A historical explanation of Chinese cybersovereignty

Tai, K.; Zhu, Y.Y.

International Relations of the Asia-Pacific Volume 22, (2022) 469–499
https://doi.org/10.1093/irap/lcab009 Advance Access published on 25 January 2022

A historical explanation of Chinese cybersovereignty

Katharin Tai[1] and Yuan Yi Zhu [2,*]

[1]*Department of Political Science, Massachusetts Institute of Technology, Cambridge, MA, USA;* [2]*Nuffield and Pembroke Colleges, University of Oxford, UK*
**Email: yuanyi.zhu@politics.ox.ac.uk*

Both authors contributed equally to this article.
Accepted 18 June 2021

Abstract

In recent years, China has become one of the most prominent voices in the debate on the future of Internet governance, in part through the aggressive promotion of what it calls a doctrine of "cybersovereignty". To date, studies of Internet governance have primarily focused on China's diplomatic efforts in this area from a security perspective and emphasized the explanatory power of China's authoritarian system when discussing the concept's underlying logic. However, relatively little attention has been paid to the historical origins of China's vision of a sovereigntized Internet, which predate the People's Republic of China and are crucial to understanding cybersovereignty in all its dimensions. This article aims to fill this gap by putting China's cybersovereignty doctrine into its proper historical context. It first charts the rise of cybersovereignty, notably through an examination of the extensive Chinese literature on the concept. The article then turns to historical antecedents for cybersovereignty within Chinese policy discourse. We argue that cybersovereignty should

be understood as part of a tradition which we describe as "compound sovereignty", a discursive strategy of legitimation which arose from China's distinctive historical experiences with the idea of sovereignty, and which is used as a strategy of legitimation and reassertion for state authority. By cross-pollinating cyber studies with insights from historical International Relations scholarship, we seek to present a less presentist, more historically anchored and methodologically diverse approach to the study of global Internet governance.

1 Introduction

Cybersovereignty has come to be understood as a core part of Chinese Internet policy, both at home, in maintaining the world's most complex and extensive censorship regime, and abroad, where China's rise as a Great Power is coinciding with the establishment of norms for international Internet governance. While the exact content of the concept is unclear, it is commonly associated with China and its existing regime of content control and Internet censorship. However, the slippery nature of cybersovereignty makes substantive study difficult, which might be one of the reasons detailed explorations in the existing literature have been sparse. In media reporting and literature on international Internet governance, China's nature as an authoritarian, one-party tends to feature as the explanation for Beijing's defense of cybersovereignty. Additional attention has been paid to a potential alliance with Russia (Margolin, 2016; Wei, 2016), which is commonly explained with reference to their shared interests as non-democratic international actors.

In this article, we argue that the focus on the linkage between China's regime type and cybersovereignty obscures an important part of the story. Beijing's choice of sovereignty-based rhetoric as the anchor for its concerns in international Internet governance and the concept's many internal inconsistencies may in fact be better understood as a Chinese rather than an authoritarian phenomenon. While Beijing could have chosen other rhetorical vehicles for its concerns, the concept of cybersovereignty, both in its initial domestic and later international use, is best understood as a function of Chinese historical understandings of sovereignty and their centrality to Chinese political discourse, rather than as a function of its political regime. This strategy, in turn, builds on the centrality of sovereignty in Chinese domestic discourses

and its function as a source of political legitimacy for political actors even before the founding of the People's Republic of China.

We draw on original research on both Chinese domestic discourse on cybersovereignty and historical research on the integration of the concept of state sovereignty into Chinese political discourses in the nineteenth and twentieth centuries. Building on Constructivist theories of International Relations, we frame the emergence of cybersovereignty within the context of China's historically contingent experiences of the notion of sovereignty, which have led to its extensive use, often through what we term 'compound sovereignty', within domestic Chinese policy discourse. It should be noted that explaining cybersovereignty as an outgrowth of Chinese history does not preclude it from being mobilized in the service of authoritarian governance and other autocratic interests. On the contrary, one of the core features of compound sovereignties has been their variability across policy areas. Nevertheless, we believe that the historical background to the emergence of cybersovereignty is necessary to understand its function within Chinese policy discourse.

2 Theoretical framework

China's development over the past three decades has led to a range of debates about the nature of its rise, so much so that 'peaceful rise' briefly became part of Chinese foreign policy (e.g. Glaser and Medeiros, 2007). This debate has also caused additional interest in the sources of Chinese foreign policy. We aim to contribute to this debate by pointing to the importance of a decade-old continuity, the centrality of sovereignty discourses and compound sovereignty in Chinese domestic policy discourses, and how they influenced an important aspect of foreign policy in the case of cybersovereignty. We build on and contribute to Constructivist theories of International Relations that have explored the role of state identity in the making of foreign policy and national interest. In particular, we argue that the history of a state's founding and the struggles around which it was formed can shape definitions of state interest and priorities in the long run – especially when actively kept alive such as through the 'century of humiliation' narrative in China (Wang, 2012).

It is important to recognize that any discussion over the role of sovereignty on the Internet is primarily a matter of degree. At the time of writing, no nation state actually defends the notion of a digital space in the spirit of Barlow's original declaration of independence for cyberspace where nation states play no role at all (Barlow, 1996). Indeed, many countries recognize their own interest in being able to lay claim to sovereignty over certain parts of the Internet, such as the US Cloud Act, which requires that US companies disclose data for investigation, even if stored abroad, by virtue of US sovereign power over corporate entities (Daskal, 2018), or European authorities enforcing content restrictions on Nazi symbolism (Wildman, 2017). Neither actor actually favors removing the role of state sovereignty from cyberspace. However, there is significant variation in the degree of 'stateness' different actors consider legitimate, even if they might all use the 'sovereignty' label to describe their positions (Siebert, 2021), and the type of state intervention that different actors consider legitimate. Thus, a simple binary of states that oppose or support sovereignty risks losing out on the many differences between actors that may all use 'sovereignty' to flag different concerns. For instance, even if experts in German parliament caution against the loss of 'digital sovereignty', (Deutscher Bundestag, 2021) they are unlikely to support the right to extensive government censorship that the Chinese government engages in. Nevertheless, there are important parallels, such as concerns about the security of hardware used in critical infrastructure (Der Spiegel, 2021). Thus, the Chinese position might best be understood as being toward the extreme end of a continuum where states defend degrees of state intervention in cyberspace, combined with a qualitative difference regarding which type of behavior is legitimate. So, what does cybersovereignty mean and where does it fit?

Existing literature usually approaches cybersovereignty as either an agenda or plan for institutional reform in international Internet governance, or as a Chinese attempt at propagating new norms for state behavior in cyberspace.

While the definition of cybersovereignty as an institutional reform agenda is compelling from the perspective of debates over China's identity as a revisionist or status quo power, this conceptual approach can explain very little of either Chinese rhetoric or foreign Internet policymaking. For one thing, cybersovereignty has not been attached to any comprehensive institutional reform, either rhetorically or in policy

practice. There was one failed attempt at giving nation states more power in the realm of Internet governance by empowering the ITU, an organization run by nation states, in 2012 (Inkster, 2016, p. 125). Although this failed vote is commonly cited as evidence of Chinese attempts to overthrow existing governance institutions, there have not been any major reform attempts of existing governance institutions since. Indeed, substantial institutional reform of existing Internet governance institutions is likely neither in China's interest nor realistic. Scholars elsewhere have noted that China has profited substantially from the existing international system (Lindsay, 2015; Weiss and Wallace, 2021) and would risk losing access to these benefits if it tried to overhaul the status quo. For instance, Chinese companies have become quite involved in technical processes such as standard setting, indicating that Chinese actors might be arranging themselves with the status quo (Ding, 2020; Triolo and Allison, 2018). In addition, any comprehensive overhaul would need to overcome substantial institutional inertia (Lindsay, 2015), which makes it practically infeasible.

At the same time, while there is some debate over China's identity as a rising power, the Chinese government lacks a track record of comprehensive attempts or even success at institutional reform in other international institutions, which, like Internet governance, share the characteristics of institutional inertia and benefiting China in their current configuration. There are many areas where the Chinese government has largely adopted a pro-status quo stance in existing institutions (Don Harpaz 2014; Ferdinand & Wang 2013; Scott & Wilkinson 2013), with some reformist behavior where core interests are concerned (Weiss and Wallace, 2021). Thus, while there might be an ideal model of international Internet governance institutions in the minds of Chinese politicians, they have to date neither articulated that agenda nor made any substantive diplomatic moves toward it in the recent past. In addition, any such attempt would likely fail or leave them worse off than the status quo.

In other contexts, cybersovereignty is located in the normative realm and described as a Chinese proposal for a new norm, i.e. a generalized rule for acceptable state behavior (Finnemore and Sikkink, 1998). These analyses tend to be based on a select few key documents and repeated Chinese policy statements that emphasize the importance of respecting state sovereignty in cyberspace. Whether these attempts at

norm entrepreneurship have been successful at establishing any norm that differs from the less intensely pro-sovereignty positions of other states or altered state behavior in any noticeable way is an open question for further research. To date, we are not aware of any research that addresses this question. Instead, even half a decade after the Chinese government began promoting cybersovereignty abroad, scholars are still wrangling over the contents of this norm, which has never been officially defined: While Nigel Inkster has summarized Chinese proposals for international internet governance as meaning that 'the free flow of information should be conditioned by the need to safeguard national sovereignty and security' (Inkster, 2016, p. 125), other scholars have variably interpreted cybersovereignty to mean an agreement to 'abstain from uninvited influence of any kind within any state's information space' (Lindsay, 2015), or as containing three separate norms, i.e. 'national governments enjoy sovereign rights', 'national governments enjoy sovereignty over all non-state actors', and 'sovereign equality of states in Internet governance' (Creemers, 2020, p. 7). While these interpretations share a focus on the role of sovereign governments, they also demonstrate some significant disagreement over the content of the norm – which would make it hard to effectively promote as a generalized rule for state behavior.

It is this confusion and ambiguity that we aim to explain. Building on recent work that emphasizes the primacy of domestic sources for Chinese foreign policy (Weiss and Wallace, 2021), we propose a historical explanation of China's cybersovereignty agenda. We argue that the history of the country, the party and political propaganda within China have shaped the development of cybersovereignty and even the timing of its appearance in important ways.

While our focus is on the specific effects within China, this argument is not exclusive to a single country. Indeed, governments and scholars have worried about the effects of Internet or globalization on state sovereignty for decades (Sassen, 1998) and recent years have seen an increasing number of actors emphasize sovereignty-related concerns in their Internet policy, such as the aforementioned concerns in Europe. However, China was the first and most prominent among these actors to emphasize sovereignty concerns in their diplomatic efforts around Internet policy, and other major international did so earlier or as long and as consistently. We argue that the particular

shape of the Chinese response was strongly informed by domestic factors, especially the existence of compound sovereignties as a discursive political tool. In addition, the salience of sovereignty concerns in Chinese political discourse and history might explain why the Chinese government was the first major international player to center sovereignty in its Internet-related diplomacy. Overall, this makes cybersovereignty in Chinese domestic and foreign policy a good example of how even foreign policy responses ostensibly centered around the same concern (sovereignty) can draw on and be shaped by domestic factors.

The role of history does not preclude sovereignty discourse being mobilized as part of the political agenda of an authoritarian state – just as it was mobilized by anticolonial movements and could justify the establishment of both democratic and autocratic states. It also does not preclude this rhetoric from having normative consequences in the international arena. However, all of these factors are analytically distinct from understanding the historical influences on the initial development of cybersovereignty in China and how it continues a history of many compound sovereignties.

3 Methods

This article adopts a mixed method approach to better understand Chinese conceptions of cybersovereignty and explain how historical experience shaped this aspect of Chinese foreign policy. In the first part, it draws on qualitative analysis of official and elite discourse on cybersovereignty to outline how the concept first developed in domestic Chinese discourse before appearing on the international level. In the second part, it combines these insights with a historical analysis of 'compound sovereignties' in domestic Chinese policy discourse to draw out parallels with the development of 'cybersovereignty'.

Research on the evolution of cybersovereignty in domestic policy elite discourse relied on the qualitative analysis of official government documents by relevant ministries, publications in the *People's Daily* and a selection of academic publications between 2000 and 2017. We choose this timeframe because it represents the birth and heyday of cybersovereignty in Chinese policy discourse: A search in Chinese language academic journals via the academic database CNKI shows that

Table 1 Mentions of 'Cybersovereignty' (2000–19)

Year	*CNKI* (journals)	*People's Daily* (print)
2000	1	0
2001	0	0
2002	0	0
2003	0	0
2004	0	0
2005	0	0
2006	0	0
2007	0	0
2008	1	0
2009	0	0
2010	0	0
2011	5	0
2012	9	2
2013	13	5
2014	33	15
2015	64	14
2016	132	44
2017	144	23
2018	72	15
2019	95	13

2017 represented a peak for cybersovereignty discourse in China, with only about half as many mentions after. Mentions in *People's Daily* already fall off after 2016 (see Table 1). This timeframe has the additional advantage of focusing on the early development of cybersovereignty before and while Lu Wei, the first director of the Cyberspace Administration of China (CAC), reportedly exerted significant influence over Chinese Internet policy both domestically and internationally (Perlez and Mozur, 2016). Since his removal from office in 2016, cybersovereignty has taken a less prominent position in both official and elite discourse. Instead, more recent diplomatic efforts have begun to also emphasize other themes, such as data governance – as evidenced e.g. by the recent 'data security initiative' spearheaded by foreign minister Wang Yi (Webster and Triolo, 2020). Notably, the latter already has

been officially attached to more concrete policy proposals than cybersovereignty ever had and thus might be a much better example of an attempt at Chinese norm entrepreneurship.

One possibility for analyzing Chinese conceptions of cybersovereignty is to focus on official documents that mention the term, extrapolate the government's intentions and future plans from them and link them back to policy implementation (Creemers, 2020). Instead, we follow Allen Carlson's more expansive strategy in his pioneering book on Chinese conceptions of sovereignty: Carlson notably distinguishes between (i) official definitions of sovereignty within China (via official government documents), (ii) discussions about sovereignty among policy elites (e.g. via publications in party publications and Chinese academia), and (iii) their implementation in foreign policy (Carlson, 2005, p. 22).

We believe that this approach is especially appropriate in the case of cybersovereignty for three reasons: First, the conceptual analysis is necessary as a first step in the case of cybersovereignty, which, rather than simply an evolution on conception of state sovereignty, is sometimes billed as a Chinese 'model' for Internet governance worldwide. Any further analysis of this concept based on policy actions or foreign understandings should start with an in-depth analysis of the Chinese understanding of cybersovereignty as a baseline. Secondly, when analyzing actions and beliefs together before having a conceptual baseline to compare them to, there is a risk of conflating the two: China may advocate 'cybersovereignty', but that does not mean that any action the government takes on Internet policy is automatically an outgrowth of its cybersovereignty concept. Prioritizing the concept and its genesis can serve as a useful baseline for assessing which policies can usefully be considered part of the implementation of cybersovereignty, and which more plausibly belong to other realms of foreign policy. Thirdly, we also believe that this focus on Chinese sources is necessary in a first step before any ascriptions from outside of China can be included in the analysis. What actors outside of China think Chinese conceptions of cybersovereignty are is likely mediated by these actors' biases or choices of source material. Hence, any attempt to understand Chinese conceptions of cybersovereignty should first and foremost rely on material from within China.

In addition, this article focuses on the first two of Carlson's categories of sources: official and elite discourse. Much research on cybersovereignty

Table 2 Government sources (2000–17)

Institution	Mentions
CAC	73
MoD	16
MoFA	38
MIIT	8
MPS	5

to date focuses on the first and last category of sources, official definitions and implementation, and the expansion to include domestic elite discourse serves as a useful methodological contribution to the existing literature (Lindsay, 2015; Schia and Gjesvik, 2017; Creemers, 2020). Since official pronouncements on cybersovereignty tend to be extremely vague, buttressing official language with analyses of policy elite discourse can add important analytical depth. As Michael Schoenhals notes, this is a common feature of Chinese political rhetoric: Certain concepts or slogans might propagate before they have taken on a specific meaning, giving room for both policy and conceptual debate and experiments at the lower levels (Schoenhals, 1992). It is this experimentation and debate that this article aims to illuminate.

To analyze official conceptions of cybersovereignty, we scraped the websites of the following institutions for official publications containing the term 'cybersovereignty' (网络主权): the CAC, the Ministry of Foreign Affairs (MoFA), the Ministry of Defense (MoD), the Ministry of Public Security (MPS), and the Ministry of Industry and Information Technology (MIIT). Among these, the CAC emerges as a clear leader in official discourse on cybersovereignty with 73 mentions in CAC documents between October 2014 and November 2016. While the relevant ministries discuss cybersovereignty much less in official publications (see Table 2), representatives do sometimes appear in the party publication *People's Daily* and their statements are considered official when they appear in party media. If this search was repeated today, there would likely be fewer sources since especially some CAC publications seem to have been censored since the original survey in 2017 and through later surveys in 2019 and 2020. We pay particular attention to relevant official policy documents in this corpus, such as

2010 White Paper on the Development of the Internet in China, the 2014 Wuzhen Declaration, and the 2017 International Strategy for Cooperation in Cyberspace.

In order to analyze elite discourse, we focus on two primary sources: *People's Daily* and the academic journal 'China Information Security'. Within *People's Daily*, we survey 133 articles published in the print publication and, in addition, all 199 publications from the 'Cyber Strategy Forum' originally published in China Information Security and republished in *People's Daily* between July 2014 and February 2017. While *People's Daily* articles do not necessarily reflect the official position of the Chinese government, they represent views of policy and propaganda elites close to the government and discussion within the realm of positions acceptable to the government. The Cyberstrategy Forum being republished by *People's Daily* lends it additional legitimacy as a forum for academic and policy professionals discussing matters of cyberpolicy among themselves, but again within a space that is considered acceptable by a publication as close to the government as *People's Daily*. In addition, we also survey all articles in 'China Information Security' discussing cybersovereignty up until 2017 as a window into the wealth of academic debate about the topic (see Table 1 for an overview).

All sources were then analyzed and coded to identify instances where cybersovereignty was either defined or linked to specific policies, and sorted by publication type affiliation of authors (if known). An even more in-depth analysis of this historical evolution with additional data might be desirable in the future. However, the above research design already contributes new insights through the inclusion of elite discourse in addition to official government documents and the combination of these insights with historical analysis.

The following section lays the foundation for this analysis by summarizing the development of cybersovereignty first in Chinese domestic and then foreign policy discourse.

4 Cybersovereignty in Chinese foreign policy

With China's rise in all areas of international politics, other actors have been wary of the possibility that the country might turn out to be a revisionist power, intent on overturning and changing the

international system as it exists today. For most traditional areas of international governance, this debate has largely considered two possible roles that China might take on: revisionist or status quo (Johnston, 2003; Wang and French, 2014). Internet governance has seen a particular permutation of this debate since the rise of the Internet as a factor in international politics has largely coincided with China's political and economic rise. This has given the Chinese government a unique opportunity to contribute to and shape the rules of international Internet governance, instead of having to accept and adapt to an established set of norms. One illustrative example of this was China's accession to the WTO, which took 13 years to negotiate and came with a set of economic reforms demanded by existing members, especially the United States (Pearson, 2001). Internet governance, on the other hand, could theoretically be China's chance to avoid similar humiliations and be a rule maker instead of a rule taker.

While there is no current agreed upon international regime of Internet governance, the relevant literature commonly contrasts state-centric models, as embodied by the International Telecommunications Union (ITU), and multi-stakeholder models, as exemplified by the Internet Corporation for Assigned Names and Numbers (ICANN; Nye, 2014, p. 5). Within this paradigm, China has generally been considered a proponent of the state-centric model and even participated in an attempt at giving the ITU a greater role in Internet governance in 2012 (Nye, 2014, p. 7). It is important to note that institutions such as ICANN and the ITU commonly discussed in relation to international Internet governance have exclusively technical mandates and that international Internet governance, at least in any form that exists at the time of writing, does not have mandate or authority related to the regulation of data flows, such as content control or data protection, which remains firmly in the hands of national governments.

Cybersovereignty has come to be considered the core feature of China's policy on international Internet governance since its first prominent appearance in a 2010 white paper on the state of the Chinese Internet (Information Office of the State Council of the People's Republic of China, 2010). Chinese government representatives have since then repeatedly attempted to promote the concept in a variety of international contexts, from the 2014 ICANN meeting in London (ICANN, 2014; Lu, 2014) to China's own World Internet Conference

in Wuzhen later the same year (Gady, 2014). The following section will first explore the broad outlines of the evolution of cybersovereignty in domestic political discourse and then describe how it suddenly turned from a domestic talking point into a mainstay of Chinese foreign policy discourse in 2014. Lastly, it will outline why cybersovereignty as a concept remains elusive and by and large does not actually contain clear prescriptions for appropriate state behavior, as we would expect from an international norm.

4.1 The evolution of cybersovereignty in Chinese discourse

The term cybersovereignty (网络主权) has been sporadically appearing in Chinese media and academic publications since the early 2000s. In one of the first mentions in a 2006 article in *International Financial News* (国际金融报), which was republished by *People's Daily*, the author explains how the Internet's Domain Name System (DNS) works and expounds on the danger of China being cut off from the rest of the world via manipulation of this very system (Xu, 2006). According to the author, this danger existed because the organization governing the DNS had been founded in the United States and, albeit a private entity, was still dominated by US interests and, according to the author, under US control. While cybersovereignty was a few years away from becoming a mainstay in Chinese official statements, the article already raised several themes that would be associated with cybersovereignty in domestic policy discourse several years later: The fear of the US' institutional dominance in international Internet governance and a deep-seated concern about growing dependence on the goodwill of foreign actors, paired with the insight that while this dependence might be increasing the country's vulnerability, being cut off from the network that connected China to the rest of the world might pose an even bigger danger. All of this was packaged in familiar Chinese foreign policy rhetoric about the need to give developing countries a louder voice in institutions of global governance.

This mix of a desire to be connected to the rest of the world, while simultaneously protecting Chinese independence and national security, maintaining as much control as possible and helping China grow into a true Great Power on the international stage, has continued to be

emblematic of cybersovereignty in its various iterations, which never really settled on a fixed meaning.

There were a few sporadic mentions in the 2000s in both academia and media, but the concept first garnered international attention when a 2010 white paper on the state of 'The Internet in China' mentioned the term in an official government document (Information Office of the State Council of the People's Republic of China, 2010). Beyond the fact that it was something China presumably wanted to protect, and other states ought to respect, the concept remained vague and largely undefined. This allowed different parts of the government to define the term in ways that reflected their policy concerns: For the next few years, scholars and commentators affiliated with the People's Liberation Army (PLA) would bring up the term repeatedly in contexts where they equated maintaining cybersovereignty with the defense against an ever-increasing number of evolving online threats (Hao, 2011; Liu, 2011). A less prominent point of view in this time period came out of the less prolific Ministry of Foreign Affairs (MoFA) and had a much stronger focus on institutional reform instead of military power: Commentators in this vein emphasized cybersovereignty as being associated with equality in the institutions of international Internet governance, linking the term to a vague agenda of institutional reform (Yang, 2012). There was no clear institutional reform agenda associated with cybersovereignty associated in any of these statements.

Between 2010 and 2014, cybersovereignty was thus mobilized in different ways by separate parts of China's sprawling bureaucracy and governance apparatus: once as a synonym for national defense in cyberspace, once as a reform agenda for international Internet governance institutions. It is notable that none of these policy goals required a linkage to sovereignty – both national security and an agenda to make existing institutions of global governance more equitable have been policy goals in their own right since the founding of the People's Republic of China. Nevertheless, cybersovereignty, which had been endorsed in the 2010 white paper, became a focal point for Internet-related policy concerns in different parts of the government.

The major push to make cybersovereignty the centerpiece of the Chinese cyberpolicy agenda and onto the international stage came in mid-2014, a few months after the founding of the CAC (Alsabah, 2016), which was supposed to address and coordinate policymaking on

an overlapping set of internet policy issues that had previously been handled in various parts of China's fractured bureaucracy. The summer saw a discussion about cybersovereignty, involving several scholars, published in *People's Daily* (Wang, 2014), newly appointed CAC director Lu Wei laid out an internationally palatable approach to Internet governance at the 50th ICANN meeting in London (Lu, 2014), and the CAC held its inaugural World Internet Conference in Wuzhen in December, where the concept of cybersovereignty took center stage (Gady, 2014). The founding of the CAC thus coincided with a more high-profile approach to international Internet governance and a starting point for the international promotion of a Chinese vision of Internet governance. It seems that Lu in particular was a driving force behind the concept, which might also explain the complete lack of mention of cybersovereignty in *People's Daily* for 15 months after he left the CAC to be investigated for corruption.[1]

However, the concept of cybersovereignty has not gained much in specificity since 2010. Instead, even as President Xi Jinping himself extolled it in his speech at the second World Internet Conference in Wuzhen in 2015 (BBC, 2015), it remained a floating concept in domestic discourse that could be attached to completely different agendas. In official CAC publications and the Cyberstrategy Forum, published in the journal *China Information Security* and *People's Daily*, cybersovereignty was at different times used to connote the government maintaining its position as the highest law-making authority within its borders, protection of Chinese cyberterritory (with varying definitions; Lu, 2014), equality of states in international Internet governance (平等权; Wang, 2014), a strengthened China that had caught up with the United States and turned into a Great Power in its own right (Lu, 2016), Chinese independence from foreign technology, national security especially via the protection of key information infrastructure (Yin et al., 2015) and preventing the spread of harmful information, maintaining Chinese connectivity with the rest of the world, protecting Chinese data from unauthorized access (Wu, 2016) and ensuring the free flow of data necessary for the economy's growing technology sector (Shen, 2014).

1 This gap in the archives might also be due to retrospective censorship. Either way, the timing indicates that Lu Wei had become closely associated with cybersovereignty.

If cybersovereignty had, at this point, been established as an important policy goal in and of itself, one might expect government institutions such as the CAC or Party publications such as the *People's Daily* to push a more unified agenda. However, the variability of cybersovereignty even in official and semi-official writing is evidence of the flexibility of cybersovereignty even as it grew more prominent: Due to the lack of definition of concrete policy goals, it could be taken to refer to almost any policy goal that was related to the Internet and might be considered advantageous to Chinese interests.

The continued elusiveness of cybersovereignty.

This seeming lack of coherence is striking for a concept that many observers have considered central to a Chinese push as a norm entrepreneur. It also confirms and strengthens the impression that emerges from the literature review above: Even if Beijing propagates cybersovereignty as if it was a norm, the concept is so variable that would be a poor option for a generalized rule for state behavior. Although sovereignty is a notion that is notoriously subject to contestation, proposing 'cybersovereignty' as a norm in the traditional sense would at least require some coherence in the Chinese position, which would (and is) being contested by other states. However, the view to domestic policy discourse above illuminates that this internal flexibility of cybersovereignty has been there since the very beginning. There are three further aspects that hint at cybersovereignty being different from, or more than, an international norm China is trying to promote and that point to how it has been shaped by domestic factors and politics.

First, the campaign in favor of cybersovereignty as an international norm has been remarkably unsuccessful and, in some areas, downright counterproductive. The Chinese government has struggled with expanding its soft power (and not for a lack of trying) for years and promotions of cybersovereignty were accompanied by moves that implied that the actors promoting it might not quite understand the international audience they were allegedly addressing. One prime example of this was the memorandum organizers slipped under the doors of participants of the first World Internet Conference in 2014 in the middle of the night before the closing ceremony. Among other things, the declaration affirmed the need to 'respect Internet sovereignty of all countries'

(Shu, 2014). Ineffectiveness does not negate the intent to promote an international norm, but it certainly indicates that there was no well-planned international campaign behind the promotion of cybersovereignty. Instead, its appearances mirror patterns from domestic propaganda, such as the announcement of a prominent new slogan that appears on posters across the country, without an official definition of what the slogan means yet (Schoenhals, 1992).

Secondly, cybersovereignty continues to be largely devoid of concrete policy proposals, which undermines its supposed role as a Chinese proposal for international Internet governance structures. Given its first mentions in the 2000s, discussions in academic circles between 2008 and 2010, percolation through different government institutions between 2010 and 2014 and finally its push onto the international stage via the CAC in 2014, relevant actors had sufficient time to develop a more concrete policy agenda that Beijing could implement on the domestic and international level. In addition, the few aspects of cybersovereignty that lend themselves to concrete policy proposals, such as institutional reform in ICANN and other Internet governance institutions, have been marked by an absence of Chinese initiative toward actual institutional reform. For instance, despite increasing participation by private Chinese entities at ICANN meetings, the organization's structure remains the same. Cybersovereignty, the alleged core feature of Chinese policy on international Internet governance, primarily consists of a bundle of sticks that do not lend themselves to concrete steps or demands.

Thirdly, cybersovereignty is not an exclusive concept. Similar to the goals of national security and institutional reform in global governance mentioned above, issues associated with cybersovereignty at various points overlap with or have simply moved into other policy areas. For example, the issue of domestic innovation and independence from foreign technologies has come to be embodied in Made in China 2025 (Laskai, 2018) and the protection of critical infrastructure has largely been subsumed in discussions about national security independent of sovereignty (Creemers, Triolo, and Webster, 2017). Other issues, such as national security, would have been considered core interests regardless of who was governing China. Others have at least been rhetorical parts of the Chinese policy agendas since long before the emergence of the Internet – most notably the call for equality in international

governance institutions (Wang and French, 2014, p. 255ff) and the emphasis on independence from foreign technologies, which has been central to industrial policy for decades (Pearson, 2014). At least domestically, cybersovereignty can refer to all of these goals and concerns – and for over 10 years, there has been little attempt to change this, which indicates that this flexibility is by design rather than simply regular political contestation. The question remains which of these aspects are actually unique to cybersovereignty and whether the concept has any hard core beyond the most basic meaning of sovereignty: the right to be left alone (see e.g. discussion in Slaughter, 2004).

In light of these contradictions arising from the development of cybersovereignty in domestic Chinese policy discourse, it might be worth considering an alternative explanation to cybersovereignty as a consolidated, well-formed piece of Chinese foreign policy. Looking back to history for an explanation, sovereignty and especially the lack thereof have been central to China's experience in engaging the rest of the world and take an accordingly prominent position in Chinese policy discourses covering a variety of areas. These usages follow certain rules, but those may only apply domestically. Attempting to seize the opportunity of the lack of governance structures in international Internet governance, China may have wanted to make use of its role as a rising power and offer up a vision for international Internet governance that could be contrasted to US attempts at promoting Internet freedom. In order to do so, Chinese bureaucrats and scholars fell back on a rhetorical and policy vehicle that had served governments for more than a hundred years in emphasizing its main concerns in other policy areas: sovereignty.

5 Sovereignty, Chinese history, and speech acts

Traditionally, the literature on sovereignty tended to fall into what has been described as the 'descriptive fallacy'. The fallacy consists of assuming that sovereignty reflects a certain empirical reality, whose exact contents can be then determined with a degree of exactitude. However, constructivist literature has criticized the contention that sovereignty is merely reflective of reality, as opposing to constituting it. According to this literature, sovereignty is best understood as a claim to authority or to an ordering power (Walker, 2003; Bartelson, 2006). Because of its

superordinate status within the international system, a claim to sovereignty has the effect of legitimizing that particular exercise of power. Neil Walker introduced the idea of sovereignty as a speech act, an insight subsequently built upon by Gammeltoft-Hansen and Adler-Nissen, who have conceptualized the speech act of sovereignty as a 'sovereignty game' (Adler-Nissen and Gammeltoft-Hansen, 2008). In their paradigm, sovereignty is best understood as a language game, with the ultimate purpose of expanding players' authority in a certain sphere. Like all games, this game involves rules, players, and moves. Sovereignty games, according to Gammeltoft-Hansen and Adler-Nissen, can be defined as 'claims to authority and the social practices that surround them' (Adler-Nissen and Gammeltoft-Hansen, 2008, p. 8). Such games involve the instrumentalization of sovereignty for various ends, typically such as the enlargement of a player's autonomy in the international arena.

China lends itself particularly well to a speech act-based analysis of sovereignty since a striking feature of Chinese discourse surrounding sovereignty is its widespread discursive use, often in contexts where sovereignty's relevance is not immediately obvious. In particular, there is within China's sovereignty discourse a proliferation of what might be described as 'compound sovereignty', whereby a qualifier is added to 'sovereignty' in order to tie it to a particular subject to emphasize its importance. Examples abound, but in recent years, in addition to cyber sovereignty, there have been education sovereignty (*jiaoyu zhuquan*), cultural sovereignty (*wenhua zhuquuan*), currency sovereignty (*huobi zhuquan*), judicial sovereignty (*sifa zhuquan*), and communications sovereignty (*chuanbo zhuquan*), to name a few (Tok, 2013). Insofar as these all involve subjects that are ordinarily amenable to the regulation of sovereign states, there is little conceptually new in each of these ideas. However, the interest lies in the linkage between relatively narrow subject areas, on the one hand, and the overarching claim to authority in the form of sovereignty on the other, which is seldom seen in Western discourse on sovereignty.

In attempting to explain the incidence of sovereignty compounds, it must be remembered that sovereignty is an unusually potent notion within Chinese political discourse. The roots of this potency are essentially historically contingent, the result of the peculiar history of the notion of sovereignty in China. Before the mid-nineteenth century, the idea of sovereignty was not a part of Chinese political thought. Instead,

it operated under the premises of *tianxia* (all under Heaven), a political-cum-religious notion whereby the world was ordered around China and its emperor, the latter claiming universal jurisdiction over the rest of the world. However, the introduction of sovereignty into the Chinese discourse in the mid-nineteenth century coincided with the beginning of the so-called Century of Humiliation, during which China concluded a number of 'Unequal' treaties, on unfavorable terms, with various Western powers and, later on, Japan (Svarverud, 2007; Kawashima, 2012). Both the republican and the Communist Chinese governments saw it as their mission to recover the lost sovereignty, whether it was in the form of ceded territory or limits placed on the exercise of domestic sovereignty, such as extraterritoriality and loss of tariff autonomy; even seemingly random subjects such as the introduction of Western-style medicine were justified as part of the sovereignty recovery project (Andrews, 2014). Thus, as Maria Adele Carrai puts, 'Chinese modern history seems to coincide with its quest for sovereignty' (Carrai, 2019, p. 220).

If anything, the importance of being seen as defending Chinese sovereignty intensified since the 1990s, as the current Chinese regime, shorn of its previous source of legitimacy based on class struggle, has sought alternative sources of legitimacy. In order to do so, it has aggressively promoted, just like its republican predecessor, the importance of recovering and of protecting Chinese state sovereignty, which in turn has created heightened expectations among the Chinese public for the Chinese government in relation to sovereignty (Wang, 2012). Hence, sovereignty in China has an emotional resonance otherwise lacking (or existing only to a reduced degree) in most Western societies, and its invocation is perceived as having greater potency than might be the case in a Western country. Its instrumentalization and invocation, in other words, are far more likely to be successful in China than elsewhere, at least in a domestic context.

The various forms of 'compound sovereignty' drop in and out of official Chinese discourse with regularity, and this appears to a great extent to be a function of the issue's salience in China at the time. For instance, the concept of educational sovereignty has existed in Chinese literature since at least the 1990s, but until recent years its only presence was in academic discourse, outside of which it had little recognition. However, soon after Xi Jinping's accession to the Chinese

presidency in 2012, he launched a campaign against 'Western values', after which the incidence of education sovereignty in official and quasi-official Chinese discourse rose sharply. Finally, in 2016, educational sovereignty was given official imprimatur as part of a crackdown on the use of foreign curricula and international schools, whose increasing popularity was viewed as being threatening by the government (Kan, 2016). The underlying content of education sovereignty appears simply to be a claim that China has the right to regulate what is being taught in its schools, an uncontroversial position; but it is safe to suggest that sovereignty in the context of education is not necessarily an obvious framing to Western eyes. Similarly, references to currency sovereignty can be found in academic works from the 1990s, but it was only singled out and given prominence as part of official Chinese discourse when China's monetary policies came under external criticism (Reuters, 2019). Chinese textbooks generally ascribe a number of powers, such as the ability to issue currency, to the broad umbrella of monetary sovereignty; again, there is little inherently new in the concept, apart from the framing of a relatively uncontroversial number of state prerogatives in terms of sovereignty (e.g. Liu and Deng, 2003, p. 35). The emergence of cybersovereignty as a term in China in the early 2000s, followed by its relative lack of prominence until the 2010 White Paper, is thus far from unique in recent Chinese history.

5.1 Cybersovereignty as sovereignty game

With this background in mind, it becomes possible to break down the use of compound sovereignties in the Chinese context into at least three distinct stages, all of which can be seen in relation to cybersovereignty. First, new compound sovereignties arise (or gain in prominence) when the state perceives its authority over a certain subject-matter to be under threat, often as the result of increasing foreign influence in the area (Carrai, 2019, p. 220). Secondly, by associating a concept with the idea of sovereignty, the state reasserts its authority over that area—the main feature of the sovereignty game. Finally, having associated the issue at hand with sovereignty and reasserted its authority in the area, the state reaps benefits in the form of the legitimacy generated as a result of its perceived defense of the nation's sovereignty. Although none of the three stages is unique to China, the third and final one—the

generation of legitimacy through the assertion of sovereignty—is especially prominent in the Chinese context due to the historical background described in the previous section.

In the case of cybersovereignty, although the concept—and precursors such as telecommunications sovereignty—have existed in Chinese discourse for some time, it was not until the release of the June 2010 Chinese Internet White Paper that it received official endorsement and widespread dissemination (Zeng et al., 2017). Not coincidentally, this was in the direct aftermath of a high-profile foreign challenge to the idea of state authority in the cyberspace. In January 2010, American Secretary of State Hillary Clinton had announced that the United States was elevating the concept of 'Internet freedom' as a key US foreign policy priority, and specifically singled out China's censorship of the Internet for criticism. Although the White Paper did not specifically mention Clinton's Internet freedom agenda, it is hard not to read it as a rebuttal to the agenda laid out by Clinton, as it contained a number of specific defenses of practices specifically attacked by Secretary Clinton, most notably its extensive practice of Internet censorship.

It is important to note that the use of sovereignty as a framing for its pushback was not in fact the Chinese government's initial response; instead, it first critiqued Clinton's speech by emphasizing the hegemonic dimensions of her proposals (Shen, 2010).[2] However, by the time of the release of the White Paper, that angle had been abandoned in favor of the cybersovereignty framing. From the Chinese point of view, this represented something of an escalation, given the importance accorded to sovereignty by the Chinese state.

But the transposition of a traditionally domestic-bound conception of sovereignty to the international sphere carries obvious conceptual challenges. To borrow from the sovereignty game terminology, whereas the players (broadly speaking America and China) and the moves (e.g. the Chinese White Paper) of the cyber sovereignty game are relatively straightforward to identify, when it comes to the rules of the game there has been significant divergence. China, the 'last bastion of Westphalia[n sovereignty]' and the 'vicar of the high church of Westphalia', maintains a resolutely traditional approach to sovereignty (Zhang, 2008, p. 161).

2 Zhong Shen is the pseudonym the *People's Daily* employs for its authoritative foreign policy editorials.

By contrast, although still acknowledged as a *grundnorm* of international society, recent Western discourse on sovereignty has been decidedly more critical. In particular, there is a growing discourse for the subordination of state sovereignty to other higher-order norms, for instance, in the realm of human rights.[3] In other words, an invocation of sovereignty in the West lacks either the rhetoric or the normative force that it has for a Chinese audience. Even the Trump administration, whose rhetoric has relied heavily on sovereignty, continued to promote Internet freedom as one of its official objectives, whilst attacking China for 'hid[ing] behind notions of sovereignty' in the cyberspace (United States, 2018).

Nevertheless, although sovereignty-based compounds appear often in Chinese state media and official documents, cybersovereignty appears to be the first of these terms to receive a wide circulation internationally. This may be due to the transnational nature of the cyberspace, and the physical presence of its core infrastructure outside of China's territorial jurisdiction, which means that cybersovereignty lends itself more naturally to internationalization than the other sovereign-based concepts in the same category.

This cleavage on the importance of sovereignty to the debate surrounding the Internet is readily apparent from Clinton's remarks on the subject and the ensuing Chinese reactions. In none of her speeches, both before and after the launch of the Chinese White Paper, did she make any reference to the issue of state sovereignty. The same is true for much of the Western literature on the subject, which tends to approach cybersovereignty from the normative perspective of its use by authoritarian regimes such as China. By contrast, Chinese discussions of the Internet freedom agenda speak of little else, going so far as to frame Clinton's remarks as an explicit attack on state sovereignty when Clinton's pronouncements on Internet freedom did not mention sovereignty at all. Indeed, Chinese framings of the Internet freedom speech tend to exaggerate its radicalness (Keating, 2010).

For instance, Chinese sources reported in 2010 that Clinton said she supported the 'open form and free flow of information free from state sovereignty (公开的形式与不受国家主权约束的信息自由流动), which

3 The trend has been the most prominent in the debate surrounding Responsibility to Protect (R2P), to which China is generally opposed on, unsurprisingly, sovereignty grounds.

would have set Internet freedom explicitly in opposition with state sovereignty (Cai, 2011; Fang, 2018, p. 413).[4] In fact, Clinton said nothing of the sort. But this purported remark was quoted extensively in Chinese literature to demonstrate that Internet freedom was about undermining national sovereignty. And whereas Clinton's speech emphasized the human rights dimensions of Internet freedom, most notably freedom of speech and information freedom, in Chinese discourse human rights are widely assumed to be subordinate to state sovereignty. (Indeed, the words for right and power, as are the words for human rights and sovereignty, are all compounds of *quan* (权), blurring these concepts' distinctiveness) (Chiu, 1968; Cao, 2004).

Cybersovereignty's rise to prominence is thus the result of a reactive process induced by external actors. Thus, it is unsurprising that its early years should have been accompanied by the conceptual and bureaucratic confusion described earlier, as various parts of the Chinese state, from the military to the foreign ministry, each attempted to fill the empty vessel of cybersovereignty with their own distinctive policy priorities. This is not in and of itself surprising. As Michael Schoenhals notes, this is a common feature of Chinese political rhetoric, where certain concepts or slogans might propagate before they have taken on a specific meaning, giving room for both policy and conceptual debate and experiments at the lower levels (Schoenhals, 1992). But this inevitably exacerbated the difficulties China encountered in achieving conceptual coherence around cybersovereignty, especially as it tried to promote the concept abroad at the same time.

Finally, having sovereigntized cyberspace, the Chinese state is able to not only legitimize its cyber policies through the assertion of sovereignty, but also generate additional legitimacy for itself through the implementation and execution of these policies. This is because, having framed its exercise of control over the cyberspace, something often unpopular with domestic Chinese audiences (Han, 2018; Lei, 2018) in sovereignty terms, it is then able to use these controls as proof that it is upholding Chinese sovereignty against foreign encroachment, which helps to fulfill the Chinese public's heightened demand for the state to defend national sovereignty.

4 Fang is known as the 'Father of China's Great Fire Wall'.

In summary, cybersovereignty can be understood as the latest iteration of a discursive strategy frequently deployed by the Chinese government domestically, but one which has not hitherto featured prominently in China's international discourse. The particular nature of cyberspace, as well as the reactive nature of China's invocation of the concept, have given it a much broader international prominence than would otherwise have been the case. Cybersovereignty, at least initially, remained internally incoherent, because of its origins as a rhetorical device as opposed to a coherent overall vision. And because sovereignty's rhetorical force is at best uneven internationally, cybersovereignty did not prove to be as effective as might have been the case in a domestic context, although unsurprisingly the countries which hold traditional, absolute conceptions of sovereignty tended to be more receptive than those where sovereignty is merely one superordinate principle among many.

6 Conclusion

The continued elusiveness of cybersovereignty has presented something of a puzzle to International Relations scholars. It has been interpreted as a sign of Chinese norm entrepreneurship, yet the exact policy positions associated with it have remained unclear over more than a decade. In addition to its lack of specificity, we have shown that cybersovereignty was initially a concept used on the domestic level, where it was associated with a wide range of policy goals, before beginning to appear in Chinese international statements. However, in its international rollout, its unspecific contents, and its overlap with Chinese policy goals from other areas, cybersovereignty has not yet taken the form of a potential generalized rule of behavior for the international community, which we might expect of a norm entrepreneur. Indeed, Chinese diplomatic efforts have recently pivoted to focus more on data governance, an area where the government has been making significant advances in expanding a specific domestic regulatory regime. We have shown that cybersovereignty is likely the continuation of a longstanding tradition of compound sovereignty in China, which has been used as a legitimation device by the Chinese leadership. This discursive flexibility of the concept of cybersovereignty in Chinese political discourse explains why established definitions of sovereignty in political science may not be sufficient to capture it. Instead, it may be better

understood as a domestic discursive strategy, used by the Chinese government for legitimation and to assert state authority, and grounded in the centrality of sovereignty to the founding of the Chinese state.

ACKNOWLEDGEMENTS

The authors would like to thank Jon Lindsay and Deborah W. Larson, the anonymous reviewers, and the participants of our panel at ISA 2019 in Toronto for their feedback and questions, which improved the paper.

Funding

Katharin Tai thanks the International Studies Association for a travel grant supporting her travel to ISA Annual Convention 2019 in Toronto, where this paper was presented.

Yuan Yi Zhu thanks Nuffield College, Oxford and Stanford University for travel grants supporting his travel to ISA 2019 Convention in Toronto, where this paper was presented.

References

Adler-Nissen, R. and Gammeltoft-Hansen, T. (eds.) (2008) *Sovereignty Games: Instrumentalizing State Sovereignty in Europe and Beyond*. Basingstoke: Palgrave Macmillan.

Alsabah, N. (2016) *Information Control 2.0: The Cyberspace Administration of China Tames the Internet*, Merics. https://merics.org/sites/default/files/2020-05/MERICS_China_Monitor_32_Eng.pdf, accessed March 22, 2021.

Andrews, B. (2014) *The Making of Modern Chinese Medicine, 1850-1960*. Vancouver: UBC Press.

Bartelson, J. (2006) The concept of sovereignty revisited, *European Journal of International Law*, 17, 463474.

Barlow, J.P. (1996). *A Declaration of the Independence of Cyberspace*. Davos: Electronic Frontier Foundation. Retrieved January 26, 2012 from https://projects.eff.org/~barlow/Declaration-Final.html

BBC (2015) Xi calls for Cyber Sovereignty, *BBC News*. http://www.bbc.com/news/world-asia-china-35109453.

Cai, W. (2011) 从技术控制到政治塑造——美国互联网自由战略的解读与批判 [*From Technical Control to Political Modeling: Interpretation and Criticism of American Internet Freedom Strategy*], Guancha. https://www.guancha.cn/indexnews/2011_03_29_55576.shtml, accessed March 22, 2021.

Carlson, A. (2005) *Unifying China, Integrating with the World: Securing Chinese Sovereignty in the Reform Era*. Stanford: Stanford University Press.

Cao, D. (2004) *Chinese Law: A Language Perspective*. London: Routledge.

Carrai, M. A. (2019) *Sovereignty in China: A Genealogy of a Concept Since 1840*. Cambridge: Cambridge University Press.

Chiu, H. (1968) The development of Chinese international law terms and the problem of their translation into English, *The Journal of Asian Studies*, 27 (3), 485501. https://doi.org/10.2307/2051152.

Creemers, R., Triolo, P. and Webster, G. (2017) *China's Ambitious Rules to Secure Critical Information Infrastructure*. New America. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/, accessed March 22, 2021.

Creemers, R. (2020) China's conception of cyber sovereignty: rhetoric and realization. https://doi.org/10.2139/ssrn.3532421.

Daskal, J. (2018) Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *Stanford Law Review Online*. 2018. 71. 9. https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/, accessed November 24, 2021.

Der Spiegel (2021): Bundestag beschließt Hürden-für-Huawei-Gesetz (Parliament passes obstacles-for-Huawei law), Hamburg: Der Spiegel, https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-2-0-bundestag-beschliesst-huerden-fuer-huawei-gesetz-a-2f50a7dc-e5f5-4b35-ba30-1ecbf1db4eed, last accessed December 3, 2021

Deutscher Bundestag (2021): Experten warnen vor Verlust an digitaler Souveränität (Experts warn of loss of digital sovereignty), Berlin: Deutscher Bundestag, https://www.bundestag.de/dokumente/textarchiv/2021/kw23-pa-auswaertiges-844396, *last accessed* December 2, 2021

Ding, J. (2020): Balancing Standards: U.S. and Chinese Strategies for Developing Technical Standards in AI, NBR, https://www.nbr.org/publication/balancing-standards-u-s-and-chinese-strategies-for-developing-technical-standards-in-ai/, last accessed December 2, 2021

Don Harpaz, M. (2014) "China's WTO Compliance-Plus Anti-dumping Policy," *Journal of World Trade* Vol. 45, No. 4 (2014), pp. 727–766

Fang, B. (2018) *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Singapore: Springer Nature Singapore.

Ferdinand, P. & Wang, J. (2013) "China and the IMF: From Mimicry Towards Pragmatic International Institutional Pluralism," *International Affairs Vo*. 89, No. 4

Finnemore, M. and Sikkink, K. (1998) International norm dynamics and political change, *International Organization*, 52, 887917.

Gady, F.-S. (2014) *The Wuzhen Summit and Chinese Internet Sovereignty*, Huffington Post, https://www.huffingtonpost.com/franzstefan-gady/the-wuzhen-summit-and-chi_b_6287040.html.

Glaser, B.S. and Medeiros, E.S. (2007) The Changing Ecology of Foreign Policy-Making in China: The Ascension and Demise of the Theory of Peaceful Rise. *The China Quarterly*. 2007. 190. 291310. https://doi.org/10.1017/S0305741007001208.

Han, R. (2018) *Contesting Cyberspace in China: Online Expression and Authoritarian Resilience*. New York: Columbia University Press.

Hao, Y. (2011) 赛博空间：狼烟四起的新战场关注网络电磁空间日趋炽烈的战略博弈 [*Cyberspace: A New Battlefield with Fire Beacons on All SidesFocus on the Increasingly Fierce Strategic Competition in the Cyber-Electromagnetic Space*], Workercn.cn. http://theory.workercn.cn/c/2011/04/15/110415111757964608827.html, accessed March 22, 2021.

ICANN (2014) *Largest Ever ICANN Meeting Convenes in London | Affirmation of Multistakeholder Model for Internet Governance by World Leaders*. https://www.icann.org/news/announcement-2014-06-23-en, accessed March 22, 2021.

Information Office of the State Council of the People's Republic of China (2010) Full text: white paper on the Internet in China, *China Daily*. https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm, accessed March 22, 2021.

Inkster, N. (2016) *China's Cyber Power*. Abingdon: Routledge.

Johnston, A. I. (2003) Is China a status quo power?, *International Security*, 27, 556. https://doi.org/10.1162/016228803321951081.

Kan, K. (2016) Shanghais move to curb international programs in schools worries parents, *The New York Times*. https://www.nytimes.com/2016/12/29/world/asia/shanghai-schools-international-curriculum.html, accessed March 22, 2021.

Kawashima, S. (2012) China, in B. Fassbender and A. Peters (eds.), *The Oxford Handbook of the History of International Law*, pp. 451474. Oxford: Oxford University Press.

Keating, J. (2010) China makes Clinton's speech look tougher than it was, *Foreign Policy*. https://foreignpolicy.com/2010/01/22/china-makes-clintons-speech-look-tougher-than-it-was/, accessed March 22, 2021.

Laskai, L. (2018) *Why Does Everyone Hate Made in China 2025?* Council on Foreign Relations. https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025, accessed March 22, 2021.

Lei, Y.W. (2018) *Law, Media, and Authoritarian Rule in China*. Princeton, NJ: Princeton University Press.

Lindsay, J. R. (2015) The impact of China on cybersecurity: fiction and friction, *International Security*, 39, 747.

Liu, Y. and Deng, R. (2003) 国际经济法 *[International Economic Law]*. Beijing: CITIC Publishing House.

Liu, Z. (2011) 怎样构建中国网络边防 [How to build China's cyber border defense], *People's Daily*Online. http://theory.people.com.cn/GB/82288/112848/112851/15478463.html, accessed March 22, 2021.

Lu, W. (2014) 鲁炜在ICANN高级别政府会议上的发言 全文 [Lu Wei's speech at the ICANN high-level government meeting full text], *GCTV*. http://www.greenchina.tv/news-9569.xhtml, accessed March 22, 2021.

Lu, W (2016) 鲁炜：担当大国责任 共建网络空间命运共同体 [*Lu Wei: Assume the Responsibility of a Great Country and Build a Community with a Shared Future in Cyberspace*], Shanghai Internet Illegal and Bad Information Reporting Center. http://www.shjbzx.cn/jbpt/n57/n63/u1ai1394.html, accessed March 22, 2021.

Margolin, J. (2016) *Russia, China, and the Push for Digital Sovereignty*, IPI Global Observatory. https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization, accessed March 22, 2021.

Nye, J. S. (2014) *The Regime Complex for Managing Global Cyber Activities*, Centre for International Governance Innovation. https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities, accessed March 22, 2021.

Pearson, M. (2001) The Case of China's Accession to GATT/WTO, in D.M. Lampton (ed.), *The Making of Chinese Foreign and Security Policy in the Era of Reform*, pp. 337370. Stanford: Stanford University Press.

Pearson, M. (2014) China's Foreign Economic Relations and Policies, in S. Pekkanen, J. Ravenhill and R. Foot (eds.), *The Oxford Handbook of the International Relations of Asia*, pp. 160178. Oxford: Oxford University Press.

Perlez, J. & Mozur, P. (2016): Lu Wei, China's Internet Czar, Will Step Down From Post, New York: New York Times. https://www.nytimes.com/2016/06/30/business/international/china-internet-lu-wei.html, last accessed December 2, 2021

Reuters (2019) 中国央行：基础货币发行方式服务国家整体利益，不存在货币主权旁落问题 [Central Bank of China: The basic currency issuance method serves the overall interests of the country, do not pose problems for currency sovereignty]. https://www.reuters.com/article/中国央行：基础货币发行方式服务国家整体利益，不存在货币主权旁落问题-idCNL3S20P01Q, accessed March 22, 2021.

Sassen, S. (1998) On the Internet and sovereignty, *Indiana Journal of Global Legal Studies*, 5(2), 545559.

Schia, N. N. and Gjesvik, L. (2017) *China's Cyber Sovereignty*. Oslo: Norwegian Institute of International Affairs.

Schoenhals, M. (1992) *Doing Things with Words in Chinese Politics: Five Studies*. Berkeley: Center for Chinese Studies, University of California, Berkeley Center for Chinese Studies.

Scott, J. & Wilkinson, R. (2013) 'China Threat? Evidence from the WTO'. *Journal of World Trade* 47, no. 4 (2013): 761–782

Shen, Y. (2014) 后斯诺登时代的全球网络空间治理 [Global cyberspace governance in the post-Snowden era], *World Economics and Politics* 5, 144155. https://sirpa.fudan.edu.cn/__local/6/6A/5C/00589F2F3BB340CAB197EFDD16C_7712150F_8AB401.pdf?e=.pdf, accessed March 22, 2021.

Shen, Z. (2010) To defend "freedom", or to defend "hegemony"?, *People's Daily Online*. http://en.people.cn/90001/90780/91343/6879251.html, accessed March 22, 2021.

Shu, C. (2014) China tried to get world internet conference attendees to ratify this ridiculous draft declaration, *TechCrunch*. http://social.techcrunch.com/2014/11/20/worldinternetconference-declaration/, accessed March 22, 2021.

Siebert, Z. (2021) Digital Sovereignty - The EU in a Contest for Influence and Leadership. Berlin: Heinrich B-ll Stiftung.

Slaughter, A.-M. (2004) Sovereignty and Power in a Networked World Order, Stanford Journal of International Law, 40, 283328.

Svarverud, R. (2007) *International Law as a World Order in Late Imperial China: Translation, Reception and Discourse, 1847-1911*. Leiden and Boston, MA: Brill.

Triolo, P. & Allison, K. (2018), "The Geopolitics of 5G," Eurasia Group, https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g, last accessed December 2, 2021

Tok, S. K. (2013) *Managing China's Sovereignty in Hong Kong and Taiwan*. New York: Palgrave Macmillan.

United States (2018) *National Cyber Strategy of the United States of America*. The White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accessed March 22, 2021.

Walker, N. (2003) *Sovereignty in Transition*. Oxford: Hart.

Wang, H. and French, E. (2014) China in global economic governance, *Asian Economic Policy Review*, 9, 254271. https://doi.org/10.1111/aepr.12068.

Wang, Y. (2014) 网络主权：一个不容回避的议题权威论坛 [Cyber sovereignty: an unavoidable issue (authoritative forum)], *Peoples Daily Online*. http://world.people.com.cn/n/2014/0623/c1002-25183696.html, accessed March 22, 2021.

Wang, Z. (2012) *Never Forget National Humiliation: Historical Memory in Chinese Politics and Foreign Relations*. New York: Columbia University Press.

Webster, G. and Triolo, P. (2020) *Translation: China Proposes Global Data Security Initiative*, New America. http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative/, accessed March 22, 2021.

Wei, Y. (2016) *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty*. The Henry M. Jackson School of International Studies.

https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/, accessed March 22, 2021.

Weiss, J. and Wallace, J. (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

Wildman, Sarah (2017): Why you see swastikas in America but not Germany, https://www.vox.com/world/2017/8/16/16152088/nazi-swastikas-germany-charlottesville, last accessed December 2, 2021

Wu, H. (2016) 发展数字经济推进数字转型 [Develop the digital economy and promote digital transformation], *China Daily*. http://china.chinadaily.com.cn/2016-09/30/content_26945911.htm, accessed March 22, 2021.

Xu, H. (2006) 域名变脸：中国迎战网络主权 [*Domain Name "Volte Face": China vs. Internet Sovereignty*], Sohu. https://it.sohu.com/20060303/n242107118.shtml, accessed March 22, 2021.

Yang, Y. (2012) 外交部条法司司长黄惠康:加强网络领域的国际交流合作 [Huang Huikang, Director of the Department of Treaty and Law of the Ministry of Foreign Affairs: Strengthening international exchanges and cooperation in the cyber field], *People's Daily Online*. http://politics.people.com.cn/n/2012/1005/c70731-19174896.html, accessed March 22, 2021.

Yin, H., Pan, Q. and Shao, L. (2015) 共同构建和平安全开放合作的网络空间——访军事科学院中美防务关系研究中心吕晶华 [Jointly build a peaceful, safe, open and cooperative cyberspaceInterview with Lu Jinghua from the Research Center for Sino-US Defense Relations of the Academy of Military Sciences], Jiefangjun Bao. https://dlib.eastview.com/browse/doc/45550103, accessed March 22, 2021.

Zeng, J., Stevens, T. and Chen Y. (2017) China's solution to global cyber governance: unpacking the domestic discourse of internet sovereignty, *Politics & Politics*, 45, 432464.

Zhang, Y. (2008) Understanding Chinese views of the emerging global order, in G. Wang and Y. Zheng (eds.), *China and the New International Order*, pp. 149167. Abingdon: Routledge.