Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order

Sukumar, A.M.; Basu, A.

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order

Arun Sukumar & Arindrajit Basu

To cite this article: Arun Sukumar & Arindrajit Basu (13 Dec 2024): Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order, Journal of Cyber Policy, DOI: 10.1080/23738871.2024.2436591

To link to this article: https://doi.org/10.1080/23738871.2024.2436591

Published online: 13 Dec 2024.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2024.2436591

Routledge
Taylor & Francis Group

Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order

Arun Sukumar and Arindrajit Basu

Institute of Security and Global Affairs, Leiden University, The Hague, Netherlands

ABSTRACT

Cyberspace is still characterised by features that draw from the liberal international order into which it was born: namely, open data flows and multi-stakeholder governance mechanisms that allow private actors to shape global technical or normative standards. The application of this 'liberal cyber order' has been resisted by Russia and China who seek a greater role for the territorial state in cyberspace governance. They have long sought new, binding rules to this effect with little success. The UN cybercrime convention bucks the trend of informal, non-binding agreements in this domain. Through an empirical analysis of proposals advanced by Russia and China during negotiations toward the cybercrime convention, this article demonstrates how they have sought to use it to develop rules that blunt the advantages enjoyed by Western liberal economies and major transnational actors in the current order. Going beyond the regulation of cybercrime, Russian and Chinese proposals empower states to thwart disruptive and intelligence-gathering cyber operations that may be conducted globally by Western adversaries. Additionally, they enhance the state's regulatory capacity over private actors at home and abroad, limiting the ability of businesses or NGOs to shape cybersecurity and human rights standards around the transfer, retention and access of data.

ARTICLE HISTORY
Received 23 May 2024
Revised 3 October 2024
Accepted 24 October 2024

KEYWORDS
Cybercrime treaty; cyber sovereignty; liberal international order; cybersecurity governance

1. Introduction

What kind of global governance regime do China and Russia seek for cyberspace? As authoritarian states with strong restrictions on the online activities of individuals, businesses and NGOs, do they simply seek greater autonomy to regulate digital technologies in their territory without foreign intervention? China and Russia have been robustly engaged, for over two decades, in discussions on internet governance at the International Telecommunications Union (ITU) (Murgia and Gross 2020; Yoo 2023), regional cooperative institutions and multi-stakeholder entities such as the Internet Corporation for Assigned Names and Numbers (ICANN) (Kennedy 2013; Negro 2020; Yan 2015). Chinese and Russian

CONTACT Arun Sukumar a.m.sukumar@fgga.leidenuniv.nl

proposals advanced at these forums have the effect of increasing states' capacity to manage the territorial conduct of private actors.

The proposals advanced by both states at international forums also signal their geopolitical interests in cyberspace. Discussions on international cybersecurity in the UN General Assembly's First Committee, where Russia and China have competed with the 'like-minded'[1] countries led by the United States and European Union on specific proposals, throw into relief those interests (Basu, Poetranto, and Lau 2021; Tiirmaa-Klaar 2021). Through their First Committee proposals, Russia and China have sought to limit the ability of Western adversaries to engage in offensive cyber operations against their digital assets and infrastructure, and simultaneously to legitimize their own strategies and practices (for example, their increasing use of proxies or 'cyber mercenaries') (Maurer 2017; Sukumar 2017).

By dint of institutional design and the fragmented nature of the cyber 'regime complex' (Nye 2014), discussions on internet governance, cybercrime and norms of responsible state behaviour in cyberspace have hitherto taken place across a number of international forums. This fragmentation has occluded from analysis a complete picture of the systemic changes that Russia and China pursue for the governance of cyberspace. Given that they are major cyber powers, it is important to understand whether and why both states seek to influence how other states govern territorial networks to advance their own broader geopolitical and geoeconomic ambitions for the domain. For instance, China and Russia would want for other states to have greater agency over domestic networks, whether for the purpose of requesting them to thwart Western cyber operations, curtail the growing influence of Western technology companies whom they see as proxies of the US or its allies, or clamp down on foreign voices and institutions critical of them. Conversely, implementing tougher restrictions on online activity at home may often require China and Russia to seek data from abroad for investigative and prosecutorial purposes. For such data requests to succeed, states must not only be aligned on what counts as criminal activity in cyberspace, there should also be few procedural hurdles for interstate data transfers. These objectives require a major reconfiguration of the way in which states currently engage with each other in cyberspace, and with private actors both domestically and internationally.

To be sure, Russian and Chinese objectives for cyberspace governance differ in important respects. As Flonk notes, Russia relies more on policy-oriented measures to regulate internet infrastructure, users and networks than China, where technical infrastructure such as the Great Chinese Firewall allows for a high degree of centralisation over content control and platforms governance (Flonk 2021). Secondly, with significantly higher economic stakes in cyberspace, China's geopolitical outlook differs somewhat from Russia's. China's cyber diplomacy and proposals are driven by a desire to support Chinese technology companies while seeking a significant degree of state control over ICT activities at home and abroad. Russia, on the other hand, does not have a significant domestic technology industry and is therefore arguably less concerned about the geoeconomic consequences of its cyber diplomacy (Broeders, Adamson, and Creemers 2019). Finally, China is more selective than Russia in the execution of cyber operations. While Moscow undertakes a broad range of disruptive and destructive cyber operations, including those aimed at systemic political destabilisation, Beijing has restricted itself to undertaking operations that incrementally advance its economic or security objectives. The difference could be attributed to the blowback that Chinese industry and states agencies would face as good-faith participants and key influencers of standards development

(Russel and Berger 2021) and digital markets were they to undertake cyber operations that cause widespread instability or degrade the availability of global internet services.

These differences notwithstanding, scholars have long highlighted the strong convergence of views between Russia and China in their ideological opposition to the liberal international order and to its application to cyberspace. This 'liberal cyber order' is marked not only by substantive norms that govern state behaviour in cyberspace but also by who sets those norms (Rovner 2023). Open data flows, multi-stakeholder governance mechanisms and deference to the exercise of civil, political and economic liberties online constitute the defining characteristics of the liberal cyber order, whose influence on the internet is historical and still discernible (Deibert and Crete-Nishihata 2012; Farrell and Newman 2021; Hollis and Raustiala 2022). In geopolitical terms, this order privileges liberal democracies and their constituents – in particular the United States and its trans-Atlantic allies who have helped incubate the growth of the internet since its early years – as rule-shapers (Farrell and Newman 2021, 2024). China and Russia are united in their goal to 'reform the liberal cyber order' (Wu 2021), which includes upending liberal norms (Flonk 2021) as well as the institutional governance mechanisms that are its mainstay (Raymond and Sherman 2024). China and Russia are not the only actors who seek a 'post-liberal cyberspace' (Barrinha and Renard 2020), but they are certainly its most powerful proponents, and frequent fellow travellers in diplomatic forums.

This article highlights Russian and Chinese efforts to orchestrate such a systemic reform or reconfiguration of the liberal cyber order through the proposed cybercrime convention currently negotiated by an Ad Hoc Committee (AHC) of the United Nations. While the AHC was established to develop a binding international instrument for states to tackle cybercrime – in official terms, counter the 'use of Information and Communication Technologies (ICTs) for criminal purposes' – we show that Russia and China have sought for it to regulate activities that go well beyond the treaty's intended scope. Their proposals, as this article empirically demonstrates, not only address cybercrime, but also implicate international cybersecurity governance and cross-border data access.

Chinese and Russian proposals at the AHC push for states to have greater control over digital infrastructure and activities. As this article's review of the literature highlights, this is consistent with longstanding Chinese and Russian views on cyberspace governance. Nonetheless, the AHC negotiations also demonstrate that their championing of 'cyber sovereignty' (Creemers 2020; Stadnik 2021; Thumfart 2021; Zeng, Stevens, and Chen 2017) is oriented towards specific objectives that in turn reveal China and Russia's aspirations towards systemic changes in cyberspace governance. Their proposals empower the territorial state to regulate certain cyber operations of geopolitical concern to China and Russia. In the guise of addressing cybercrime, they also allow states to shape policies and standards on the storage and security of data, to exert control over digital activities abroad that bear on territorial concerns, and to fashion the governance of cross-border data flows as an exclusively intergovernmental prerogative with few procedural or human rights safeguards. Taken together, these proposals undermine key tenets of the liberal cyber order, that, through open networks and digital markets, have conferred geopolitical and geoeconomic advantages to liberal democracies and transnational actors based largely in Western states. Indeed, we present these findings as helping to advance a theoretical frontier in the literature on Chinese and Russian approaches to cyberspace governance. Whereas extant analyses (see Section 2) have shone a spotlight

on the domestic and global impact of China and Russia's sovereignty-centric proposals, newer scholarship has begun to examine the order-level consequences of such proposals. China and Russia, these scholars note, foreground the territorial state in cyberspace for explicitly systemic objectives (Wu 2021) and have attempted 'hegemonic socialisation', i.e. persuading states who are likely to agree to order-level changes (Hulvey 2021, 2022). Meanwhile, the order-level impact of their proposals has been clearly acknowledged and addressed as such by states like Brazil and India (Basu 2024; Paulus 2024), whose support is crucial for any major change to the liberal cyber order.

Analysing cybercrime proposals by Russia and China contextually and holistically is also important because their presentation before the AHC itself cannot be considered coincidental or opportunistic. The AHC negotiations are expressly oriented towards a treaty, in contrast to the non-binding, voluntary 'norms' on responsible behaviour that have hitherto guided interstate engagement in this domain. Moscow and Beijing have long sought to set multilateral rules not only for international cybersecurity (Levinson 2021) but also for internet governance, mainly via the ITU (Radu and Gregorio 2023). Those efforts have thus far not succeeded (Grigsby 2017). Attempts by both states to promote technical standards that allow for greater state control over the governance of critical internet resources have not yet gained currency in multi-stakeholder forums that set standards for the internet (Hogeveen 2022). Given the backdrop of 'pervasive informality' (Sukumar, Broeders, and Kello 2024) in intergovernmental and multi-stakeholder models of cyberspace governance, the AHC provides a rare avenue for Russia and China to shoehorn their proposals into an instrument that binds the conduct of states.

At the time of writing, a draft convention text has been agreed upon by all participating states at the AHC. The final convention is expected to be adopted at a formal General Assembly vote later in 2024 (UNODC 2024). As our empirical findings reveal, several proposals by Russia and China were rejected in earlier versions of the AHC draft text, while some others were reintroduced by either state in later stages of negotiation. Even if those proposals fail to gain acceptance, their tabling, and in some cases, persistent diplomatic efforts to push them through, indicate the importance both states attach to them, and their contribution to systemic reordering in cyberspace.

Section 2 reviews the literature on Chinese and Russian approaches to cyberspace governance, framed against the backdrop of their broader challenge to the liberal international order. This section highlights why it is important to study their AHC proposals within this broader context, and why Russia and China have specifically sought the AHC to float those proposals. Section 3 offers a background to the cybercrime negotiations and explains how the article collected and reviewed data on Chinese and Russian AHC proposals. Section 4 forms the empirical core of this paper. It highlights various AHC proposals made by both states, dividing them into two broad categories that reflect the essence of their challenge to the liberal cyber order: one, proposals to constrain the actions of strategic Western adversaries who benefit from open digital networks, and two, proposals to enhance territorial and extraterritorial control over private actors.

2. China and Russia's challenge to the liberal cyber order

International order refers to the 'explicit principles, rules, and institutions' that manage and reflect 'core relationships' and 'settled expectations' between states (Ikenberry

2001). The liberal international order is broadly premised on three elements: freer trade and security cooperation that is based on predictable and recognised rules, cooperation through multilateral institutions that is increasingly shifting to informal mechanisms, and the progressive growth of liberal democratic values and institutional arrangements across societies (Acharya 2017; Ikenberry 2010). Applying the liberal domestic values of 'predictability, access, and representation' to international politics (Deudney and Ikenberry 1999), the LIO allows private actors – especially with transnational interests such as corporations and NGOs – to engage and seek direct representation in rules, norms or institutions (Handreider 1978; Moravcsik 2003; Scherer et al. 2006).

In recent years, international relations scholarship has extensively debated the challenge posed by 'revisionist' powers like Russia and China to the LIO across regimes such as international security, trade and climate (Johnston 2019; Lake, Martin, and Risse 2021; Weiss and Wallace 2021; Zürn 2018). The nature of Chinese and Russian challenges to the LIO differ substantially. China, according to Goddard (2018), is a 'bridging revisionist' that is likely to use the existing international economic and political order to foment 'rule-based revolution', i.e. to transform existing rules over time to those more disposed to its interests. If its geoeconomic diplomacy in particular is any indication, China does not seek an overhaul of the LIO, but 'prefers a more conservative version that emphasises Westphalian norms of sovereignty and non-interference' (Weiss and Wallace 2021). Russia, with fewer economic stakes in the LIO, has been more inclined to test its limits through 'violent action' (Goddard 2018) in contravention of basic tenets of the UN Charter and modern international relations. The outcomes of their challenges to the LIO depend in large measure on the approaches of emerging powers – with some of whom the liberal order still resonates ideologically or economically, despite their differences with the hegemon, the United States (Efstathopoulos 2021). In this regard, Russia and China's joint emphasis on 'hollowing out' the LIO into its constitutive sovereigntist elements (Johnston 2019) – the sovereign equality of states, treaty-based agreements in lieu of informal agreements, consent-based dispute settlement mechanisms – may appeal to a broader audience, including emerging powers (Dugard 2023).

The challenge posed by Russia and China to the LIO presents a necessary context to the understanding of 'cyber ordering' or the organisation of relations between states in cyberspace (Kello 2017). As Barrinha and Renard note, cyberspace was itself the creation of the liberal order – characterised by open networks as well as private and decentralised governance (Barrinha and Renard 2020). As is now widely acknowledged, various aspects of the cyber order have faced contestation from state and non-state actors in recent decades, resulting in a 'retreat of liberal values' (Barrinha and Renard 2020; Deibert and Rohozinski 2011; Mueller 2017). As powerful nation states, China and Russia present the most potent challenge to the order. The remainder of this section reviews extant scholarship that analyses the Chinese and Russian challenge to the liberal cyber order, with a particular focus on cybersecurity governance. Then it highlights why studying proposals at the AHC negotiations offer a clearer picture of the alternative framework of rules that Russia and China want in cyberspace.

2.1. Russian and Chinese approaches to global cybersecurity governance

We identify three strands of scholarship examining China and Russia's approach to cybersecurity governance. The first strand includes conceptual and empirical

assessments of the notion of cyber sovereignty, deployed discursively by both countries in domestic and international settings. This body of scholarship offers important insights into the evolution of domestic policy discourse and legislation by China and Russia to attain 'cyber sovereignty' and 'information security' respectively, two related concepts that have been at the crux of both countries' approaches to the governance of cyberspace.

China's evocation of 'cyber sovereignty' as a policy goal can be traced back to the 2010 White Paper on the internet in China published by the state council, the country's apex administrative body (Information Office of the State Council 2010). The concept has since made an appearance in speeches by China's political leadership as well as its international cyberspace strategy (People's Republic of China 2017). Tracing its discursive evolution over the years, scholars have distilled 'cyber sovereignty' into two main components (Creemers 2020; Fung 2022). The first constitutive element is the core role of the state in 'information management' (Fung 2022), mainly by asserting territorial control over both domestic and foreign non-state actors. Such control may be exerted through technical measures or regulations around online activities within its jurisdiction (Deibert 2015; Qiao-Franco 2024). Control over the information environment is also exerted by facilitating a shift in global internet governance away from multi-stakeholder processes to articulate policy or technical standards towards intergovernmental processes under the auspices of the UN (Creemers 2020; Fung 2022).

The second constitutive element of cyber sovereignty is the equality of states in cyberspace (Zeng, Stevens, and Chen 2017) which China has framed primarily in terms of the right to non-interference in a state's internal affairs. On the other hand, Russia's policy discourse on 'information security' has a longer lineage, but is essentially aligned with many of the aforesaid goals of China. First articulated in the 2000 Doctrine on Information Security, this concept is presented as a 'triad' of state, society and individual interests, whose protection from internal and external threats is ultimately the remit of the government (Stadnik 2021). Over time, Russian controls over digital networks have mimicked Chinese measures (Weber 2017). Such measures in Russia include online content filtering, mandatory data localisation, protection of critical information infrastructure and the 2019 Law on the Russian segment of the internet that aims to ward off external threats through centralised internet traffic routing and a national domain name system (Hakala and Melnchyuk 2021; Stadnik 2021). Russia has also sought the development of a legally-binding instrument for cyberspace, and to restrain states from weaponizing 'information to undermine the political, economic and social system' of others (Korzak 2021).

China and Russia's pursuit of cyber sovereignty and information security is largely animated by the survival of its political institutions and the quest for social stability. However, there is also an important global dimension to these concepts, which the second strand of scholarship unpacks (Barrinha and Turner 2024; Flonk, Jachtenfuchs, and Obendiek 2020; Gao 2022; Jiang 2010; Nocetti 2015). Analyses of Chinese and Russian proposals made at international forums have highlighted their substantive impact on users, businesses and NGOs as well as inter-state relations. Beijing and Moscow have emerged as entrepreneurs of 'illiberal norms' (Flonk 2021), relating mainly to the control of online content and the governance of digital platforms, in venues such as the Shanghai Cooperation Organisation (SCO), BRICS and the UN.

Their proposals also contribute to the creation of 'sovereigntist spheres', where states articulate policy and set standards on online content and internet governance, often superseding global, multi-stakeholder processes (Flonk, Jachtenfuchs, and Obendiek 2020). Why would other states that have benefited from global standards opt into such sovereigntist enclaves? Simmons and Hulvey note that states are 'anxious [of being] overwhelmed by global forces', among which the internet figures prominently (Simmons and Hulvey 2022). Facing a 'sovereign identity crisis' in the age of the internet, they argue, states develop 'border orientation preferences' to ensure digital policies mirror the governance of territorial boundaries (Simmons and Hulvey 2022). In this way, they try to ensure state-society relations are not destabilised by globalisation or open information flows.

Finally, a third strand of scholarship examines how China and Russia engage tactically with norms of responsible state behaviour in cyberspace (Creemers 2021; Fung 2022; Raymond and Sherman 2024). This literature has contributed significantly to the study of 'cyber diplomacy' by major powers and non-state actors. It focuses especially on the diplomatic rhetoric and narratives (Barrinha and Turner 2024; Hansel 2023) deployed by Moscow and Beijing to bolster support for their proposals (Fung 2022), as well as their gaming of multilateral negotiation procedures – supporting consensus-based agreements, limiting private participation, 'stack[ing] the deck' with illiberal initiatives (Raymond and Sherman 2024) – for the same purpose.

To summarise, China and Russia's engagement with cybersecurity governance is characterised in the literature as driven mainly by the pursuit of cyber sovereignty, i.e. the enhancement of the state's capacity to govern territorial networks and digital assets. The most conspicuous tool deployed in the pursuit of cyber sovereignty is online content control. Both states have engaged in diplomatic efforts to export their model of cyber sovereignty, especially to developing countries. The emergence of 'sovereigntist spheres' akin to China and Russia, scholars point out, is likely to cause the 'fragmentation' of the liberal cyber order (Flonk, Jachtenfuchs, and Obendiek 2020). Fragmentation, as per existing literature, could refer either to the fragmentation of regulatory regimes across jurisdictions, including liberal economies (Bradford 2023), or to the technical splintering of the internet into non-interoperable, territorial networks (Drake, Cerf, and Kleinwachter 2016). Pertinently, Mueller cautions against exaggerating the prospect of the technical fragmentation of the internet (Mueller 2017, 17, 18). Fragmentation, he notes, is possible only if a critical mass of internet-users defect from the global internet, establishing technical incompatibilities that could sustain multiple 'internets' for a significant period of time. The economic and security costs of such defections may not outweigh the network benefits (Mueller 2017; Polatin-Reuben and Wright 2014). That said, Chinese industry players like Huawei have presented proposals on technical standards on 'decentralised internet infrastructure' at the International Telecommunication Union (ITU). These proposals have been socialised by Chinese actors as 'New IP' technologies, which aim to '[reinvent] the internet's core architecture,' (Hoffmann, Lazanski, and Taylor 2020) and potentially create 'non-interoperable networks' across the globe (Sharp 2020). The main challenge to the liberal cyber order consequently lies not only in a possible technical fragmentation of the internet but in ongoing attempts to subject its governance, domestically and internationally, to the territorial state.

2.2. Significance of the Ad Hoc Committee on cybercrime

The enhanced cyber sovereignty of states, especially developing countries, allow them to resist 'US [economic and political] hegemony in cyberspace' (Gao 2022). As challengers to the liberal cyber order, this is admittedly an important goal for China and Russia. Nevertheless, as major global players themselves, both states seek rules in a sovereignty-centric cyber order that specifically benefit them, drawing in no small part on their own traditional strengths and preferences in dealing exclusively with governments abroad. The following paragraphs highlight what those goals might be, why it has been challenging for China and Russia to achieve them, and how the AHC acquires salience in this context.

As a systemic objective, China and Russia seek to constrain certain inherent advantages that Western economies enjoy in the liberal cyber order. An open and free internet – a core tenet of the liberal order – not only has normative appeal but also confers instrumental geopolitical advantages to Western liberal states (Lahmann 2021), to which both states are especially sensitive (Lokot and Wijermars 2023). 'Internet freedom', which has been a key US foreign policy goal, is also an enabler of market access for multinational corporations – many of them based in the US – to gain from digital economies around the world (DeNardis and Hackl 2015; Farrell 2006; Farrell and Newman 2021). It is a tool for soft power promotion in cyberspace, facilitating the import of Western cultural, ideological and intellectual motifs and themes by developing states (Rothkopf 1997). An open internet is also beneficial to covert and overt military, intelligence and law enforcement agencies in the West that enjoy 'home-field advantage' (Buchanan 2022) in a domain largely developed and innovated upon in liberal economies. Strategic adversaries such as China and Russia want to constrain the capabilities of the United States and like-minded countries to gather intelligence and 'persistently engage' (Goldsmith 2022; US Cyber Command 2022) digital networks to surveil and mount offensive cyber operations.

Achieving this broader goal through the reform of existing multilateral institutions has proved challenging for Russia and China. Firstly, new rules that enhance the sovereign capacities of states are likely to be incompatible with rules incubated by existing liberal regimes, in which both Russia and China are willing participants. Any attempt to coerce other states into their preferred regimes will invite retaliation or be simply ignored for other, preferential regimes (Cha 2023). Even if China or Russia were to set new rules, their challenge would be to draw away middle powers or developing countries, whose economic or security dependencies with advanced liberal economies may compel them to stick with existing regimes. The 'counterhegemonic coalitions' (Schweller and Pu 2011) that both states have sought to incubate have had little success drawing in countries that were not already in their geopolitical orbit. Initiatives such as the Shanghai Cooperation Organization's Code of Conduct on Information Security or the China-promoted Global Initiative on Data Security seem unlikely to register acknowledgment among broader multilateral initiatives (Kynge 2023). In China's case particularly, it has struggled also to shore up support for 'counter-institutionalization' in global economic governance, through initiatives such as the Belt and Road Initiative and Asian Infrastructure Investment Bank (AIIB) that do not conflict with the Bretton Woods institutions but attempt to 'decrease [their] relevance' (Zürn 2018). In the domain of international security, prospects for counter-institutionalization are likely to be even harder (Zürn 2018).

Furthermore, the world is witnessing a discernible shift towards informal global governance (Snidal 2021; Westerwinter, Abbott, and Biersteker 2021)., undermining efforts by Russia and China to create a new international order through binding rules. Empirically documented by scholars of international law and international relations, this phenomenon has catalysed the proliferation of informal alliances, ad hoc coalitions and task forces in economic and security domains (Bradley, Goldsmith, and Hathaway 2023; Reykers et al. 2023). This shift has arguably been precipitated by the US's turn towards non-binding agreements, largely for reasons of domestic politics, such as difficulties in getting Senate ratification of treaties or the lack of interest in treaty-based cooperation from populist elites (Copelovitch and Pevehouse 2019). The relative decline in traditional multilateral governance deprives China and Russia, among others, of opportunities to supplant existing rules and formal regimes. The cybersecurity regime is a prime example of this phenomenon, being characterised by 'pervasive informality' (Sukumar, Broeders, and Kello 2024). At the UN, for instance, Russia has for more than two decades sought an international treaty on cybersecurity, only to have its proposals rebuffed by Western countries (Farrell and Newman 2021). Neither the UN GGE nor the OEWG, the two main multilateral venues for discussions on international cybersecurity, has the power to bind states with its recommendations, and both have articulated in their stead voluntary norms suggesting the contours of 'responsible state behaviour' for the domain (Kavanagh 2017). Informal global governance, including in cyberspace, has paved the way for private entities to forge multi-stakeholder partnerships in various governance domains (Johnstone, Sukumar, and Trachtman 2023). In comparison to treaty negotiations, which traditionally offer limited roles for NGOs and private actors to offer substantive inputs, informal channels tend to be more open and inclusive.

The AHC negotiations arguably address both concerns for Russia and China, and explain the scope of their proposals. Although there exists an international cybercrime instrument – the Budapest Convention – it is not signed by either state, nor for that matter by the overwhelming majority of developing countries in Asia and Africa. There is little need to develop a 'counter-institutional' coalition against the Budapest Convention, when most major non-signatories have expressed their reservations about the instrument. The AHC, on the other hand, comprises all UN member states, making it easier for Russia and China to build coalitions and attract countries into their orbit on their specific proposals. To be sure, both still need to engage in diplomacy to evangelise their proposals and appear to acknowledge this reality (Barrinha and Turner 2024; Zhang and Creemers 2024). As Barrinha and Turner (2024) note, Russia even took a more accommodative stand towards non-state actor participation in the cybercrime discussions in order to shore up international support.

Secondly, the AHC discussions were very clearly geared towards a cybercrime treaty which would create binding rules. This treaty bucks the trend of informal agreements in this domain. Shoehorning proposals on cybersecurity into the cybercrime convention allowed China and Russia to address topics that either are off the table at the UN GGE or OEWG, such as cyber-enabled espionage, or do not limit the use of offensive cyber weapons by (Western) states. Consequently, their AHC proposals reflected the regulation of a whole gamut of issues that have systemic, 'order'-level effects on cyberspace. Prior to highlighting those proposals in finer detail, a brief background on the negotiations themselves is necessary.

3. Cybercrime negotiations at the United Nations

The 'Comprehensive International Convention on Countering the Use of Information and Communications Technologies (ICTs) for Criminal Purposes' negotiated by an intergovernmental Ad Hoc Committee will be the first binding UN instrument on any issue pertaining to the governance of cyberspace. The AHC was established by the UN General Assembly in 2019. Like the Budapest Convention developed by the Council of Europe – in some respects the precursor not only to this instrument but also to several regional agreements on cybercrime (Shires 2024) – the objective of the AHC is to develop global benchmarks on identifying cybercrime and enabling international cooperation to address it.

The political backdrop to the AHC negotiations is important. Neither Russia nor China are signatories to the Budapest Convention. China has stayed away from the Budapest Convention for two reasons: firstly, signing the CoE Convention would be contrary to its longstanding position that global governance, including of cyberspace, should be under the aegis of the UN; secondly, China has also argued that it was not consulted when the Budapest Convention was being drafted (Zhang and Creemers 2024). Russia, until its expulsion in 2022 from the body, remained the only Council of Europe member not to have signed the Budapest Convention. Moscow has offered three reasons for its decision: the low number of offences addressed by the Budapest Convention; the lack of official statistics regarding its implementation; and the Convention's allowing states to access data located in another state without the latter's authorisation, thereby violating its sovereignty (Ministry of Foreign Affairs of the Russian Federation 2021).

Russia has instead been a longstanding champion for a cybercrime treaty negotiated under the auspices of the UN (Gullo and Rodriguez 2023). Cybercrime discussions at the UN were previously guided through an open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (United Nations General Assembly 2011). The UN General Assembly resolution of December 2019 that established the AHC was a culmination of an effort by Russia to lay the diplomatic and procedural groundwork for a successful vote (Lederer 2019; Rowe 2020). In 2018, for example, Russia managed to push through a resolution requiring that the Secretary General collate country perspectives on cybercrime (United Nations General Assembly 2018). Importantly, this resolution was titled 'Countering the use of information and communications technologies for criminal purposes', rather than simply a 'convention on cybercrime'. The 2018 resolution marked a clear and important departure from the way 'cybercrime' had been used in international discussions, especially around the Budapest Convention and also in Expert Group discussions (Hakmeh and Tropina 2021). As the next section highlights, this shift is significant because it correlates to Russia and China seeking an expansive scope for the AHC convention by bringing a broad range of criminal activities within its ambit (Zhang and Creemers 2024).

While Europe, the United States and other like-minded states initially opposed the establishment of the AHC and did not support the Russian proposal, they have since participated actively in various negotiation sessions and intersessional consultations (Lewis and Painter 2023). The AHC negotiations commenced in 2022 with plans originally for at least six negotiating sessions. At the time of writing, all planned negotiating sessions have been completed. No consensus outcome was attained at the originally stipulated

concluding session in January 2024 and negotiators requested more time to complete deliberations. Consequently, a final session was scheduled for July-August 2024, during which a draft convention text was agreed upon by all participating countries. A General Assembly vote is expected in December 2024 to formally adopt the treaty (Digi Watch 2024). Civil society groups and human rights campaigns have criticised the final text of the treaty due to insufficient human rights safeguards; its overly broad scope and presentation alongside a General Assembly resolution that could enable the reintroduction of cyber-enabled crimes; threats to security researchers; cementing expansive surveillance powers; enabling extensive data sharing without compatible human rights standards and safeguards and a lack of provisions on government accountability (Article 19 2024; Rodriquez 2024; Tropina 2024).

The Ad Hoc Committee was made up of the representatives of all UN member states and allowed the participation of non-voting private stakeholders, including civil society organisations and technology companies.[2] The negotiations were divided into eight broad thematic clusters, which ended up as the various operating sections of the final text of the draft convention. These included general provisions, relating to: criminalisation; jurisdiction; procedural measures of cooperation, especially among law enforcement agencies; general measures of international cooperation; preventive measures; and proposals on technical assistance and information exchange as well as mechanisms of implementation.

At the first three sessions, states contributed various draft provisions that could be integrated into each cluster. In April and September 2023, states held discussions on a Consolidated Negotiating Document (CND) that was prepared by the Chair.

While Russia and China have been active in all sessions, the former was more active than the latter. At the first AHC session in early 2022, Russia even suggested that the AHC adopt the complete text of a draft convention it first published in 2021. At the second and third sessions, Russia and China made joint proposals, especially on procedural cooperation, which are elaborated upon in the next section. To be sure, while Russia and China have led efforts on proposals challenging the liberal cyber order at the AHC, other countries including Pakistan and Iran have also been vocal about specific concerns, such as removing human rights safeguards within the Convention (Bannelier 2023). While a detailed examination of these efforts is outside the scope of this paper, it is pertinent to note that Russia and China are not working in isolation but often collaborating with a small coalition of states to effect their proposals.

3.1. Data collection and analysis

This article's analysis of Russian and Chinese proposals at the AHC is based primarily on a review of six documents containing proposals advanced by participating states prior to each negotiating session at the AHC. The first two documents pertain to proposals advanced separately by Russia (Russia Draft 2021) and China (China Suggestion 2022) at the first AHC negotiating session in February 2022. The subsequent two documents analysed were jointly published by Russia, China and several developing countries in June 2022 (Russia Joint Proposal June 2022) as well as in September 2022. Finally, we reviewed two versions of the Consolidated Negotiating Document (CND) – tabled in April 2023 (Ad Hoc Committee April 2023) and September 2023[3] before the AHC – that

contain red line-edits to the draft convention made by all negotiating parties. The CND/DTC was tabled by the Chair of the AHC and did not indicate in any way whether red-line edits (or even the text in black letters) were likely to find place in the final draft of the convention. States had the option to reintroduce proposals and object to existing proposals until the final stage of negotiations. Red-line edits made by states or coalitions of states are particularly valuable for our analysis as looking at them helps in attributing specific proposals to states and tracking their evolution. The Chair of the AHC additionally convened informal consultations, closed working groups on certain articles/clusters of articles and multi-stakeholder consultations. However, as details of these meetings are not on public record, they are not included in our analysis.

In addition to proposals tabled at all six negotiation sessions, we also reviewed publicly accessible oral statements made by Russia, China, the United States, the EU and other like-minded countries accessed through the United Nations Web Television (UN WebTV) portal. In all, we reviewed documentary and media sources dating from February 2022 to September 2023.[4] To triangulate our analysis, we consulted secondary literature including media coverage of the negotiations and analyses from blogs and podcasts authored by diplomats, legal practitioners and scholars.

4. Unpacking Chinese and Russian proposals at the AHC

This section highlights two sets of Chinese and Russian proposals at the AHC that, by enhancing the territorial capacity of states, attempt to limit strategic operations undertaken by their Western adversaries as well as the ability of influential non-state actors to set global technical standards or advance norms on cybersecurity and human rights. The first set of proposals seek the criminalisation of certain offensive cyber operations against critical information infrastructure (CII) and for the purpose of conducting espionage. Russia and China's goal here is to ensure that the openness of global digital networks do not allow adversaries the operational ability and freedom to execute such operations. A second category of proposals facilitate greater territorial and extra-territorial control of states over data, users and digital infrastructure. They do so not just through an expansive approach to defining crimes in cyberspace, but also through proposals to expand the jurisdiction of states over users and data abroad that are implicated in the commission of a crime in their own territories. These proposals on extra-territorial jurisdiction are complemented by those that relax procedural and human rights safeguards on the cross-border sharing of data between law enforcement agencies.

Taken *in toto*, these proposals offer an alternative framework of rules that blunt key attributes of the liberal cyber order highlighted in Section II and consequently limit the inherent advantages enjoyed by Western states and transnational private actors in this order.

Table 1 highlights both sets of proposals, along with the specific provisions or changes Russia and China have sought at various stages of the AHC negotiations.

4.1. Constraining strategic adversaries in cyberspace

China and Russia have called on states at the AHC to criminalise cyber operations targeting critical infrastructure as well as cyber-enabled espionage. To be sure, Russia and China

Table 1. Summary of relevant proposals advanced by Russia and China at the AHC.

Goals	AHC proposals	Russia	China
Goal 1: Constrain strategic adversaries advantaged by the liberal cyber order	Thwart cyber operations against critical infrastructure and critical information infrastructure (CII)	Sought to criminalise 'unlawful interference with CII' and has reintroduced the proposal after it was removed in the Chair's text of September 2023	Introduced the criminalisation of 'unlawful interference' with CII in initial proposals but did not reintroduce it after it was removed from the Chair's draft
	Declare cyber-enabled espionage without domestic legislative backing unlawful	Incorporated an expanded version of the Budapest Convention provision on electronic interception	Initial proposal on countering the collection or interception of data stored in foreign states was not subsequently reintroduced
Goal 2: Enhance territorial and extra-territorial state powers	Criminalise cyber-enabled crimes	Sought to criminalise several cyber-enabled crimes and attempted to reintroduce them in September 2023 draft	Sought initially to criminalise several cyber-enabled crimes but reintroduced only the crimes on public safety, online trafficking of drugs and laundering of proceeds of crime into the September 2023 draft
	Safeguards for mutual legal assistance requests	Pushed for the removal of safeguards that enabled the refusal of MLA for political offences or prosecutions that might amount to persecution on account of sex, race, language, religion, nationality, ethnic origin or political opinions	Didn't endorse Russia's push for deletion
	Facilitate data collection, retention and transfer between states	Advocated reforms to domestic criminal law systems that would enable the easier prosecution of crimes committed through the use of ICTs	Advocated reforms to domestic criminal law systems that would enable the easier prosecution of crimes committed through the use of ICTs
	Dilute human rights safeguards, generally and with respect to interstate data transfers	Tried to remove the provision on human rights safeguards altogether	Didn't endorse Russian proposal to remove entire provision on human rights safeguards; instead, sought to limit safeguards on cross-border data transfers between states
	Enhance jurisdiction over actors and infrastructure	Pushing for automatic jurisdiction based on effects doctrine	More balanced approach pushing for true and sufficient link to establish jurisdiction
	Exert control over private service providers	Criminalisation of the unlawful provision of service. Codes of Conduct for private service operators	Requires that private sector actors take specific measures to counter criminal activity

have arguably engaged in cyber operations that would fall foul of the same provisions they seek in this regard. Their own acts of commission have not deterred their AHC diplomacy arguably for two reasons. The first explanation is that Russia and China perceive for themselves an exceptional status in an alternative cyber order, in much the same way they routinely accuse the United States and its allies of 'hypocritical' actions that contravene the liberal order (Cai 2019, 160). Here, the distinction between the approaches of Russia and China is important. Russia has long sought binding rules against the targeting of critical infrastructure, while its conduct, both through operations undertaken by state

agencies and via state-supported private groups, has been in flagrant contradiction to those proposals (Korzak 2021). Moscow, which is more 'confrontational and disruptive' (Broeders, Adamson, and Creemers 2019) towards the liberal cyber order, is apparently comfortable with its simultaneous championing and violation of cybersecurity rules. China, on the other hand, has been less forthcoming with specific proposals for cyberspace and tends more to point out the 'double standards' (Ministry of Foreign Affairs of the People's Republic of China 2023) of the US, particularly in relation to surveillance and espionage. This distinction, as the following paragraphs show, is reflected in the two countries' degree of willingness to push their proposals at the AHC in the face of opposition – Russia more, China less so. A second, issue-specific explanation is that Russia and China have both turned increasingly towards private actors to undertake disruptive or data-gathering operations (Lonergan 2022; Maurer 2017). In contrast to Western liberal economies, which rely on cyber commands and intelligence agencies that are operationally or institutionally accountable to domestic oversight mechanisms, Russia and China's cyber statecraft is characterised by their reliance on proxies (Giles 2023; Hmaidi 2023; Sherman 2022). Unsurprisingly, their AHC proposals criminalise only the conduct of states, allowing both states to claim plausible deniability for proxy actions and exploit the challenges of legally attributing proxy cyber operations to governments. Chinese and Russian proposals at the AHC specifically take aim against US policies such as 'persistent engagement' and 'defend forward', which seek to disrupt 'malicious cyber activity at its source' through the 'proactive' monitoring of foreign networks by US government agencies (Fischerkeller and Harknett 2019; US Cyber Command 2022).

4.2. Critical infrastructure and cyber operations

The protection of CI has been discussed at the UN GGE and OEWG for nearly a decade. In 2015, the UN GGE articulated a norm calling on states to 'not conduct or knowingly support ICT activity' that 'intentionally damaged critical infrastructure or otherwise [impaired]' its use (Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2015). Since its publication, several multi-stakeholder and intergovernmental bodies have articulated their own version of the norm, specifying either guidelines around state behaviour with respect to CI or identifying certain sectors as 'critical' and therefore deserving of protection (Kouloufakos 2023). Turning the attention of the UN GGE towards the protection of CI has been a longstanding goal of all major actors involved in the process, but in Russia's case, its proposals should also be viewed in the broader geopolitical context of its diplomacy towards a cybersecurity treaty at the UN (Lilly and Cheravitch 2020).

Moscow's pursuit of a UN cybersecurity treaty was itself an attempt to constrain the development and use by the US and its allies of cyber offensive capabilities and generally limit the (then) advantages that the latter had in this domain (Croft 2012; Demidov and Chernenko 2015). The GGE format of discussions was the result of a US-Russia compromise to develop a 'framework of responsible state behaviour' through voluntary guidelines in lieu of a new treaty. The 2015 UN GGE's norm on the protection of CI, however, limited only those actions that would violate a state's obligations under existing international law. In other words, the norm concerned itself exclusively with cyber operations that either qualified as a 'use of force' or otherwise resulted in a major loss of functionality or

physical effects (Haataja 2023). Intelligence or espionage operations, including those with the intent of embedding themselves within critical infrastructure for the purposes of deploying countermeasures or 'active cyber defence' measures (Broeders 2021) would be potentially excluded. The sixth UN GGE in 2021 affirmed this view (Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2021).

With the GGE process not delivering the outcome it hoped for, Russia has since turned its attention towards the AHC. In 2022, the lead Russian negotiator to the UN GGE suggested that 'cybercrime is frequently used to disguise attacks against critical infrastructure [and] undermine [the] political and economic situation of governments' (Ministry of Foreign Affairs 2022). Moscow has sought to criminalise 'unlawful interference' with critical infrastructure and critical information infrastructure (CII) since the first session of AHC negotiations, notwithstanding initial opposition from the US and like-minded countries in the European Union (Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes 2023; "EU Statement – UN Ad-Hoc Committee for a UN Convention on Cybercrime: Objectives and Scope of the Convention and EEAS." 2022). Specifically, the Russian proposal suggests that parties should adopt 'legislative and other measures as are necessary under domestic law' to criminalise the creation of software or other digital information that can interfere with CII to destroy, impede or *even copy* information contained therein (Russia First Draft Article 10 bis 2021) [emphasis added]. The proposal makes clear that surveillance and intelligence-gathering operations would be covered under its remit. Further, the provision also criminalises non-compliance by private actors with government-issued guidelines related to securing CII if such non-compliance results in an attack or damage to information systems. The effect of this proposal is that multinational companies who supply or operate industrial control systems could also be implicated by domestic penal provisions.

In the UNGA First Committee, China too has called on states to refrain from targeting the 'critical infrastructures of other states' (People's Republic of China 2017). Further, China has passed domestic legislation protecting CII, imposing duties and responsibilities on operators (Data Security Law of the People's Republic of China 2021). China's first submission at the AHC sought to criminalise the 'intrusion and destruction of ICTs facilities, systems, data or CII'. The Chinese proposal seeks to criminalise not only illegal 'access' and 'interference' with computer data and 'information systems' but also the lesser 'infringement of critical information infrastructure' (China Suggestion, Article 3(1) 2021). The protection of CII is also flagged by several joint Russian and Chinese proposals on international cooperation in the AHC. One such proposal seeks an 'equal right' to states for 'the protection of its information resources and critical information infrastructures from misuse and unauthorised interference' (Russia Joint Proposal June 2022, Art. 46 (5)). As the above statements indicate, China and Russia's emphasis at the AHC is on CII, and not CI *per se*. While most countries share common perceptions of what constitutes CII (ITU-World Bank 2021; Cybersecurity Authority of Singapore 2018; Russia First Draft 2021), it is still important to distinguish it from critical infrastructure. CII refers to information or communication systems or any other network resources that are by themselves required for discharging 'vital' services within a nation or essential to the uninterrupted functioning of critical infrastructure such as industrial control systems. Broad international

convergence on many definitional aspects of CII notwithstanding, China's position in particular – underpinned by its domestic law – is notable in the present context. China's CII Security Protection Regulations, which took effect in 2021, defines CII to include systems whose 'data leakage' may 'gravely harm', *inter alia*, the 'public interest' (Data Security Law of the People's Republic of China 2021). In contrast, the EU's focus, for example, is on the destruction or disruption of such infrastructure. Consistent with Russian proposals (Russia First Draft 2021, Article 11), and reading China's AHC proposals alongside its domestic regulation (China's Suggestion 2021, Article 3(2)), it would appear that Beijing has pursued a catch-all approach to CII as well as actions targeting such infrastructure that would be proscribed (including surveillance and espionage).

While the Russian proposal on CII was removed in the Draft Text of the Convention (DTC) tabled by the AHC Chair before the Sixth Negotiating Session in September 2023, Moscow proposed its reintroduction into the negotiating process in the final session (Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes 2023, Article 10 bis). Notably, China did not support Russia's proposal to reintroduce criminal provisions on CII. US agencies assess that the People's Liberation Army (PLA) has been targeting and compromising US critical infrastructure potentially to leverage such access during conflict (United States Department of Defense 2023; Washington Post 2023). If accurate, these assessments would partly explain China's reluctance to push harder for criminal penalties against compromising CII through a cybercrime treaty. There is also the important consideration, noted at the beginning of this article, of China's global economic interests in cyberspace which outstrip those of Russia. China arguably would consider itself better off with *some* cybercrime treaty than none at all, which Russia's maximalist bargaining threatened to do at various stages of the AHC.

4.3. Cyber-enabled espionage

A related issue on which China and Russia have both floated AHC proposals is espionage. The issue of cyber-enabled espionage has been the proverbial 'elephant in the room' as far as international cybersecurity discussions are concerned (Broeders 2024). Save for the US–China cybersecurity agreement that proscribed espionage for economic purposes (Yoo 2015), there are no major international agreements that address the issue, either in terms of legal provisions or normative guardrails. On the other hand, China and Russia have sought to use the AHC negotiations on cybercrime to address cross-border espionage. To be sure, the Budapest Convention calls on states to criminalise electronic 'interception without right' that is committed 'intentionally'. States could also require commission with 'dishonest intent' (Budapest Convention 2001, Article 3) for criminality. However, as scholars have noted, the Budapest Convention only addresses the criminality of *individual* actions, and therefore is limited in addressing state espionage (Crootof 2019; Rowe 2020).

In contrast, China proposed at the AHC negotiations to hold *states* accountable for the interception of data (China Suggestion, Article 4(1) 2022). The proposal read:

> States shall not directly collect the data stored in foreign states from enterprises or individuals by technical means bypassing network security protection measures if such measures are against the laws of that foreign state.

The proposal not only highlighted a restriction on state activity, but also specifically emphasised the need to shield 'enterprises and individuals' from espionage activities. The Budapest Convention, in comparison, only refers to interception 'to and from' computer systems. While cyber operations that 'bypass network security protection measures' could refer to both disruptive operations as well as cyber-enabled espionage, China's proposal should be read in the context of its domestic measures aimed at countering espionage. In 2023, China revised its counter-espionage law to include expansively the protection of 'documents, data, materials and items related to national security and interests' (Zhang 2023). The revision specifically emphasised cyber operations, whether destructive or intelligence-gathering in nature, that targeted critical information infrastructure and 'confidential-related units' within state organs in China. The objective of the revised law is ostensibly to discourage multinational corporations and their employees from collaborating with foreign spy agencies (Marsh and Waldersee 2023; Reuters 2023) and has even resulted in the detention of a foreign national accused of spying (*Global Times* 2023a; *Global Times* 2023b). The geopolitical context is especially significant: in light of Chinese attempts to isolate itself from much of the world in the immediate aftermath of the COVID-19 pandemic, Western intelligence agencies have publicly emphasised the need to build 'strong human intelligence capability' in the country (Barnes and Wong 2023; CGTN 2023). Through its AHC proposal, China sought not only to secure an international commitment that mirrored its domestic law but ultimately to provide it the legal imprimatur to thwart and deter US and Western intelligence operations that undermine its geopolitical or geoeconomic interests (Azcarate 2023). Meanwhile, Beijing itself has reportedly leaned on proxy actors who make use of increasingly sophisticated methods for cyber espionage, that gives it greater room for deniability. Take for instance, the use by Chinese actors of disaggregate, compromised nodes such as private servers and IoT devices that make attribution to a single group or entity challenging (Raggi 2024).

Russia's original proposal tabled at the first AHC session similarly sought to criminalise the use of 'technical means to intercept traffic data and data processed by means of ICT that are not intended for public use' (Russia First Draft 2021, Article 7). This is similar to the formulation in the Budapest Convention, although it is slightly modified to stipulate that interception carried out without 'appropriate authorisation' or in 'violation of established rules' should be unlawful. The Budapest Convention's formulation on interception, as noted previously, is more permissive towards espionage and only proscribes those operations conducted 'without right' by another state. Russia's standard is narrower, and allows for states to determine by domestic regulation what constitutes 'inappropriate' interception.

4.4. Enhancing sovereign capacity against domestic and extraterritorial threats

A second set of AHC proposals by Russia and China seeks to enhance the ability of governments to 'detect, suppress, investigate and prosecute' criminal activities – designated so by domestic law – within their own territories but also abroad (DTC September 2023, Article 1(1); Russia First Draft 2021, Article 31). The latter objective has been sought through procedural measures that ease access to electronic evidence located in other countries and the dilution of human rights safeguards, especially in relation to the

handling of data transferred between states. In promoting these proposals, China and Russia's overarching goal is arguably to limit the power of multinational technology companies as well as civil society organisations and coalitions, which are mainly based in, or draw their market strength or legitimacy from, advanced liberal economies. As highlighted previously, the effect of these proposals would be to limit the technical standard or policy-setting capacity of influential private actors on data governance and security, such as encryption and data storage. Admittedly, these proposals would also limit the ability of Chinese and Russian companies to set standards and shape policy. This outcome is in line with the heightened degrees of control, both from a policy and corporate governance perspective, that both states have exerted over their major technology players in recent years (Zhang 2024).

We study six sets of proposals within this broader category (see Table 1) that advance this objective.

4.5. Addressing 'cyber-enabled' crimes

The first category of proposals pertains to the types of crimes that can be prosecuted through the AHC convention. Both states have sought the criminalisation of 'cyber-enabled' crimes, i.e. crimes that have an ICT component relevant to their commission, as opposed to 'cyber-dependent' crimes, which fit more the traditional 'CIA' crimes – targeted by the Budapest Convention – that affect the confidentiality, integrity and accessibility of systems (Wilkinson 2023). Many of these cyber-enabled crimes relate to the publication of online content, which is tightly regulated in authoritarian states. The AHC's title itself – a committee to elaborate a treaty on 'the use of ICTs for criminal purposes' – was the effort of Russian resolutions at the UN General Assembly (Wilkinson 2023). Non-government organizations (NGOs) and civil society organisations have not only decried the inclusion of content-related crimes as posing a 'heightened risk' (Privacy International and Electronic Frontier Foundation 2022) to the exercise of human rights but also as impeding the work of journalists or whistle-blowers (Electronic Frontier Foundation 2022). Russia and China have sought also to criminalise, respectively, 'digital data to mislead the user' and the 'dissemination of false information' (Martin 2023), although these proposals have generated concern among industry and civil society (Bannelier 2023). Neither formulation appears to have made it to the final rounds of negotiations. Russia, along with a number of developing countries, also proposed an all-encompassing clause to ensure the cybercrime treaty did not 'preclude a State Party from establishing as an offence any other unlawful act committed intentionally with the use of information and communication technologies that causes significant damage', which remains a legally ambiguous threshold (DTC September 2023, Art. 15 undecies). Targeting a broad range of 'cyber-enabled crimes' mirrors domestic criminal law provisions in both China and Russia and has been viewed by some experts as a means of legitimising and exporting their domestic governance models (Iyengar, Gamer and Rathi 2023). Instrumentally, China's focus has been on crimes faced by its own law enforcement agencies (Zhang and Creemers 2024). Wider criminal provisions in domestic law and international treaty law boost state authority to assert control over individuals and companies that use cyberspace.

4.6. Provisions on mutual legal assistance, human rights, jurisdiction and non-state actors

Beyond seeking an expansive scope for the cybercrime treaty, we identify five areas where China and Russia have pushed for greater power for states to regulate digital activities at home and abroad. First, Russia has sought through the AHC convention to limit exemptions and safeguards against mutual legal assistance (MLA) requests by a state. These include rejecting clauses that allow states to refuse MLA requests for the prosecution of political offences (DTC September 2023, Art. 40 Clause 21 (c) bis) or those motivated by a 'person's sex, race, language, religion, nationality, ethnic origin or political opinions' (DTC September 2023, Art. 40 Clause 21 (c) ter).

Second, both China and Russia have advocated procedural reforms to domestic criminal law that would enable the easier prosecution of crimes committed through the use of ICTs. Russia has sought to 'ensure that electronic evidence derived or extracted from [any ICT] shall have the probative value in criminal procedure' (DTC September 2023, Article 30 bis). China and Russia have suggested that states should establish 'relevant legal procedures and technical standards for the collection, retention and provision of electronic evidence to ensure the authenticity, integrity and legality of electronic evidence' (DTC September 2023, Article 30 ter).

Third, these states have, along with others, sought to limit human rights safeguards against the prosecution of cybercrime. Russia has objected to several proposals that introduce human rights safeguards against criminal prosecution, including in the case of 'persons and groups in vulnerable situations' (DTC September 2023, Article 5(2)). Moscow has also rejected a proposal to include the effective protection of human rights as a key element of cross-border technical assistance and capacity-building (DTC September 2023, Article 54). While China has not backed Russia on the proposal to remove human rights safeguards altogether, it has resisted attempts to introduce oversight mechanisms or limitations in the way governments can process and retain personal data transferred between states under the AHC convention (DTC September 2023, Article 36 sub-clause 2). Russia has also sought the use of the term 'unlawful' across the Consolidated Negotiation Text of the AHC draft to refer to specific acts that invite criminal prosecution. In contrast, the US, EU and like-minded countries prefer the phrase 'without right', which is more commonly used in the Budapest Convention. This distinction is important: 'unlawful' actions would be determined solely on the basis of domestic legislation, whereas the more permissive formulation 'without right' acknowledges the universal legitimacy of certain actions, such as accessing a free and open public computer system, instituting 'protection activities' (such as stronger encryption or cybersecurity safeguards) with the permission of those involved in transmitting data, or those actions taken in the pursuit of human rights such as privacy or free expression (Budapest Convention 2001).

Fourth, Russia and China's efforts to regulate extraterritorial activity go beyond proposals for expansive MLA. Notably, Russia has sought to extend states' jurisdiction to cases in which 'the offence is committed wholly or partly outside [their territory] but its effect in the territory [would] constitute an offence or result in the commission of an offense' (DTC September 2023, Art. 22 sub-clause 2 c bis). Similarly, Russia has sought automatic jurisdiction for states if the 'offence is committed against the State Party' (DTC September

2023, Article 22 sub-clause 2 d). China has qualified its support to Russia's invocation of the 'effects doctrine'[5] (Estey 1997). Jurisdiction, in China's view, should be based on a 'true and sufficient' link with criminal activities, giving priority to the place where the consequence of criminal activity occurs, where it is committed and the location of the perpetrator (China Suggestion 3(7) 2022).

Finally, both states have sought explicit control over internet service providers by national agencies. Such proposals have been an integral part of all Russian and Chinese drafts and contributions made to the AHC over six negotiating sessions. In its first draft proposal submitted to the AHC, Russia included two articles that specifically address the role of the private sector and ISPs, and also sought a code of conduct for their governance (Russian Federation 2021, Article 43). China's proposals, while not as extensive, require companies and service providers to 'take technical measures and other necessary measures to effectively respond to criminal activities' (China's Suggestion 2022, Article 3 (6)). Notably, both states have sought the criminalisation of the 'unlawful provision of service', understood as the providing of essentially any digitally-enabled service with 'the intent that the service or technical support be used for the commission of any of the offences' (DTC September 2023, Article 10 ter). Presumably, the service provider's 'intent' in this case would be discerned by states themselves, which enables the prosecution of any service provider that does not restrict internet services to communities or geographic areas proscribed by the state. Given the broad scope of offences that Russia and China, along with other authoritarian regimes, want to criminalise, this proposal could severely restrict the scope of operation of Virtual Private Networks or even secure messaging platforms that are set up with the intention of enabling secure and private communication away from the gaze of the state. These proposals are notable and offer important context to what China sees as the role of ISPs in 'decentralised internet infrastructure' models that it has floated at standards bodies.

Russia's push for greater control over extraterritorial activity also throws into relief its original justification for not signing the Budapest Convention. Moscow has long expressed concerns over Article 32 of the Budapest Convention because it enables cross-border law enforcement access to territorial data without authorisation from the respective State Party. At the AHC negotiations, Russia has proposed that all cooperation under the cybercrime convention happens exclusively with the authorisation of State Parties. The cumulative effect of Russia's proposals would be that states become the sole arbiters of cross-border data access, but also have few procedural safeguards or human rights restrictions to refuse sharing data with other governments.

5. Cybercrime negotiations and the future of the liberal cyber order

Russia and China's proposals at the AHC reflect their efforts to shape systemically the governance of cyberspace, away from its liberal underpinnings. They attempt to reconfigure the norms and rules governing international relations in cyberspace by casting the territorial state as its main actor. Much like Western states have benefitted from a liberal order rooted in the dilution of the territorial state and the delegation of key cyberspace governance functions to private actors (Farrell and Newman 2021), Russia and China seek geopolitical advantages from the alternative order they propose.

Draft measures on the protection of CII and the criminalisation of cyber-enabled espionage constrain the freedom that Western intelligence agencies and commands enjoy in cyberspace for information-gathering and disruptive operations. On the other hand, stronger control over online content and the activities of digital services providers as well as weaker procedural and substantive safeguards on cross-border data-sharing between governments ensure that states can regulate private actors at home and also exert control over the data of users and entities held abroad (Harvey and Moore 2022). The goal of these proposals is to limit the autonomy and influence of (mostly) Western technology companies in determining data flows and cybersecurity outcomes through their in-house policies and technical standards (Klonick 2017).

Russia and China's pursuit of an alternative cyber order is backed by several statements on issues discussed in the paper. While a detailed examination of these statements and strategies is outside the scope of this paper, we highlight a few notable examples. Beijing's repeated references to the US's 'empire of hacking' (Reuters 2023) and Moscow's claims of US targeting critical infrastructure for subversive 'political and economic' operations suggest that their proposals at the AHC are motivated by overarching geopolitical motives, rather than by narrow domestic ones (Ministry of Foreign Affairs of the Russian Federation 2022). Further, both countries have tried to use the platform of the AHC to promote their model among developing countries through language referencing the need for a systemic shift in cyberspace governance. China has declared that the AHC treaty should 'adjust [to] and create new contours for ensuring the security of states' (China Intervention Sixth Session Morning, UN Web TV 2023, 01:01:00 to 01:07:00). This messaging has been emphasised repeatedly by the Russian delegation as well. An article written by the Deputy Head of the Russian delegation amidst the AHC negotiations argued that the 'prospects for the global digitalisation process as a whole, the effectiveness and dynamics which depend on ensuring security, are in question' (Chernukhin 2023).

Indeed, Russia and China's diplomatic strategies at the AHC appear to exploit the Global South's 'discontent' against the LIO (Endaylalu 2022). Both states have argued that debates on human rights are manufactured by states (liberal economies) who seek to 'retain their dominant position in the information sphere' at the cost of 'practical cooperation' on cybercrime (Russian Federation 2022). In other words, the messaging here is not that human rights are bad, but that developing nations have more urgent priorities which are not highlighted in the current order. Relatedly, both states have also underlined the need for new rules to prosecute cybercrime, appealing to the deeply felt sentiment among African and Asian countries to be norm-makers and not norm-takers (Acharya 2011). China's opening intervention at AHC negotiations stressed that including 'cyber-enabled crimes' in the cybercrime treaty is a way of ensuring that international law kept 'pace with the trends' (China, Intervention Sixth Session Morning, UN Web TV 2023, 01:01:00 to 01:07:00). Russia has emphasised the fact that many countries stayed away from the Budapest Convention because they were not involved in its creation (Seger 2016), denouncing the instrument as having failed to win the 'minds and hearts' of the developing world (Chernukhin 2023).

As Table 2 illustrates, Russia and China's own cyber diplomacy at the AHC has received steady support from some of its allies, but many developing countries and emerging powers (Chivvis and Geaghan-Breiner 2024) have largely remained silent in response.

Table 2. States' responses to China and Russia's proposals at September 2023 negotiations.

Goals	AHC proposals	Endorsed RU and CN in September 2023 negotiation session	Against RU and CN in September 2023 negotiation session
Goal 1: Constrain strategic adversaries advantaged by the liberal cyber order	Thwart cyber operations against CI and CII	Iran, Belarus, Burkina Faso, Venezuela and Egypt	Australia, United States, EU and its member states, New Zealand, Georgia, Norway, United Kingdom, Liechtenstein, Canada, Chile, Japan and Mexico
	Declare cyber-enabled espionage without domestic legislative backing unlawful	Not reintroduced in September 2023	
Goal 2: Enhance territorial and extra-territorial state powers	Criminalise cyber-enabled crimes	Only Egypt, Iran and Venezuela were for all cyber-enabled crimes	United Kingdom, New Zealand, United States, EU and its member states, Norway, Australia, Canada, Japan and Mexico objected to all cyber enabled crimes
	Safeguards for mutual legal assistance requests	Tanzania, Morocco and Egypt	Costa Rica, EU and its member states, Côte d'Ivoire, Lebanon, Dominican Republic, Ghana, Liechtenstein, Georgia, Guatemala, Paraguay, Brazil, Vanuatu, Australia, United States, Norway, Canada, Ecuador, Kenya, United Kingdom, Philippines, Albania, Switzerland, Algeria, Tonga, Israel and Japan
	Facilitate data collection, retention and transfer between states	Cuba, Pakistan and Belarus	Costa Rica, Canada, Australia, New Zealand, United States, Senegal, Brazil, Paraguay, Switzerland, EU and its member states, Liechtenstein, Malaysia, Colombia, Chile and Israel, Guatemala, Cabo Verde, Ecuador, United Kingdom, Albania, CARICOM, Georgia, Norway, Japan
	Dilute human rights safeguards, generally and with respect to interstate data transfers	Vietnam, Venezuela and Burkina Faso	Vanuatu, Brazil, EU and its member states, Switzerland, Georgia, Uganda, United States, Canada, New Zealand, Senegal, Namibia, Lao PDR and the Holy See
	Enhance jurisdiction over actors and infrastructure	Syria, Belarus and Nicaragua	EU and its member states, United States, Switzerland, UK, Uruguay, New Zealand, Costa Rica, Chile, Israel, South Africa, Paraguay, Liechtenstein, Colombia, Georgia, Norway, Australia and Canada
	Exert control over private service providers	Venezuela and Egypt	United Kingdom, New Zealand, United States, EU and its member states, Norway, Australia, Canada, Japan and Mexico

The Draft Text of Convention (DTC) circulated by the AHC's chair in September 2023 omitted several proposals from China and Russia, especially on the scope and coverage of 'cyber-enabled crimes' as well as protection of CII. However, Russia attempted to reinsert all those proposals back into the DTC as red-line edits. China, as Table 1 has illustrated, appears to have been less persistent in terms of reintroducing its original proposals. China's more moderate approach, as indicated in the first half of this paper, arguably reflects its heightened economic stake in cyberspace, compared to Russia's all-or-nothing strategy. Further, Russia's approach to the AHC negotiations reflects its strategy in the UN GGE and UN OEWG, where it scoped out similarly maximalist positions before engaging in

last-minute, backroom deals to secure consensus within both groups. Chinese cyber diplomacy generally tends to avoid such grand bargains, and in the AHC appears to have prioritised some of its proposals over others.

Regardless of their outcomes, it is clear from Russia and China's proposals that both states view the proposed AHC convention on cybercrime as an opportunity to chart new rules for the road for cyberspace. In a domain characterised mainly by informal norms of responsible behaviour and technical standards – a consequence of the liberal ordering of cyberspace – both states have arguably found it difficult to challenge the economic and normative clout of major private actors and to constrain the strategic advantages of powerful Western adversaries. They have sought consequently to use the prospective AHC treaty to usher in a cyber order that lends primacy to the territorial state – not only to govern domestic digital activity but also to shape international data flows and the use of offensive cyber capabilities.

Notes

1. The 'like-minded states' refer to a multilateral coalition led by the United States and EU member states committed to advancing 'norms of responsible behaviour' for states in cyberspace (Sukumar Broeders and Kello 2024).
2. Website available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
3. From the sixth AHC session in September 2023, the Consolidated Negotiating Document (CND) was referred to as the Draft Text of the Convention (DTC).
4. At the time of submission, subsequent revisions to the DTC released in November 2023 and February 2024 do not record red-line edits offered by states.
5. The effects doctrine is a principle of international law "whereby a state claims jurisdiction over a non-national for activities outside its territory simply on the basis of" effects produced in that state. *See* Grant and Barker, 2009, https://www.oxfordreference.com/display/10.1093/acref/9780195389777.001.0001/acref-9780195389777-e-720.

Acknowledgement

The authors thank Isabella Wilkinson for comments on a previous draft of this article.

Disclosure statement

The authors report that there are no competing interests to declare.

Funding

The Hague Program on International Cyber Security is supported by the Ministry of Foreign Affairs, The Netherlands.

Notes on contributors

Arun Sukumar is an Assistant Professor at Leiden University's Institute of Security and Global Affairs and a researcher with The Hague Program on International Cyber Security. His research examines the creation and interpretation of rules for responsible state behaviour in cyberspace and, more broadly, of security regimes around emerging technologies.

Arindrajit Basu is a PhD candidate at Leiden University and a Member of the Digital Democracy Network, Carnegie Endowment for International Peace. He was formerly Research Lead at the Centre for Internet and Society, India.

ORCID

Arun Sukumar http://orcid.org/0000-0001-7137-0525
Arindrajit Basu http://orcid.org/0000-0003-0768-5834

References

Acharya, Amitav. 2011. "Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World." *International Studies Quarterly* 55 (1): 95–123.

Acharya, Amitav. 2017. "After Liberal Hegemony: The Advent of a Multiplex World Order." *Ethics & International Affairs* 31 (3): 271–285. https://doi.org/10.1017/S089267941700020X.

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Fifth Session. 2023. "Consolidated Negotiating Document on the Preamble, the Provisions on International Cooperation, Preventive Measures, Technical Assistance and the Mechanism of Implementation and the Final Provisions of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes 21 April." https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf.

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. 2023. "Draft Text of the Convention." UNODC. 2 September. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf.

Article 19. 2024. "UN Cybercrime Convention: A blueprint for human rights violations." Article 19, October 18. https://www.article19.org/resources/un-cybercrime-convention-a-blueprint-for-human-rights-violations/#:~:text=ARTICLE%2019%20urges%20UN%20member,prevent%20or%20deter%20transnational%20cybercrime.

Azcarate, Cristina. 2023. "China's New Counter-espionage Law: Possible Domestic and Global effects." *Global Affairs*, 7 July. https://www.unav.edu/web/global-affairs/new-chinese-counter-espionage-law-possible-domestic-and-global-effects.

Bannelier, Karine. 2023. "The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights." *Lawfare*, 31 January.

Barnes, Julian E. and Edward Wong. 2023. "In Risky Hunt for Secrets, US and China expand global spy operations." *New York Times*, 17 September. https://www.nytimes.com/2023/09/17/us/politics/us-china-global-spy-operations.html.

Barrinha, Andre, and Thomas Renard. 2020. "Power and diplomacy in the post-liberal cyberspace." *International Affairs* 96 (3): 749–766. https://doi.org/10.1093/ia/iiz274.

Barrinha, Andre, and Rebecca Turner. 2024. "Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia and India." *Contemporary Security Policy* 45 (1): 72–109. https://doi.org/10.1080/13523260.2023.2266906.

Basu, Arindrajit. 2024. "Ideological Agnosticism and Selective Engagement: How India Sees the Global Cybersecurity Norms Debate." India in Transition (blog). https://casi.sas.upenn.edu/iit/arindrajitbasu

Basu, Arindrajit, Irene Poetranto, and Justin Lau. 2021. "The UN Struggles to Make Progress on Securing Cyberspace." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491.

Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology*. New York: Oxford University Press.

Bradley, Curtis, Jack Goldsmith, and Oona Hathaway. 2023. "The Rise of Nonbinding International Agreements: An Empirical, Comparative, and Normative Analysis." *University of Chicago Law Review*, 90. https://live-chicago-law-review.pantheonsite.io/sites/default/files/2023-09/01_Bradley_ART_Final.pdf.

Broeders, Dennis. 2021. "Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?" *Journal of Cybersecurity* 7 (1): 1–14. https://doi.org/10.1093/cybsec/tyab010.

Broeders, Dennis. 2024. "Cyber Intelligence and International Security. Breaking the Legal and Diplomatic Silence?" *Intelligence and National Security* 1–17, https://doi.org/10.1080/02684527.2024.2398077.

Broeders, D. W. J., L. Adamson, and R. J. E. H. Creemers. 2019. "A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace." https://hdl.handle.net/1887/136465.

Buchanan, Ben. 2022. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press.

Cai, Congyan. 2019. *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously*. New York: Oxford University Press.

CGTN. 2023. "Beijing Voices Concerns over CIA's Building of Spy Network in China," 24 July. https://news.cgtn.com/news/2023-07-24/Beijing-voices-concerns-over-CIA-s-building-of-spy-network-in-China-1lHvKyRGHYc/index.html.

Cha, Victor D. 2023. "Collective Resilience: Deterring China's Weaponization ofEconomic Interdependence" *International Security* 48 (1): 91–124. https://doi.org/10.1162/isec_a_00465.

Chernukhin, Ernest. 2023. "How the World Can Counter Use of ICTs for Criminal Purposes." *Jakarta Post*, 4 November. https://www.thejakartapost.com/opinion/2023/11/04/how-the-world-can-counter-use-of-icts-for-criminal-purposes-.htm.

Chivvis, Christopher S. and Beatrix Geaghan-Breiner. 2024. *Emerging Powers and the Future of American Statecraft*. 9 April. Washington, DC: Carnegie Endowment for International Peace.

Copelovitch, Mark and Jon C. W. Pevehouse. 2019. "International Organizations in a New Era of Populist Nationalism." *Review of International Organizations* 14 (2): 169–186.

Council of Europe. 2001. The Convention on Cybercrime (Budapest Convention, ETS No.185) and its Protocols. ('Budapest Convention').

Creemers, Rogier. 2020. "China's Conception of Cybersovereignty: Rhetoric and Realization." In *Digital Technologies and Global Politics*, edited by Dennis Broeders, and Bibi Van Den Berg, 107–144. London: Rowman & Littlefield.

Creemers, Rogier. 2021. "Common Destiny in Cyberspace: China's Cyber Diplomacy." In *Global East Asia: Into the Twenty-First Century*, edited by Frank N. Pieke, 263–270. Berkeley: University of California Press.

Croft, Adrian. 2012. "Russia Says Many States Arming for Cyber Warfare," *Reuters*, 25 April, sec. Energy, https://www.reuters.com/article/germany-cyber-idUSL6E8FP40M20120425.

Crootof, Rebecca. 2019. "International Cybertorts: Expanding State Accountability in Cyberspace," *Cornell Law Review* 103 (3): 565–644.

Cybersecurity Authority of Singapore 2018 "Cybersecurity Act: Frequently Asked Questions." https://www.csa.gov.sg/faqs/cybersecurity-act.

Deibert, R. 2015. "Authoritarianism Goes Global: Cyberspace Under Siege." *Journal of Democracy* 26 (3): 64–78.

Deibert, R. J. and M. Crete-Nishihata. 2012. "Global Governance and the Spread of Cyberspace Controls." *Global Governance* 18 (3): 339–361.

Deibert, Ronald and Rafal Rohozinski. 2011. "Contesting Cyberspace and the Coming Crisis of Authority." In *Access Contested*: *Security*, *Identity*, and *Resistance* in *Asian Cyberspace*, edited by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan L. Zittrain. Cambridge, MA: The MIT Press. https://doi.org/10.7551/mitpress/9780262016780.003.0006.

Demidov, Oleg, and Elena Chernenko. 2015. "The Game of Rules." *Russia in Global Affairs* 3. https://eng.globalaffairs.ru/articles/the-game-of-rules/.

DeNardis, Laura, and Andrea M. Hackl. 2015. "Internet Governance by Social Media Platforms." *Telecommunications Policy* 39 (9): 761–770.

Deudney, Daniel, and John Ikenberry. 1999. "The Nature and Sources of International Liberal Order." *Review of International Studies* 25 (2): 179–196.

Digi Watch. 2024. "UN Cybercrime Treaty Heads to Final Vote amid US Support." *Diplo Foundation*. November 15. https://dig.watch/updates/un-cybercrime-treaty-heads-to-final-vote-amid-us-support.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwachter. 2016. "Internet Fragmentation: An Overview." *Future of the Internet Initiative White Paper*. https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Dugard, John. 2023. "The Choice Before Us: International Law or a 'Rules-based International Order'?" *Leiden Journal of International Law* 36 (2): 223–232. https://doi.org/10.1017/S0922156523000043.

Efstathopoulos, C. 2021. "Southern Middle Powers and the Liberal International Order: The Options for Brazil and South Africa." *International Journal* 76 (3): 384–403. https://doi-org.ezproxy.leidenuniv.nl/10.1177002070202110429 15.

Electronic Frontier Foundation. 2022. "Letter to the UN Ad Hoc Committee to Elaborate a Cybercrime Treaty-fourth Session." 6 January. https://www.eff.org/deeplinks/2022/12/letter-un-ad-hoc-committee.

Endaylalu, Gashaw Ayferam. 2022. "The implication of the Rise of China to the US-led liberal international order: The case of One Belt and One Road Initiatives." *Chinese Journal of International Review*, 4 (1): 1–27. https://doi.org/10.1142/S2630531322500020

Estey, Wade. 1997. "The Five Bases of Extraterritorial Jurisdiction and the Failure of the Presumption against Extraterritoriality." *Hastings International and Comparative Law Review* 21 (1): 177.

"EU Statement – UN Ad-Hoc Committee for a UN Convention on Cybercrime: Objectives and Scope of the Convention | EEAS." 2022. https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-ad-hoc-committee-un-convention-cybercrime-objectives-and-scope-convention_en?s=63.

Farrell, Henry. 2006. "Regulating Information Flows: States, Private Actors, and E-commerce." *Annual Review of Political Science* 9:353–374.

Farrell, Henry, and Abraham L. Newman. 2021. "The Janus Face of the Liberal International Information Order: When Global Institutions are Self-Undermining." *International Organization* 75: 333–358.

Farrell, Henry, and Abraham Newman. 2024. *Underground Empire: How America Weaponized the World Economy*. New York: Henry Holt and Company.

Fischerkeller, Michael P., and Richard J. Harknett. 2019. "Persistent Engagement, Agreed Competition and Cyberspace Interaction Dynamics and Escalation." *Cyber Defense Review* 5 (2): 267–287.

Flonk, Daniëlle. 2021. "Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control." *International Affairs* 97 (6): 1925–1944. https://doi.org/10.1093/ia/iiab146.

Flonk, Daniëlle, Markus Jachtenfuchs, and Anne S. Obendiek. 2020. "Authority conflicts in internet governance: Liberals vs sovereigntists." *Global Constitutionalism* 2:364–386.

Fung, Courtney J. 2022. "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): 256–274. https://doi.org/10.1080/23738871.2023.2178946.

Gao, Xinchuchu. 2022. "An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model." *International Spectator* 57 (3): 15–30.

Giles, Keir. 2023. *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*. London: Royal Institute of International Affairs (Chatham House).

Global Times. 2023a. "Chinese FM Confirms Detention of Japanese National on Suspicion of Spying." 27 March. https://www.globaltimes.cn/page/202303/1288035.shtml.

Global Times. 2023b. "Japanese Citizen Placed under Compulsory Measures in Line with Law for Suspected Engagement in Espionage Activities: Chinese FM." 21 September. https://www.globaltimes.cn/page/202309/1298630.shtml.

Goddard, Stacie. 2018. "Embedded Revisionism: Networks, Institutions, and Challenges to World Order." *International Organization* 72 (4): 763–797. https://doi.org/10.1017/S0020818318000206.
Goldsmith, Jack, ed. 2022. *The United States Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*. Oxford: Oxford University Press.
Grant, John P., and J. Craig Barker. 2009. "Effects Doctrine." In *Encyclopaedic Dictionary of International Law* edited by John P. Grant and J. Craig Barker, 174. New York: Oxford University Press. https://www.oxfordreference.com/display/10.1093acref/9780195389777.001.0001/acref-9780195389777-e-720.
Grigsby, Alex. 2017. "The End of Cyber Norms." *Survival* 59 (6): 109–122. https://doi.org/10.1080/00396338.2017.1399730.
"Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security." 2021. "UN General Assembly, Seventy-sixth Session." https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement.
"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." 2015. "UN General Assembly, Seventieth Session." https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.
Gullo, Karen and Katitza Rodriguez. 2023. "UN Cybercrime Draft Treaty Timeline." *Electronic Frontier Foundation*, 7 April. https://www.eff.org/deeplinks/2023/04/un-cybercrime-treaty-timeline.
Haataja, Samuli. 2023. "Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law." *International Journal of Law and Information Technology* 30 (4): 423–443. https://doi.org/10.1093/ijlit/eaad006.
Hakala, Janne and Jazlyn Melnchyuk. 2021. "Russia's Strategy in Cyberspace." *NATO CCDCOE*. https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210.
Hakmeh, Joyce and Tatiana Tropina. 2021. "Russia's Vision for a Cybercrime Treaty." *Directions blog*. 16 September. https://directionsblog.eu/russias-vision-for-a-cybercrime-treaty/.
Handreider, Wolfgang. 1978. "Dissolving International Politics: Reflections on the Nation State." *American Political Science Review* 72 (4): 1276–1287.
Hansel, M. 2023. "Great Power Narratives on the Challenges of Cyber Norm Building." *Policy Design and Practice* 6 (2): 182–197.
Harvey, Callum, and Christopher Moore. 2022. "The client net state: Trajectories of state control over cyberspace." *Policy and Internet* 15 (1): 133–151.
Hmaidi, Antonia. 2023. *'Here to Stay' – Chinese State-Affiliated Hacking for Strategic Goals*. Berlin: Mercator Institute for China Studies (Merics).
Hoffmann, Stacie, Dominique Lazanski, and Emily Taylor. 2020. "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet." *Journal of Cyber Policy* 5 (2): 239–264.
Hogeveen, Bart. 2022. "US Candidate Beats Russian to Secure top UN Telecommunications UN Job." *The Strategist*, 7 October. https://www.aspistrategist.org.au/us-candidate-beats-russian-to-secure-top-un-telecommunications-job/.
Hollis, Duncan B., and Kal Raustiala. 2022. *The Global Governance of the Internet*. SSRN Scholarly Paper. Rochester, NY: Temple University Beasley School of Law. https://doi.org/10.2139/ssrn.4197418.
Hulvey, Rachel Anne. 2021. "Developing Order through Socialization: China's Ideological Persuasion to Build a Rules-Based Order for Cyberspace." *GigaNet Symposium*. 30 October.
Hulvey, Rachel Anne. 2022. "Cyber Sovereignty: How China is Changing the Rules of Internet Freedom." Working Paper No. 2. *UC Institute of Global Conflict and Cooperation*. June.
Ikenberry, John G. 2001. *After Victory: Institutions, Strategic Restraint and the Rebuilding of Order after Major Wars*. Princeton: Princeton University Press.
Ikenberry, John G. 2010. "The Liberal International Order and Its Discontents." *Millennium: Journal of International Studies* 38 (3): 509–521. https://doi.org/10.1177/0305829810366477.
Information Office of the State Council of the People's Republic of China. 2010. "The Internet in China." https://cryptome.org/0001/cn-internet.htm.
International Telecommunications Union - World Bank 2021. "Enhancing the Protection and Cyber-Resilience of Critical Information Infrastructure | Digital Regulation Platform." https://

digitalregulation.org/enhancing-the-protection-and-cyber-resilience-of-critical-information-infrastructure/.
Iyengar, Rishi, Robbie Gramer, and Anusha Rathi. 2023. "Russia is Commandeering the U.N. Cybercrime Treaty." *Foreign Policy*. 31 August. https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/.
Jiang, Min. 2010. "Authoritarian Informationalism: China's Approach to Internet Sovereignty." *SAIS Review of International Affairs* 30 (2): 71–89.
Johnston, Alastair Iain. 2019. "China in a World of Orders: Rethinking Compliance and Challenge in Beijing's International Relations." *International Security* 44 (2): 9–60.
Johnstone, Ian, Arun Mohan Sukumar, and Joel Trachtman, eds. 2023. *Building an International Cybersecurity Regime. Multistakeholder Diplomacy*. Cheltenham, UK: Edward Elgar Publishing.
Kavanagh, Camino. 2017. *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*. Geneva: UNIDIR.
Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.
Kennedy, Daniel. 2013. "Deciphering Russia: Russia's Perspectives on Internet Policy and Governance." *Global Partners Digital*. https://www.gp-digital.org/wp-content/uploads/pubs/FINAL%20-%20Deciphering%20Russia.pdf.
Klonick, Kate. 2017. "The New Governors: The People, Rules and Processes Governing Online Speech." *Harvard Law Review* 131: 1599–1670.
Korzak, Elaine. 2021. "Russia's Cyber Policy Efforts in the United Nations. Tallinn Paper No.11, NATO Cooperative Cyber Defence Centre of Excellence." https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf.
Kouloufakos, Triantafyllos. 2023. "Untangling the Cyber Norm to Protect Critical Infrastructures." *Computer Law & Security Review* 49: 1–12. https://doi.org/10.1016/j.clsr.2023.105809.
Kynge, James. 2023. "China's Blueprint for an Alternative World Order." *Financial Times*, 22 August. https://www.ft.com/content/8ac52fe7-e9db-48a8-b2f0-7305ab53f4c3.
Lahmann, Henning. 2021. "On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace." *Duke Journal of Comparative and International Law* 32:61–107.
Lake, David, Lisa L. Martin, and Thomas Risse. 2021. "Challenges to the liberal order: Reflections on international organization." *International Organization* 75 (2): 225–257.
Lederer, Edith M. 2019. "UN Gives Green Light to Draft Treaty to Combat Cybercrime," *Associated Press*, 28 December. https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15.
Levinson, N. S. 2021. "Idea entrepreneurs: The United Nations Open-Ended Working Group and cybersecurity." *Telecommunications Policy* 45 (6): 102–142.
Lewis, James Andrew and Christopher Painter. 2023. "The Proposed United Nations Cybercrime Convention." *Inside Cyber Diplomacy*, 7 August. https://www.csis.org/podcasts/inside-cyber-diplomacy/proposed-united-nations-cybercrime-convention.
Lilly, Bilyana, and Joe Cheravitch. 2020. "The past present and future of Russia's Cyber Strategy and Forces." In *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*, edited by T. Jancarkova, L. Lindstrom, M. Signoretti, I. Tolga, and G. Visky, 129–155. Tallinn: NATO CCDCOE Publications.
Lokot, Tetyan, and Marielle Wijermars. 2023. "The Politics of Internet Freedom Rankings." *Internet Policy Review* 12 (2): 1–35.
Lonergan, Erica. 2022. "Cyber Proxies in the Ukraine Conflict: Implications for International Norms." *Council on Foreign Relations*, 21 March. https://www.cfr.org/blog/cyber-proxies-ukraine-conflict-implications-international-norms.
Marsh, Sarah and Victoria Waldersee. 2023. "German Car Industry Urges Berlin to Address Anti-spy Laws with Beijing." *Reuters*, 25 September. https://www.reuters.com/business/autos-transportation/german-car-industry-urges-berlin-address-anti-spy-laws-with-beijing-2023-09-25/.
Martin, Alexander. 2023. "China Proposes UN Treaty Criminalizes 'Dissemination of False Information'." *The Record*, 17 January. https://therecord.media/china-proposes-un-treaty-criminalizing-dissemination-of-false-information.

Maurer, Tim. 2017. *Cyber Mercenaries: The State, Hackers and Power*. New York: Cambridge University Press.

Ministry of Foreign Affairs of the Russian Federation. 2021. "International Community has Come Closer to 'Cybercrime' Vaccine." *Ministry of Foreign Affairs of the Russian Federation*.

Ministry of Foreign Affairs of The People's Republic of China. 2023. Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on April 12,2023. MFA (blog). April 12,2023. https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202405/t20240530_11347502.html

Ministry of Foreign Affairs of the Russian Federation. 2022. "Comment by Ambassador Andrey Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security, Acting Director of the Department of International Information Security of the MFA of Russia 'Cyberspace: War or Peace?" *To Newsweek*, 22 March – Министерство Иностранных Дел Российской Федерации. https://www.mid.ru/tv/?id=1806093&lang=en.

Moravcsik, Andrew. 2003. "Taking Preferences Seriously: A Liberal Theory of International Politics." *International Organization* 51 (4): 513–553. https://doi.org/10.1162/002081897550447.

Mueller, Milton. 2017. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge, UK: Wiley.

Murgia, Madhumita and Anna Gross. 2020. "Inside China's Controversial Mission to Reinvent the Internet." Financial Times, 27 March. Accessed January 28, 2021. https://www.ft.com/content/ba94c2bc-6e2711ea-9bca-bf503995cd6f.

Negro, Gianluigi. 2020. "A history of Chinese Global Internet Governance and its Relations with ITU and ICANN." *Chinese Journal of Communication* 13 (1): 104–121.

Nocetti, Julien. 2015. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91 (1): 111–130.

Nye, Joseph. 2014. "The Regime Complex for Managing Global Cyber-activities." Global Commission on Internet Governance Paper Series, 1.

Paulus, Alexandra. 2024. *Building Bridges in Cyber Diplomacy: How Brazil Shaped Global Cyber Norms*. Cham: Springer.

People's Republic of China. 2017. "Wangluo kongjian guoji hezuo zhanlüe (International Strategy of Cooperation on Cyberspace)." 3 January. *Translation*. https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm.

People's Republic of China. 2017. "Wangluo kongjian guoji hezuo zhanlüe (International Strategy of Cooperation on Cyberspace)." China Daily (blog) 3 January, 2017. https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm.

People's Republic of China. 2022. "China Suggestions on the Scopes, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes." https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf ("China's Suggestion 2021).

Polatin-Reuben, Dana and Joss Wright. 2014. "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet." In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*.

Privacy International and Electronic Frontier Foundation. 2022. "Privacy International and Electronic Frontier Foundation's Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty." *Electronic Frontier Foundation*, December. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/PI-EFF_comments_on_consolidated_text_December_2022.pdf.

Qiao-Franco, Giangyu. 2024. "An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries?" *Global Studies Quarterly* 4:1–11.

Radu, Roxana, and Giovanni De Gregorio. 2023. "The new era of internet governance: Technical fragmentation and digital sovereignty entanglements." In *Hybridity, Conflict and The Global Politics of Cybersecurity*, edited by Fabio Cristiano and Bibi Van Den Berg, 1–15. London: Rowman & Littlefield.

Raggi, Michael. 2024. "IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders." *Mandiant*. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks.

Raymond, Mark, and Justin Sherman. 2024. "Authoritarian Multilateralism in the Global Cyber Regime Complex: The Double Transformation of an International Diplomatic Practice." *Contemporary Security Policy* 45 (1): 110–140.

Reuters. 2023. "US Companies in China Struggle with Raids, Slow Deal Approvals, Anti-Espionage Law." 29 August. https://www.reuters.com/business/raids-exit-bans-us-companies-face-growing-hurdles-china-2023-08-29/.

Reykers, Yf, John Karlsrud, Malte Brosig, Stephanie C. Hofmann, Christiana Maglia, and Pernille Rieker. 2023. "Ad hoc Coalitions in Global Governance: Short-notice, Task- and Time-specific Cooperation." *International Affairs* 99 (2): 727–745. https://doi.org/10.1093/ia/iiac319.

Rodriquez, Karitza. 2024. "The UN Cybercrime Convention: Analyzing Risks to Human Rights and Global Privacy." Just Security (blog). August 27, 2024. https://www.justsecurity.org/98738/cybercrime-convention-human-rights/.

Rothkopf, David. 1997. "In Praise of Cultural Imperialism? Effects of Globalization on Culture." *Foreign Policy* 107 (3): 38.

Rovner, Joshua. 2023. "The Liberal Cyber Order." *War on the Rocks (blog)*. 13 March. https://warontherocks.com/2023/03/the-liberal-cyber-order/.

Rowe, Brenda I. 2020. "Transnational State-sponsored Cyber Economic Espionage: A Legal Quagmire." *Security Journal* 33:63–82.

Russel, Daniel R., and Blake H. Berger. 2021. *Stacking the Deck: China's Influence in International Technology Standards Setting*. Washington, DC: Asia Society Policy Institute. https://asiasociety.org/sites/default/files/2021-11/ASPI_StacktheDeckreport_final.pd.

Russian Federation. 2022. Russia's Statements at the Sixth Session of the OEWG. https://webtv.un.org/

Russian Federation also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan. 2022. "Second Session Submission." https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf (Russia, China Second Session Submission) ('June 2022').

Russian Federation. 2021. "United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes." *UNODC*. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf ("Russia First Draft 2021").

Scherer, Andreas Georg, Guido Palazzo, and Dorothée Baumann. 2006. "Global Rules and Private Actors: Toward a New Role of the Transnational Corporation in Global Governance." *Business Ethics Quarterly* 16 (4): 505–532.

Schweller, Randall L., and Xiaoyu Pu. 2011. "After Unipolarity: China's Visions of International Order in an Era of U.S. Decline." *International Security* 36 (1): 41–72.

Seger, Alexander. 2016. "India and the Budapest Convention: Why not?" *Observer Outreach Foundation*. 20 October. https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/.

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

Sherman, Justin. 2022. "Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior." *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/.

Shires, James. 2024. "Career Connections: Transnational Expert Networks and Multilateral Cybercrime Negotiations." *Contemporary Security Policy* 45 (1): 45–71.

Simmons, Beth A., and Rachel Hulvey. 2022. "Cyberborders: Exercising State Sovereignty Online." *Temple Law Review* 95:617.

Snidal, Duncan. 2021. "Cooperation Under Autonomy: Building and Analyzing the Informal Intergovernmental Organizations 2.0 Dataset." *Journal of Peace Research* 58 (4): 859–869.

Stadnik, Ilona. 2021. "Seeking a New Order for Global Cybersecurity: The Russian Approach to Cyber-sovereignty." In *Routledge Companion to Global Cyber-Security Strategy*, edited by Scott N. Romaniuk and Mary Manjkikian, 153–164. Abingdon: Routledge.

Sukumar, Arun M. 2017. "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" *Lawfare*, 4 July. https://www.lawfaremedia.org/article/un-gge-failed-international-law-cyberspace-doomed-well.

Sukumar, Arun, Dennis Broeders, and Monica Kello. 2024. "The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-State Actors and Diplomacy." *Contemporary Security Policy* 45 (1): 7–44. https://doi.org/10.1080/13523260.2023.2296739.

Thumfart, Johannes. 2021. "The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the Covid-crisis 2020/21 as catalytic event." In *Enforcing Rights in a Changing World: Computers Privacy Data Protection (CPDP)*. Vol. 14, edited by D. Hallinan, P. de Hert, and R. Leenes, 1–44. Brussels: Hart Publishing.

Tiirmaa-Klaar, Heli. 2021. "The Evolution of the UN Group of Governmental Experts on Cyber Issues." *Cyberstability Paper Series New Conditions and Constellations in Cyber*. The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf.

"Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)." 2021. "DigiChina (blog)," 29 June. Accessed September 29, 2024. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

Tropina, T. 2024. "This is Not a Human Rights Convention!': The Perils of Overlooking Human Rights in the UN Cybercrime Treaty." *Journal of Cyber Policy* 1–21. https://doi.org/10.1080/23738871.2024.2419517.

United Nations General Assembly. 2018. "Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 65/230." https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement.

United States Department of Defense. 2023. "Military and Security Developments Involving the People's Republic of China." https://media.defense.gov/2023/Oct/19/2003323409/−1/−1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

UNODC. 2024. "United Nations: Member States Finalize a New Cybercrime Convention." 9 August.

US Cyber Command. 2022. "Cyber 101-Defend Forward and Persistent Engagement." 25 October. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

Washington Post Live. 2023. "Transcript: Securing Cyberspace: Investing in Cyber Resilience." 12 October. https://www.washingtonpost.com/washington-post-live/2023/10/12/transcript-securing-cyberspace-investing-cyber-resilience/.

Weber, Valentin. 2017. "Why China's Internet Censorship Model Will Prevail Over Russia's." *Council on Foreign Relations*. 12 December. https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.

Weiss, Jessica Chen and Jeremy L. Wallace. 2021. "Domestic Politics: China's Rise and the Future of the Liberal International Order." *International Organization* 75 (2): 635–664. https://doi.org/10.1017/S002081832000048X

Westerwinter, Oliver, Kenneth Abbott, and Thomas Biersteker. 2021. "Informal Governance in World Politics." *The Review of International Organizations* 16 (1): 1–27. https://doi.org/10.1007/s11558-020-09382-1.

Wilkinson, Isabella. 2023. "What is the UN Cybercrime Treaty?" *Chatham House*, 2 August. https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.

Wu, Chien-Huei. 2021. "Sovereignty Fever: The Territorial Turn of Global Cyber Order." *Zeitschrift Für Ausländisches Öffentliches Recht Und Völkerrecht / Heidelberg Journal of International Law* 81 (3): 651–676. https://doi.org/10.17104/0044-2348-2021-3-651.

Yan, Li. 2015. "Reforming Internet Governance and the Role of China." *Focus Asia: Perspective and Analysis*. https://www.files.ethz.ch/isn/188532/2015-LiYan-Reforming-Internet-Governance-and-the-role-of-China.pdf.

Yoo, Christopher S. 2015. "Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures." *All Faculty Scholarship*. 1540. https://scholarship.law.upenn.edu/faculty_scholarship/1540https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2541&context=faculty_scholarship.

Yoo, Christopher S. 2023. *Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Standard-setting Arena*. Philadelphia: University of Pennsylvania Institute for Law and Economics. https://laweconcenter.org/resources/crouching-tiger-hidden-agenda-the-emergence-of-china-in-the-global-internet-standard-setting-arena/.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'." *Politics and Policy* 45 (3): 432–464.

Zhang, Angela. 2024. *High Wire: How China Regulates Big Tech and Governs its Economy*. Oxford: Oxford University Press.

Zhang, Eric Siyi, and Rogier Creemers. 2024. *Towards a UN-Centric Cybercrime Treaty: Chinese positions and interests at the UN Ad Hoc Committee for a cybercrime convention*. Leiden: Leiden Asia Centre. https://leidenasiacentre.nl/towards-a-un-centric-cybercrime-treaty/.

Zhang, Marina Yue. 2023. "China's New Anti-Espionage Law Is Sending a Chill through Foreign Corporations and Citizens Alike." *The Conversation*, 27 September. http://theconversation.com/chinas-new-anti-espionage-law-is-sending-a-chill-through-foreign-corporations-and-citizens-alike-212010.

Zürn, Michael. 2018. "Contested Global Governance." *Global Policy* 9 (1): 138–145.