusion mechanisms relates to diffusion through the manipulation of utility calculations by providing positive or negative incentives to the potential norm recipient.[31] For example, an agent of diffusion can induce other actors to adopt their ideas by attempting to change the latter's utility functions. Specifically, such an agent may provide rewards, such as financial and technical assistance, or may impose costs through sanctions.[32]

The second mechanism of diffusion is socialization, whereby actors develop shared cognitive beliefs and common norms through their interactions. This process, in turn, shapes actors' perceptions of the legitimacy of certain norms or policies and may result in redefining actors' normative considerations due to the internalization of norms.[33] Rather than regarding socialization as a two-way process,[34] this study adopts Risse's interpretation of socialization as a mainly sender-driven mechanism.[35] In this interpretation, socialization is closer to the concept of persuasion, referring to situations in which the sender tries to enforce adoption 'about the validity claims inherent in any causal or normative statement'.[36] In our empirical study, the direct mechanism of socialization is primarily concerned with the norm sender's role, especially the actor's creation or use of different institutional configurations as platforms to exchange ideas, perspectives and practices.[37] Institutional environments characterized by the exchange of opinions and practices can potentially lead to changes in normative considerations and expectations regarding the appropriateness of actions.[38] Via this conceptualization of diffusion mechanisms, diffusion theory provides a sophisticated framework for analysing China's attempts to promote its diffusion objects in cyber governance beyond its borders.

[30] While transnational diffusion literature also provides explanations regarding diffusion mechanisms driven by the norm recipient (e.g. competition, emulation, lesson-drawing), the discussion of these indirect mechanisms falls outside the scope of this research and is therefore excluded from the analytical framework.

[31] Thomas Risse, 'The diffusion of regionalism', in Tanja A. Börzel and Thomas Risse, eds, *The Oxford handbook of comparative regionalism* (Oxford: Oxford University Press, 2016), pp. 87–108.

[32] Tanja A. Börzel and Thomas Risse, 'From Europeanisation to diffusion: introduction', *West European Politics* 35: 1, 2012, pp. 1–19, https://doi.org/10.1080/01402382.2012.631310.

[33] Risse, 'The diffusion of regionalism'.

[34] Xiaoyu Pu, 'Socialisation as a two-way process: emerging powers and the diffusion of international norms', *Chinese Journal of International Politics* 5: 4, 2012, pp. 341–67, https://doi.org/10.1093/cjip/pos017.

[35] Risse, 'The diffusion of regionalism'.

[36] Thomas Risse, '"Let's argue!": communicative action in world politics', *International Organization* 54: 1, 2000, pp. 1–39 at p. 7, https://doi.org/10.1162/002081800551109.

[37] Beth A. Simmons and Zachary Elkins, 'The globalization of liberalization: policy diffusion in the international political economy', *American Political Science Review* 98: 1, 2004, pp. 171–89, https://doi.org/10.1017/S0003055404001078.

[38] Risse, 'The diffusion of regionalism'.

Understanding the substance of China's cyber-norm cluster

This section examines the substance of China's cyber norms by considering a norm cluster's tripartite nature. Despite contrary suggestions in the literature, China's cyber-governance norms are hardly static or fixed. Indeed, the cyber governance-related core values and behaviours that China has sought to promote have evolved over time, demonstrating the increasingly multidimensional nature of China's normative underpinnings in cyber governance.

Problems identified by China in global cyber governance

Close scrutiny of China's official discourses reveals a tendency to emphasize at least two major problems concerning global cyber governance. First, China has identified and acknowledged a growing range of security concerns derived from the rapid development of information and communication technologies (ICTs) and the increasing interconnectedness between physical space and cyberspace. For example, in a submission to the UN Open-ended Working Group on developments in information and telecommunications in the context of international security, China spelled out numerous existing and potential threats, such as surging cyber attacks, cybercrimes, cyberterrorism and fake news, as well as the leaking and abuse of personal data, all of which pose a significant threat to states' security and stability.[39] As one interviewee pointed out, while national security and social stability have long been the focal point of Beijing's considerations for its domestic governance of cyberspace, in recent years there has been a diversification of cybersecurity subjects in China's policy documents and political discourse.[40] This indicates that from the government's perspective, cyberspace security concerns have become increasingly multidimensional, encompassing not only national security but also issues such as economic security and individual privacy.[41]

Second, China has increasingly highlighted that 'problems with the internet such as unbalanced development, unsound regulation, and unreasonable order are becoming more prominent', with 'cyber-hegemonism' posing a new threat to world peace and development,[42] thereby demonstrating the government's growing discontent with the current framework and global cyber-governance rules. Notably, in recent years China has increasingly expressed concern that 'cyberspace is becoming increasingly militarized, politicized, and ideology-centric, over-interpreting the concept of security' in light of growing geostrategic competition in the technology domain.[43] China's official discourse further underscores that

[39] United Nations Office for Disarmament Affairs, 'China's submissions to the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security', 7 Nov. 2022, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

[40] Author's interview with a researcher from a Chinese state-led think tank, 10 July 2023.

[41] Author's interview with a researcher from a Chinese state-led think tank, 10 July 2023.

[42] State Council Information Office, 'Jointly build a community with a shared future in cyberspace', 7 Nov. 2022, http://www.scio.gov.cn/zfbps/zfbps_2279/202303/t20230320_705525.html.

[43] Permanent Mission of the People's Republic of China to the UN, 'Remarks by Amb. Zhang Jun at Security Council open debate on cyber security', 29 June 2021, http://un.china-mission.gov.cn/eng/chinaandun/securitycouncil/thematicissues/other_thematicissues/202106/t20210629_9127432.htm.

'the current distribution and management system of critical internet resources is imbalanced and unjust', with certain countries 'willfully [sic] suppress[ing] other States' ICT enterprises and impos[ing] unfair and unjust barriers on global ICT supply chain and trade, jeopardizing global development and cooperation'.[44]

China's core values in cyber governance

In response to these major problems, China has sought to promote a set of core values concerning global cyber governance, while emphasizing two relatively longstanding principles—cyber sovereignty and multilateralism—and a newly emerging norm of balancing security and development. Based on these values, the Chinese government has recommended adopting various appropriate behaviours and practices in global cyber governance.

Concerning cyberspace governance, the first fundamental value that China has long pursued, mentioned in many studies, centres on respect for sovereignty in cyberspace. This notion first gained prominence in a 2010 white paper titled 'The internet in China',[45] wherein China advocated global cooperation in cyberspace 'based on equality and mutual benefit'.[46] The five principles of international cyber-governance cooperation proposed by the Chinese delegation at the 2012 Budapest Conference on Cyberspace also included cyber sovereignty as a key element, highlighting that 'cyber sovereignty is the natural extension of state sovereignty into cyberspace and should be respected and upheld'.[47]

The concept of cyber sovereignty remains highly contested despite its proactive promotion by China as a core norm in the international arena. Some studies have found China's articulation of the norm of cyber sovereignty vague and even inconsistent across different policy documents.[48] However, analysts have identified three distinct facets within China's interpretation of cyber sovereignty—namely, national security and domestic and international governance.[49] Thus, from the perspective of national defence, cyber sovereignty is intrinsically linked to territorial sovereignty, representing a well-established norm derived from the principle of sovereignty under international law.[50] In terms of domestic governance, the possible stimulating impacts of the internet and other ICTs on widespread civil dissent and

[44] Ministry of Foreign Affairs of the People's Republic of China, 'China's positions on international rules-making in cyberspace', 20 Oct. 2021, https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405183.html.

[45] State Council Information Office, 'The internet in China', 8 June 2010, https://china.usc.edu/prc-state-council-internet-china-june-8-2010.

[46] State Council Information Office, 'The internet in China'.

[47] China Daily, 'Chinese gov't to strengthen int'l cooperation on cyber issues', 4 Oct. 2012, https://usa.chinadaily.com.cn/china/2012-10/04/content_15796970.htm

[48] Creemers, 'The Chinese conception of cybersecurity'; Alex Mueller and Christopher S. Yoo, 'Crouching tiger, hidden agenda?: The emergence of China in the global internet standard-setting arena', Research Paper no. 23–33, *Federal Communications Law Journal*, vol. 76, 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4528546.

[49] Sarah McKune and Shazeda Ahmed, 'Authoritarian practices in the digital age: the contestation and shaping of cyber norms through China's internet sovereignty agenda', *International Journal of Communication*, vol. 12, 2018, pp. 3835–55.

[50] Anupam Chander and Haochen Sun, 'Sovereignty 2.0', *Vanderbilt Journal of Transnational Law* 55: 2, 2022, pp. 283–324, https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss2/2.

disobedience, as well as increasing demands to tackle cyber risks and to enhance smart and e-governance at the domestic level, have driven China's advocacy of cyber sovereignty.[51] Consequently, when promoting the cyber-sovereignty norm, China has emphasized the right of all sovereign states to decide their own paths of cyber development, models for cyber regulation and public policies concerning the internet without foreign interference.[52] Lastly, building upon this second dimension, China envisions an international cyberspace-governance system wherein individual states have the authority to determine regulations governing internet infrastructure and activities within their borders. China has substantiated this perspective of cyber sovereignty by frequently citing universally recognized international legal principles—specifically, the principles of non-intervention and self-determination.[53]

Based on China's conceptualization, to safeguard the principle of cyber sovereignty, the government envisions numerous appropriate behaviours in global cyber governance. For example, China's official discourse emphasizes that states should exercise jurisdiction over ICT infrastructure, resources, data and ICT-related activities within their own territories[54] while having 'the right to make ICT-related public policies, laws and regulations to protect legitimate interests of their citizens, enterprises and social organizations'.[55] China also opposes any state's use of cyberspace to interfere in other states' internal affairs, highlighting that each state has the right 'to choose its online development path, its network management model, its public Internet policies and equal participation in international cyberspace governance'.[56]

The second core value of cyber governance proactively promoted by China is adherence to multilateralism, revealing China's desired model of global cyberspace governance and often seen as a contrasting or alternative norm *vis-à-vis* multistakeholderism.[57] Compared to the private sector-led multi-stakeholder approach promoted by many western states, China prioritizes a multilateral approach to governing cyberspace, emphasizing greater government involvement and a leading role for the UN in building an international consensus on rules.[58] China began signalling a multilateral approach as early as 2010, with the publication of its above-mentioned white paper advocating multilateral cooperation to address the increasingly serious problem of transnational network crimes. In particular, the document stressed the Chinese government's pivotal role in internet adminis-

[51] Zeng et al., 'China's solution'; author's interview with a researcher from a Chinese state-led think tank, 10 July 2023.

[52] Ministry of Foreign Affairs of the People's Republic of China via Xinhua, 'Full text: International strategy of cooperation on cyberspace', 1 March 2017, http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm.

[53] Yoo and Mueller, 'Crouching tiger'.

[54] Ministry of Foreign Affairs, 'China's positions on international rules-making in cyberspace'.

[55] Ministry of Foreign Affairs, 'China's positions on international rules-making in cyberspace'.

[56] Xi Jinping, 'Remarks at the opening ceremony of the Second World Internet Conference', 16 Dec. 2015, https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/.

[57] Gao, 'An attractive alternative?'.

[58] Cuihong Cai, 'Global cyber governance: China's contribution and approach', *China Quarterly of International Strategic Studies* 4: 1, 2018, pp. 55–76, https://doi.org/10.1142/S2377740018500069.

tration.[59] In 2015 Lu Wei, then head of the Cyberspace Administration of China, explained the major difference between a multi-stakeholder and a multilateral approach, describing the former as following a 'people-centred' logic that allows all stakeholders in cyber governance to make rules on an equal footing, while in the latter the state sets the rules based on the idea of cyber sovereignty.[60]

For China, promoting the norm of multilateralism in cyber governance is primarily driven by two different yet interrelated considerations. Specifically, in contrast to China's approach, the private sector-led multi-stakeholder approach inevitably leads to cross-border, private, distributed internet architecture, posing a threat to state sovereignty.[61] Therefore, multilateralism, as an alternative norm, places states and public authorities at the centre of the governance framework. Additionally, since China has long been dissatisfied with the existing normative cyber governance framework primarily devised and shaped by the western camp, it can rectify what it considers an 'unjust and imbalanced' system of global cyber governance by pursuing multilateralism as an alternative mode of governance.[62] Based on multilateralism, China has explicitly highlighted appropriate behaviours and actions, proposing that no state should seek hegemony in cyberspace governance[63] and asserting that the UN should play a prominent role in encouraging the development of cyber-governance norms, with all countries participating in the management and distribution of global internet resources on an equal footing.[64] Specifically, China's prioritization of a multilateral approach can be traced back to its initial pullback from engagement with the US-led ICANN during the 2000s and its support of a 2003 UN proposal that ICANN be ultimately replaced by the UN or another state-led multilateral governance body.[65] In comments to the UN Working Group on Internet Governance published in 2005, China explicitly stressed that sovereign governments and governmental organizations should play leading roles under the UN's framework. In addition, China's advocacy of multilateralism also manifests in official support for the International Telecommunication Union (ITU) over the Internet Engineering Task Force (IETF) as the key arena for setting internet standards, primarily because the former is a government-led multilateral platform, while the latter primarily adopts a multi-stakeholder approach that prioritizes the role of civil society and industry actors.[66]

The third core value pursued by China entails a growing emphasis on balancing development and security in cyberspace governance—a newly developed normative position that has received relatively limited attention in the literature. China's

[59] State Council Information Office, 'The internet in China'.

[60] Wei Lu, 'Cyber sovereignty must rule global internet', *Huffington Post*, 14 Feb. 2015, https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060.

[61] Laura DeNardis, *The internet in everything: freedom and security in a world with no off switch* (New Haven, CT: Yale University Press, 2020).

[62] Ministry of Foreign Affairs, 'China's positions on international rules-making in cyberspace'.

[63] Xi, 'Remarks at the opening ceremony of the Second World Internet Conference'.

[64] Ministry of Foreign Affairs, 'China's positions on international rules-making in cyberspace'.

[65] Michael Brener, 'Digital neocolonialism or benevolent hegemony?', *Columbia Political Review*, 6 May 2006, https://www.cpreview.org/articles/2006/05/digital-neocolonialism-or-benevolent-hegemony.

[66] Justin Sherman, 'China's war for control of global internet governance', 17 July 2022, http://doi.org/10.2139/ssrn.4174453.

intention to highlight the nexus between cybersecurity and development can be traced back to the 2010 white paper's brief, yet explicit, mention that 'internet security is a prerequisite for the sound development and effective utilization of the internet'.[67] A growing number of key official statements and policy papers concerning China's cyber-governance approaches, including Xi Jinping's often-quoted 2015 speech at the World Internet Conference (WIC),[68] have explained this normative position, as have more recent documents, such as 'China's position on global digital governance',[69] published by the Ministry of Foreign Affairs in 2023. Interestingly, in a similar way to the concept of cyber sovereignty, the norm of 'a balanced approach to development and security'[70] has evolved over time, gradually developing into a multifaceted concept with at least two dimensions. These two dimensions are concerned with China's conceptualization of cyber governance both domestically and internationally.

The first dimension focuses on a balanced strategy encompassing technological advancement, economic growth and the safeguarding of national security and public welfare, featuring the necessity of maximizing economic development opportunities while mitigating the growth of security risks derived from emerging domestic ICTs.[71] While protecting national security has long been the focus of China's domestic cyber-governance policies, recent years have witnessed an incremental shift in China's official narratives concerning this policy domain. Specifically, multiple needs—to balance the national security rationale, to protect digital infrastructure and control data flows (with growing economic imperatives) and to facilitate the development of a competitive digital economy and data market—have been increasingly recognized.[72] For example, article 12 of China's 2021 Data Security Law explicitly states that 'the state firmly places equal emphasis on safeguarding data security and protecting data development and use', implying that adherence to data sovereignty and national security principles aligns with opportunities to use data to drive innovation and the digital economy.[73]

A more recent development in China's discourse on cyber governance, the second dimension of this core value calls for a more cautious interpretation of cyber security and a more development-focused approach to cyberspace governance at the international level. Specifically, China believes that cyber governance has become increasingly militarized, politicized and ideology-centric, over-interpreting the concept of security.[74] To prevent cyberspace from becoming a new

[67] State Council Information Office, 'The internet in China'.

[68] Xi, 'Remarks at the opening ceremony of the Second World Internet Conference'.

[69] Ministry of Foreign Affairs of the People's Republic of China, 'China's position on global digital governance', 25 May 2023, https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405184.html.

[70] Ministry of Foreign Affairs, 'China's position on global digital governance', 25 May 2023.

[71] United Nations Office for Disarmament Affairs, 'China's submissions'.

[72] Xuechen Chen and Xinchuchu Gao, 'Comparing the EU's and China's approaches in data governance', in Elaine Fahey and Isabella Mancini, eds, *Understanding the EU as a good global actor: ambitions, values and metrics* (Cheltenham: Edward Elgar, 2022), pp. 209–25.

[73] Chen and Gao, 'Comparing the EU's and China's approaches'.

[74] Permanent Mission of the People's Republic of China to the UN, 'Remarks by Amb. Zhang Jun at Security Council open debate on cyber security'.

battlefield, China has proposed a more development-centred approach to promote security, calling on countries to implement more proactive, inclusive and coordinated strategies and policies to promote the balanced development of ICTs at the global level; to vigorously develop new models and new formats, such as the digital economy; and to oppose technological hegemony.[75]

Framing its commitments to cyber security from a developmental perspective can be regarded as China's effort to push back on the growing trend of securitization of China's cyber governance in the western context, especially against the backdrop of the US–China tech war. Nevertheless, in international organizations, China faces a more diverse audience that does not share similar or common cyber-governance values and regulations. Consequently, the developmental frame has enabled China to resonate with a broader audience from the international community. In particular, international organizations have tended to emphasize the synergies between China's Digital Silk Road (DSR) project and the UN's Sustainable Development Goals (SDGs). Partly as a result of China's efforts to connect these, the UN Department of Economics and Social Affairs is implementing a multi-country project to strengthen national capacities for jointly building its flagship infrastructure project, the Belt and Road Initiative, towards the SDGs.[76]

Based on this normative position, China's official discourses have featured numerous appropriate behaviours to balance development with security in cyber governance. For instance, to contest the US's longstanding dominant position in global cyber governance, China has proposed that states avoid excessively expanding and misusing security concerns to hinder and repress the rightful economic and technological growth of other states.[77] China's claim primarily derives from its growing discontent with the US's significant control over global internet resources,[78] fuelled by increasing tension between the two powers, due to the ongoing tech war as well as the West's increasing trend of securitization towards China's technology and cybersecurity policy.[79] Furthermore, China has proactively advocated that all states 'maintain an open, secure and stable supply chain of global digital products and services' and 'enhance policy coordination, promote fair and free trade and investment … and oppose trade barriers and trade protectionism [in] a global digital market'[80] to cultivate an open, inclusive, fair and just environment for digital development globally.[81] In brief, to better capture the substance of China's normative position on cyber governance, we argue that its cyber norms can be better conceptualized as a dynamic norm cluster containing

[75] Permanent Mission of the People's Republic of China to the UN, 'Remarks by Amb. Zhang Jun at Security Council open debate on cyber security'.

[76] UN Department of Economic and Social Affairs, 'Jointly building the "Belt and Road" towards the Sustainable Development Goals', undated, https://www.un.org/en/desa/jointly-building-%E2%80%9Cbelt-and-road%E2%80%9D-towards-sustainable-development-goals.

[77] Ministry of Foreign Affairs, 'China's position on global digital governance'.

[78] Xinhua, 'China urges US to stop jeopardizing cybersecurity', State Council Information Office, 8 Feb. 2024, http://english.scio.gov.cn/pressroom/2024-02/08/content_116994133.htm.

[79] Xuechen Chen and Xinchuchu Gao, 'Analysing the EU's collective securitisation moves towards China', *Asia Europe Journal*, vol. 20, 2022, pp. 195–216, https://doi.org/10.1007/s10308-021-00640-4.

[80] Ministry of Foreign Affairs, 'China's position on global digital governance'.

[81] Chen and Gao, 'Analysing the EU's collective securitisation moves'.

two major problems, three core values and a set of appropriate behaviours. The following table provides a summary of China's norm cluster in cyber governance.

Table 1: Mapping China's norm cluster in cyber governance

Problem	*Value*	*Examples of appropriate behaviour featured in China's official discourse*
Emerging and potential threats to national security and international peace	Cyber sovereignty	State as the key actor responsible for enhancing critical ICT infrastructure protection and handling security challenges. All countries should have the right to choose their own path of network development and governance model, and to participate on an equal basis in global governance of cyberspace. All countries have the right to formulate public policies, laws and regulations on cyberspace in the context of their national conditions. No country should use the internet to interfere in other states' internal affairs; or engage in or support cyber activities that endanger other states' national security.
Cyber-hegemony with an unbalanced and unjust system of cyber governance and politicization of cyberspace.	Multilateralism	No country should seek hegemony in cyberspace. The UN should play a prominent role in encouraging the development of cyber-governance norms.
Widening digital divide across different states and regions as a broader global developmental issue	Balance between security and development	Ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the internet. Refrain from overstretching and abusing the issue of security to contain and suppress the legitimate economic and technological development of other states. Maintain an open, secure, and stable supply chain of global digital products and services. Promote information infrastructure connectivity. States should enhance policy coordination, promote fair and free trade and investment, and oppose trade barriers and trade protectionism in a global digital market.

Explaining China's diffusion mechanisms

After mapping the substance of China's cyber-norm cluster, this section further unpacks the government's mechanisms for promoting and externalizing this cluster. We reveal that China has primarily relied on a combination of two different mechanisms—socialization and positive incentives—to promote its cyber norms. Our observation confirms diffusion theory's assumption that the boundaries between diffusion mechanisms are often blurred in practice.

Socialization

Our findings identify three key features underlying China's use of socialization as a key mechanism to promote its cyber norms and regulations. First, China often utilizes socialization actions within regional organizations as the initial stage of its attempts to disseminate its cyber norms internationally, since regional organizations, which are usually characterized as having a limited number of participants sharing similar norms and values, are likely to generate support for an emerging norm.[82] As a result, regional organizations' member states often adopt a unified stance on norms, consequently increasing the likelihood of norm acceptance at the international level. China's implementation of this strategy, particularly within the SCO and BRICS, has achieved certain successes.[83] For instance, heads of member states at the SCO agreed to 'encourage building a peaceful, secure, fair and open information space based on the principles of respect for state sovereignty and non-interference in the internal affairs of others',[84] demonstrating McKune and Ahmed's observation that internet sovereignty enjoys prominence and coherence among SCO members.[85] Similar norm convergence could be observed within BRICS, where, at the grouping's summit meeting in 2017, member states explicitly recognized the need to 'advocate the establishment of internationally applicable rules for security of ICT infrastructure'.[86] More recently, in the declaration issued at the 14th BRICS summit of 2022, members reaffirmed their support for the principle of multilateralism and the leading role of the UN in governing the internet.[87]

Within these regional organizations, given the high level of convergence of cyber norms aligning with China's preferred norms, China has unsurprisingly leveraged its socialization actions as the initial step in disseminating its cyber norms globally. One notable example is the SCO's defence of state sovereignty in

[82] Annika Björkdahl, *From idea to norm: promoting conflict prevention,* PhD diss., Lund University, 2002, pp. 50–51.

[83] Flonk, 'Emerging illiberal norms'.

[84] Shanghai Cooperation Organization, 'Declaration by the heads of member states of the Shanghai Cooperation Organization on building a region of lasting peace and common prosperity', 7 June 2012, https://worldjpn.net/documents/texts/SCO/20120607.D2E.html.

[85] McKune and Ahmed, 'Authoritarian practices'.

[86] BRICS Information Centre, University of Toronto, 'BRICS leaders Xiamen declaration', 4 Sept. 2017, http://www.brics.utoronto.ca/docs/170904-xiamen.pdf.

[87] BRICS Information Centre, University of Toronto, 'XIV BRICS Summit Beijing declaration', 23 June 2022, http://www.brics.utoronto.ca/docs/220623-declaration.html.

cyberspace at the international level.[88] In 2011 China and Russia, with the other SCO member states, jointly submitted a first draft of an 'international code of conduct for information security' to the UN,[89] emphasizing the respect of sovereignty in cyberspace, which most western states subsequently rejected. Despite this initial failure, an updated version was submitted to the UN in 2015, stressing the importance of internet sovereignty.[90] In March 2017, China expanded this initiative, presenting an *International cyberspace cooperation strategy* at the UN Conference on Disarmament.[91] China underscored that the updated draft rules would address universal concerns over the 'privacy of citizens and national sovereignty being violated' in cyberspace.[92]

Second, the creation of new bilateral and multilateral institutions and initiatives forms part of China's wider socialization strategy. A critical example is the World Internet Conference (WIC), held in Wuzhen, China since 2014 as a major platform for China to promote its cyber governance vision. At WIC 2015, President Xi advocated that sovereignty 'covers all aspects of state-to-state relations, which also includes cyberspace'.[93] In 2020 the WIC's organization committee launched the 'Initiative on jointly building a community with a shared future in cyberspace', proposing that 'efforts should go into conducting cooperation and dialogues at global, regional, multilateral, bilateral, and multi-party levels in a bid to enhance mutual trust among countries in cyberspace'.[94] Although the 2014 WIC declaration was poorly drafted and not signed by many attendees, in 2022 China established the WIC as an international organization headquartered in Beijing and dedicated to serving as 'a global internet platform for shared growth through discussion and collaboration'.[95] By June 2023 the WIC had 110 members from 23 countries and regions.[96] Although the WIC continues to evolve, observers note that China intends to utilize it to advocate a top-down approach to internet governance that is firmly rooted in its principles of cyber sovereignty and multilateralism.[97]

[88] Sebastian Harnisch, 'Spreading cyber-autocracy? The Shanghai Cooperation Organization and the diffusion of norms of "internet sovereignty"', in Marianne Kneuer and Thomas Demmelhuber, eds, *Authoritarian gravity centers: a cross-regional study of authoritarian promotion and diffusion* (New York: Routledge, 2020).

[89] United Nations, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, 2011, https://digitallibrary.un.org/record/710973?v=pdf.

[90] Henry Rõigas, 'An updated draft of the code of conduct distributed in the United Nations—what's new?', undated, https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new.

[91] Xinhua, 'SCO member countries propose updated cyber security draft rules to UN', State Council of the People's Republic of China, 10 Jan. 2015, http://english.www.gov.cn/news/international_exchanges/2015/01/10/content_281475037033064.htm.

[92] Xinhua, 'SCO member countries propose'.

[93] Shannon Tiezzi, 'China vows no compromise on "cyber sovereignty": Xi Jinping doubles down on the controversial concept at the 2nd World Internet Conference', *The Diplomat*, 16 Dec. 2015, https://thediplomat.com/2015/12/china-vows-no-compromise-on-cyber-sovereignty.

[94] Xinhua, 'World Internet Conference calls for shared cyberspace future', State Council Information Office, 19 Nov. 2020, http://english.scio.gov.cn/chinavoices/2020-11/19/content_76925575.htm.

[95] World Internet Conference, 'WIC welcomes first anniversary as an international organization', 13 July 2023, https://www.wicinternet.org/2023-07/13/c_902483.htm.

[96] World Internet Conference, 'WIC welcomes first anniversary as an international organization'.

[97] Justin Sherman, 'China's new organization could threaten the global internet', *Slate*, 29 July 2022, https://slate.com/technology/2022/07/china-world-internet-conference-organization-standards.html.

Additionally, China's global initiatives have been vital instruments for the socialization of its cyber norms. Examples include the Global Initiative on Data Security (2020), the China–LAS Cooperation Initiative on Data Security (2021, with the League of Arab States), the Data Security Cooperation Initiative of China+Central Asia (2022) and the Global AI Governance Initiative (2023). These initiatives, underpinned by China's prioritization of cyber sovereignty and a state-centric multilateral approach, as well as its increasing focus on balancing security with development, demonstrate China's ambition to compete with the West in advocating norms and crafting regulations for cyber governance.

Among these instruments, the Global Data Security Initiative (GDSI) provides a striking illustration of China's socialization of its cyber norms and regulations through such means. In August 2020, the US State Department launched the Clean Network Initiative, aiming to exclude Chinese technologies from the global supply chain. The GDSI was introduced the following month as a counter-response, with the goal of dispelling the US's portrayal of Chinese technologies as 'malign and untrustworthy'.[98] The GDSI proposed three principles—multilateralism, security development, and fairness and justice—to guide cyber cooperation,[99] the former two paralleling China's preferred cyber norms. The GDSI has also served as a basis for China's socialization actions within different platforms. For instance, at the SCO summit in November 2020, President Xi described the GDSI as contributing to a 'peaceful, secure, open, cooperative and orderly' cyberspace to ensure security and stability.[100]

Third, in seeking to socialize its cyber norms and regulations, China has increasingly emphasized its leadership in global standard-setting. In line with its preferred government-led standards development process, China prioritizes its socialization actions within government-led multilateral standards-developing organizations (SDOs) when exporting its standards. Because these SDOs are composed of government representatives, they are well aligned ideologically with China's favoured government-led multilateral approach to global cyber governance.[101] The Chinese government's influence is particularly striking in the ITU, the UN's specialized agency for information and communication technologies. A recent example of Chinese firms' efforts to promote China-led standards in the ITU concerns the telecommunications company Huawei's new internet protocol (IP) and subsequent IPv6+ proposal. In September 2019, Huawei submitted proposals to the ITU's Telecommunications Standardization Advisory Group (TSAG) to initiate a project based on the new IP contribution in TSAG C-83. It is noteworthy that discussions of the problems of the current version of IP standards are underway in many SDOs, particularly in the IETF. In contrast, the ITU was not initially involved in these discussions.[102] The fact that Huawei presented the

[98] Chaeri Park, 'Knowledge base: China's "Global Data Security Initiative"', *Digichina*, 31 March 2022, https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative.

[99] Park, 'Knowledge base'.

[100] Park, 'Knowledge base'.

[101] Fiona Pollock and Emily Taylor, 'Understanding China's engagement in technical standards bodies', *Democracy and Society*, vol. 18, 2021–2022.

[102] Julia Voo and Rogier Creemers, *China's role in digital standards for emerging technologies—impacts on the Netherlands*

'new IP' to the ITU, rather than the IETF, implies China's preferred engagement with government-led SDOs.

The Chinese government has leveraged more influence within the ITU by providing Chinese companies with the funds and expertise required to draft strong standards proposals. Producing proposals is a time-consuming and labour-intensive process; thus, China's actions can arguably alter the landscape of standard-making within the ITU.[103] However, observers have pointed out that some Chinese stakeholders submit proposals that are of low quality or are irrelevant to market needs.[104] In addition, an interviewee from the Ministry of Industry and Information Technology stated that 'China is still learning the rules within the ITU. There is a long way to go.'[105] Therefore, the increasing number of Chinese proposals within the ITU has not necessarily led to a high rate of success.

In recent years, despite Beijing's prioritization of socialization actions in government-led SDOs, it is worth noting that Chinese firms have been increasingly active in industry-led multi-stakeholder standards bodies. An example is Chinese firms' participation in the IETF, an important industry-led standards organization for the internet. In March 2021, Huawei and its subsidiary Futurewei sent 72 representatives to an IETF meeting, while Cisco registered 62, Google 32 and Apple only ten.[106] Similarly, the number of Chinese firms participating as voting members in the Third Generation Partnership Project (3GPP), a multi-stakeholder body responsible for setting 5G standards, has doubled in recent years, to 110 in January 2020.[107] Huawei alone has sent nearly twice as many representatives to 3GPP meetings as has Qualcomm, a US-based leading multinational corporation developing digital wireless telecommunication products and services.[108]

It is worth pointing out that even within industry-led multi-stakeholder standards organizations, Chinese firms' actions are arguably influenced by the government's preferences. Critics have stated that Chinese firms are sometimes pressured by the government to vote as a bloc.[109] A telling example concerns public criticism of Lenovo, a Chinese technology company, in 2018. In 2016, at a 5G standards-setting meeting at 3GPP, Lenovo backed Qualcomm's proposed standard instead of Huawei's. In 2018, against the backdrop of US bans on the use of Chinese telecommunications equipment, Lenovo was publicly denounced as a 'traitor' to China on account of its 2016 vote.[110] The founder of Lenovo, Liu

and Europe (Leiden: Leiden Asia Centre, 2021).

[103] Matt Sheehan and Jacob Feldgoise, 'What Washington gets wrong about China and technical standards', Carnegie Endowment for International Peace, 27 Feb. 2023, https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards.

[104] US–China Business Council, *China in international standards setting: USCBC recommendations for constructive participation*, 2020, https://www.uschina.org/reports/china-international-standards-setting.

[105] Authors' interview with a member of staff of the Ministry of Industry and Information Technology, Beijing, 8 July 2023.

[106] Pollock and Taylor, 'Understanding China's engagement'.

[107] Daniel R. Russel and Blake H. Berger, *Stacking the deck: China's influence in international technology standards setting* (Asia Society Policy Institute, 2021), https://asiasociety.org/sites/default/files/2021-11/ASPI_StacktheDeck-report_final.pdf.

[108] Russel and Berger, *Stacking the deck*.

[109] US–China Business Council, *China in international standards setting*.

[110] Frank Hersey, 'Lenovo founder in public backlash for "unpatriotic 5G standards vote"', *Technode*, 16 May 2018,

Chuanzhi, had to release a public statement amid an increasingly tense public backlash, stating that 'Chinese companies should be united and cannot be played off against one another by outsiders'.[111] The possibility of Chinese firms' government-coordinated voting raised concerns over the government's manipulation of the standard-setting process in SDOs. Nevertheless, the consensus-based nature of voting rules in industry-led SDOs makes it difficult for a single participant to push its preferred vision through those of other parties.[112] Therefore, observers have pointed out that there is no need to exaggerate the Chinese government's influence on industry-led SDOs.[113]

To summarize, China has conducted socialization actions within various SDOs to export its cyber regulations, including prioritizing its leadership role in government-led standards organizations and increasing the participation of Chinese firms in industry-led ones. The increasing number of Chinese proposals combined with possible coordinated voting could potentially strengthen China's ability to set standards in SDOs. However, in practice, due to the low quality of some Chinese proposals and the consensus-based nature of voting rules in most SDOs, China's socialization actions in SDOs have not always achieved success.

Positive incentives

China's socialization actions are often intertwined with positive incentive mechanisms, especially when China promotes its cyber norms alongside likeminded actors. Specifically, these mechanisms can be divided into the following two main categories: providing financial support and digital infrastructure, and facilitating information exchange and collaborative actions.

For example, the DSR project can be regarded as a critical component of China's positive incentive mechanisms. Under the umbrella of DSR, China is seeking to strengthen its 'discursive power'[114] and to expand its cyber norms and regulations by providing physical infrastructure, including 5G technology, fibre-optic cables that transmit data, and data centres that store data, in the digital sphere. China is engaged in digital infrastructure projects in approximately 80 countries and has invested US$79 billion in DSR projects globally, according to the RWR Advisory Group,[115] setting the stage for it to further its own standards in these countries. Countries that have chosen specific companies to construct digital infrastructure face a path-dependent effect—that is, the difficulty of switching to another company due to sunk costs that might be caused by shifts and technical

https://technode.com/2018/05/16/lenovo-huawei-5g.

[111] Liu Chuanzhi, Yang Yuanqing and Zhu Linan, "Xingdongqilai, shisidayinglianxiangrongyubaoweizhan" [To arms, win the defensive battle for Lenovo's honour!], 16 May 2018, https://mp.weixin.qq.com/s/JDlmQbG-Fkxu-_D2jsqNz3w.

[112] Sheehan and Feldgoise, 'What Washington gets wrong'.

[113] Sheehan and Feldgoise, 'What Washington gets wrong'; US–China Business Council, *China in international standards setting*.

[114] Author's interview with a researcher from a Chinese state-led think tank, 10 July 2023.

[115] Clayton Cheney, 'China's Digital Silk Road: strategic technological competition and exporting political illiberalism', Pacific Forum, July 2019, https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf.

compatibility. Consequently, Chinese companies' construction of digital infrastructure increases the possibility of China's preferred technical standards gaining adoption in these countries. For instance, with its digital infrastructure construction in African countries, Huawei is strongly inclined to push its preferred network solutions—namely, the IPv6 approach. In 2022, Huawei co-released a white paper with the African Telecommunication Union on IPv6 development in Africa, intended to guide the innovation and development of IPv6 technology across the continent.[116] These countries' use of Huawei's digital infrastructure and network technologies makes any future shift to alternatives increasingly challenging, leading to path-dependence effects and therefore granting Huawei a competitive advantage.

China's positive incentives also occur in the form of exchanging information, providing technical assistance and undertaking joint actions. The Regional Anti-Terrorist Structure (RATS), the SCO's operational unit that was formed to promote the cooperation of member states against 'three evils' (terrorism, extremism and separatism), is China's major channel for mobilizing socialization by sharing information and through joint action.[117] Along these lines, China hosted two RATS anti-cyberterror exercises, in 2015 and 2017, and provided technical assistance and training.[118] Other examples include the creation of the first BRICS Technology Transfer Centre, in Kunming, and the first BRICS Institute of Future Networks in China, in Shenzhen.[119] Both projects demonstrate Chinese interest in promoting and strengthening BRICS technological cooperation in cyberspace. Beijing also proactively promotes information exchange by signing memorandums of understanding (MoUs) with DSR countries, calling for the mutual recognition of standards.[120] However, critics point to the fact that these MoUs are often ceremonial and have no substance.[121]

We found limited evidence indicating China's employment of negative incentive mechanisms, which stands in stark contrast to the EU's strategy for promoting its cyber norms and regulations, as exemplified by measures such as the EU General Data Protection Regulation (GDPR). This instrument is often presented as a pivotal mechanism for the EU to disseminate its cyber norms and regulations, achieved by imposing high costs for non-compliance, with potential sanctions of up to 4 per cent of a company's global turnover for GDPR violations. There is a notable overlap between China's emerging data governance framework and

[116] Huawei, 'ATU, African Union & Huawei release Africa IPv6 development white paper', Huawei Blog, 14 Nov. 2022, https://blog.huawei.com/2022/11/14/atu-african-union-huawei-release-africa-ipv6-development-white-paper.

[117] Stephen Aris, *Shanghai Cooperation Organization: mapping multilateralism in transition*, no. 2, IPI (International Peace Institute), Dec. 2013, https://www.ipinst.org/wp-content/uploads/publications/ipi_e_pub_shanghai_cooperation.pdf.

[118] McKune and Ahmed, 'Authoritarian practices'.

[119] 'BRICS set up new institutional branch to strengthen cooperation on ICT', Xinhua, 7 Aug. 2019, http://www.xinhuanet.com/english/2019-08/07/c_138289903.htm.

[120] Gao, 'An attractive alternative?'.

[121] Tim Nicholas Rühlig, *Technical standardisation, China and the future international order: a European perspective* (Brussels: Heinrich-Böll-Stiftung, 2020), p. 25.

the GDPR.[122] However, due to the elastic and evolving nature of China's cyber norms, as well as Beijing's longstanding normative commitment to respect for sovereignty and non-interference, China tends to avoid the use of negative incentives as a diffusion mechanism. Compared to the EU, China's avoidance of negative incentive mechanisms is crucial because it could potentially limit the global application of China's data governance framework as well as its broader cyber-governance framework.

Conclusion

By investigating the substance of China's cyber norm cluster, as well as the mechanisms through which it externalizes its cyber norms, this study problematizes the conventional scholarly discussions that have focused primarily on Beijing's promotion of single norms through a single mechanism. We argue that the substance of China's cyber norms can be better conceptualized as a norm cluster by taking into consideration the tripartite structure of problems, values and appropriate behaviours. Specifically, driven by its dissatisfaction with the myriad problems it has identified in the existing normative structure of global cyber governance, Beijing has sought to promote three core values—cyber sovereignty, multilateralism and the balance between security and development. Our analysis also depicts the multifaceted nature of these norms, highlighting the evolving and dynamic characteristics of China's normative position in cyber governance. Furthermore, by delving into the norm-diffusion mechanisms, we reveal that China has utilized a dynamic combination of socialization and positive incentive strategies to externalize its cyber norms. For policy-makers and policy analysts, a more nuanced investigation and a deeper understanding of the diverse nature of China's cyber-governance norms and behaviours could facilitate a better comprehension of the rationale and normative considerations that underpin China's rapidly developing policy formation and external strategies in the realm of cyber governance.

At the conceptual level, this study contributes to the development of new avenues for research on cyber norms and norm diffusion, with a particular focus on emerging cyber powers in the non-western context. While the past two decades have witnessed a growing body of literature examining the processes of norm construction and norm diffusion in the sphere of global cyber governance, existing studies focused heavily on the role of conventional norm entrepreneurs, exemplified by the UN and a relatively limited range of western liberal democratic actors such as the US, EU and NATO and offered insufficient insight into how cyber norms are conceptualized and promoted by emerging cyber powers such as China. Furthermore, drawing on the last theoretical advancements from the norm diffusion literature, we contest the reductionist understanding of cyber-governance norms as single norms. Instead, we conceptualize them as norm clusters, namely a looser collection of interlocking components comprising a specific set of problems, values and behaviours. This conceptual approach offers a more sophisti-

[122] Author's interview with a researcher from a Chinese state-led think tank, 10 July 2023.

cated and fine-grained understanding of the nature of international norms, as well as the interplay between the normative considerations of political actors and their policy choices. This understanding can be applied to the study of other empirical cases and policy sectors.

At the empirical level, our study contributes to broadening the scope of empirical research on China's cyber-governance norm entrepreneurship while identifying additional avenues for further research. First, it unpacked the multifaceted nature of China's cyber norms, particularly emphasizing the emerging cyber norm of balancing security and development. Future research could assess whether various cyber norms advocated by China consistently align. For instance, an assessment could be made of whether China's increasing emphasis on balancing security and development undermines its advocacy for cyber sovereignty. Second, the findings reveal that China has utilized a combination of socialization and positive strategies to diffuse its cyber norms. While we did not uncover evidence showing that China uses different mechanisms of socialization for different cyber norms, it would be interesting to explore the reasons behind the selective use of mechanisms. Third, this article illustrates that the Chinese government has become increasingly proactive in promoting its own normative positions in cyber governance. However, this norm promotion process has not automatically led to the effective adoption of China's norms outside its borders. Exploring factors that hinder China's emerging role as a norm entrepreneur, such as vaguely defined cyber norms in China's official discourses, as well as a lack of coordination in crafting norm diffusion strategies between the government and private-sector entities, is an interesting avenue for future research.