DOI:
10.1111/polp.12202

Citation for published version (APA):
Zeng, J., Stevens, T. C., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'. *Politics and Policy*, *45*(3), 432-464. https://doi.org/10.1111/polp.12202

China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'

Jinghan Zeng, Tim Stevens and Yaru Chen

Accepted for publication in *Politics & Policy* 45(3), DOI: 10.1111/polp.12202

Abstract

Under Xi Jinping's leadership, China has actively promoted "Internet sovereignty" as a means to reshape the discourse and practices of global cyber governance. By analysing Chinese-language literature, this article unpacks the Chinese discourse of Internet sovereignty. Despite significant interest in promoting it as China's normative position on cyberspace, we find Chinese formulations of Internet sovereignty are fragmented, diverse and under-developed. There are substantial disagreements and uncertainty over what Internet sovereignty is and how it can be put into practice. This is principally due to the evolving pattern of Chinese policy formation, whereby political ideas are often not clearly defined when first proposed by Chinese leaders. This article argues that an under-developed domestic discourse of Internet sovereignty has significantly restricted China's capacity to provide alternative norms in global cyberspace. Appreciating this ambiguity, diversity and, sometimes, inconsistency is vital to accurate understanding of transformations in global cyber governance occasioned by China's rise.

*

"In order to promote reforms in global cyberspace governance, we should insist on the following principles: first, respect Internet sovereignty. The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace… We should respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing."

– *Xi Jinping, excerpt from his keynote address to the World Internet Conference in 2015* (Xinhua News 2015)

Introduction

The rise of digital information communications technologies (ICT), particularly the Internet, has played a significant role in political and socioeconomic transformation. One common argument is that the Internet has helped to undermine authoritarian regimes, or has promoted their removal, by facilitating multiple new modes of information dissemination beyond state control. Less often heard, although of equal importance, is the use by authoritarian regimes of Internet technologies to further their political ambitions. Not only is China the world's largest authoritarian regime but it is the most populous country in terms of Internet users. These factors, and its sophisticated Internet governance strategy, make China a remarkable case study in this field. It has prompted substantial literature examining China's authoritarian use of Internet governance and its political implications (Hughes and Wacker 2003; King, Pan, and Roberts 2013; Noesselt 2014; Yang 2009; Zeng 2016a; Zheng 2007). Yet, China's normative positions in governing the Internet remain an under-explored aspect of its foreign and domestic policy.

Coincident with its "peaceful rise", China has become more willing and able to export its norms pertaining to global governance in order to reshape international order in its favour. The promotion of "Internet sovereignty" (*wangluo zhuquan*) indicates a milestone in China's increasing willingness to set norms in the field of global Internet governance. Internet sovereignty – also translated as "cyber sovereignty" – was brought to renewed public attention during Chinese President Xi Jinping's address to the Beijing-sponsored World Internet Conference in Wuzhen in 2015. As the opening quote indicates, Xi asserted China's position that the Internet should be governed according to the same principles as other fields of international relations.

While the issue of sovereignty in cyberspace has been discussed in the literature of Internet governance, there is a lack of understanding on China's domestic discourse of "Internet sovereignty". This is understandable given the relative novelty of Chinese efforts to promote their norms of Internet governance in global fora, but is nevertheless a deficit in our understanding of contemporary Chinese politics and its implications for global cyber governance.

This article studies how Internet sovereignty is viewed within China, with specific reference to academic agreements and disagreements on the meaning and validity of the concept. By analysing Chinese language literature, we intend to develop a deeper appreciation of the domestic Chinese debate about Internet sovereignty and communicate this to a wider non-Chinese speaking community. Despite significant interest in promoting Internet sovereignty as a normative position on cyberspace, we find this to be a weakly defined concept within China. There are substantial disagreements and uncertainty over what Internet sovereignty is and how it can be put into practice, although there is a general agreement with the official line that national sovereignty should also apply in cyberspace. At the time of writing, the origins, meaning and implementation of Internet sovereignty are sufficiently contested that much conceptual development is still required.

We argue that this is principally due to the evolving pattern of policy formation in China, whereby political ideas are often not clearly defined when first put forward by Chinese leaders. Many political ideas are still developing and have yet to cohere into stable bodies of theory that can be more rigorously tested, and as such are often abstract and immature. This adds to the difficulties of scholars trying to unpack Chinese discourses of Internet sovereignty.

This domestic dynamic, we suggest, has significant implications for understanding the transformation of global governance and international order and its articulation with China's rise. Under Xi Jinping's leadership, China has initiated a series of normative and strategic concepts in order to increase its discursive power and influence. It has made considerable efforts to transform itself from a "norm taker" into a "norm shaper", if not yet quite a "norm maker" (Pu 2012; Zeng and Breslin 2016). The case of Internet sovereignty provides another opportunity to explore this process in Xi's China. It indicates China's ambition to legitimise its domestic coercive activities in cyberspace, as well as developing a normative position supporting China's foreign policy and interests abroad.

Nonetheless, ambition does not equate to success. This article argues that this fragmented, diverse, and sometimes immature discourse of Internet sovereignty has significantly restricted China's capacity to provide alternative norms in global cyberspace, let alone apply them in global cyberspace governance. It remains to seen when or whether China will be able to develop a more rigorous and practical approach to global cyber governance.

The article is organized as follows. We first review the literature on sovereignty and the Internet and then analyse the domestic origin of Chinese Internet sovereignty. This demonstrates how the Chinese Communist Party (CCP)'s regime insecurity and its recent shift to "social management" policies has translated into a range of stricter policies aimed at regulating domestic Internet use, which have been justified using the emergent term, Internet sovereignty. We then move to introduce our research methods and identify the links between academia and policy formation in China. In the third section, we look more closely at how this term has arisen in official discourse, before turning to academic discussions as to how it should be interpreted and operationalised. We identify a strong consensus that sovereignty is applicable to cyberspace but also disagreements about the derivation of Internet sovereignty and the problem of defining sovereign borders in cyberspace. The article concludes with remarks on the domestic and international political implications of China's understanding and promotion of Internet sovereignty.

Internet and Sovereignty

The relationship between the Internet and sovereignty has exercised scholars since the 1990s and is informed by the transformation of international politics under conditions of globalization (Agnew 2009; Cohen 2012; Sassen 1996; Strange 1996). Early analyses identified the transnational nature of the Internet as rendering obsolete sovereignty principles derived from or operable over discrete physical territory (Johnson and Post 1997; Reidenberg 1997). Moreover, cyberspace was proposed as a radical space with its own emergent sovereignty, beyond the authority or control of states (Barlow 1996; see also Wu 1997). Subsequent analyses have picked apart the polysemic concept of sovereignty – "a basket of goods that do not necessarily go together" (Krasner 2001, 233) – in an attempt to discern more precisely how the Internet affects the theory and practice of sovereignty.

Betz and Stevens (2011), for instance, find the Internet offers no direct challenge to the international legal sovereignty of states. International law grants all states sovereign equality and the Internet does not materially affect this situation. In contrast, the Internet has significant implications for state sovereignty if this is understood as the ability either to control cross-border information flows or to exert domestic authority within territorial borders (Betz and Stevens 2011, 55-74). This gives rise, perhaps paradoxically, to measures that require diminution of sovereignty in one area to preserve it in another. The European Convention on Cybercrime (2001), for example, aims to reduce national cybercrime levels through transnational police cooperation leading to cross-border investigations. To do this, states must "pool" their legal sovereignty but at the expense of their sovereign authority over what happens within and across their own borders (Keohane 2002), including changes in national legislation.

This multilateral approach to problem-solving also supports the matrix of Internet governance forms, although few have yet attained global reach. It is a matter of much discussion, for instance, why there has not yet emerged an overall global regime for cybersecurity (DeNardis 2014; Mueller 2010; Nye 2014; Saran 2016). Threats to sovereignty are often cited as reasons why states cannot seem to cooperate globally on issues like cybercrime and cyberespionage which each individually cites as a threat to national and economic security. For fear of jeopardising sovereignty, many states refuse multilateral modes of cooperation that might help save it, leading to a fragmented system of global governance (Stevens 2017). This is widely seen as evidence of states asserting their "Internet sovereignty" in and over cyberspace (Deibert 2010; Demchak and Dombrowski 2013; Gourley 2014).

Whilst fragmentation may not be terminal for the prospects of Internet governance (Mueller 2017; Stevens 2017), it is clear that perceptions of Internet sovereignty differ greatly between states, as do norms relating to sovereignty and governance more generally (Brousseau, Marzouki, and Méadel 2012). What facet one state prioritises, another may deem less important, and competing interpretations of Internet sovereignty are the source of national behaviours that engender political conflict between states. This has been particularly noteworthy in the relations between China and Western democracies, foremost amongst which is the United States (Jiang 2010; Lindsay and Reveron 2015; Powers and Jablonski 2015, 155-179; Shen 2016; Stevens 2012).

These analyses are valuable in interrogating inter-state differentiation and why this presents obstacles to global Internet governance but do not address domestic Chinese debates as to the meaning of Internet sovereignty itself, or how these translate into domestic and foreign policy. This article aims to fill the gap by analysing the Chinese domestic debate of Internet sovereignty and its impact on China's position of global cyber governance.

China's Internet Policy: Domestic Insecurity and Rising Power in Global Cyberspace

A key domestic frame for Chinese Internet policy is the remarkable diffusion of the Internet across its vast population. At the time of writing, the latest official figures (January 2016) indicate that 688 million Chinese are online, just over half the national population and the largest community of Internet users in the world (China Internet Network Information Center 2016). Were these "netizens" to form an independent country, it would be the world's third most populous (Carter 2015). Internet uptake is likely to increase as smartphone and broadband penetration continues, especially in rural areas. The increased access to Internet resources and platforms, including social media, has affected state-society relations in many ways. China has yet to face its equivalent of the Arab Spring, or any serious threat to internal stability, but like all authoritarian regimes it has viewed with concern the potential catalysing effects of Internet and other ICTs on mass civil dissent and disobedience (Brantly 2014; Diamond 2010; Lynch 2011; Mackinnon 2012; Morozov 2011).

For example, China responded nervously to anti-government uprisings in the Middle East in 2011 and arguably overreacted to any stirrings of civil dissent, online or off (Breslin 2012, Dickson 2011). In 2011, when the Arab Spring reached its peak, the Chinese state response to the anonymous call for a Chinese "Jasmine Revolution" included extra efforts to place human rights activists and dissidents under house arrest or in prison, online censorship of terms like “jasmine”, and deploying police to deter – or perhaps more accurately, to crack down on – popular protests (Ramzy 2011).

Two years later, immediately after the military coup in Egypt in July 2013, the Chinese state propaganda machine doubled down on its efforts to link democratization movements in the Middle East with potential chaos at home. Here, the CCP’s propaganda strategy followed a negative approach that aimed to legitimatize its one-party system by discrediting liberal democracy (Zeng 2015). In this context, “Arab Spring” and related terms (e.g. “Jasmine Revolution”) suddenly shifted from a political taboo of Chinese state-owned media to a hot topic that was frequently mocked in China. To understand this inconsistent response, the specific historical conditions of China need to be considered briefly.

Despite China’s rise, regime insecurity has been a constant concern of Chinese leaders (Zeng 2015). While market reforms laid the foundations for China’s present economic status, it also leads to rampant corruption and widening disparities between rich and poor that unsettle the CCP and its claims to political power. The development and growth of ICTs have exacerbated this situation, affording citizens multiple new opportunities to create, find and disseminate information at odds with state narratives. The transnational nature of the Internet has allowed for an “invasion” of Western liberal ideas like democracy that bring into question the legitimacy of the one-party state and the viability of traditional models of centralised information control. As such, many argue that the development of Internet would deliver democracy in China (Liu and Chen 2012). The Chinese government, however, has responded with impressive technical efforts to prevent and deter access to potentially destabilising ideas. The best-known of these is the Golden Shield Project, original plans for which date to the late 1990s (Inkster 2015; Walton 2001). Via the so-called “Great Firewall of China”, this blocks access to blacklisted Internet resources and censors network traffic for banned keywords and phrases.[1] It also encourages behavioural change in Internet users for fear of criminal investigation and prosecution, via a matrix of technical surveillance, legal and regulatory measures (Deibert *et al.* 2011; Deibert 2015).

Since 2011-12, Internet policies have been further developed to support “social management”, a wide-ranging official concept stressing social stability, public security and the enduring leadership of the CCP (Pieke 2012). It is a technocratic and creative response to global change that preserves the socialist ideology upon which government legitimacy is founded, in symbiosis with neoliberal principles that enable economic growth and social mobility. The Internet is an important site of social management implementation, in which the state “is both more powerful and resourceful and less direct and invasive” (Pieke 2012, 149).

One example is Sina Weibo, the Chinese microblogging equivalent of Twitter. The state has implemented various regulations requiring users to register their real names to use Weibo, thereby strengthening its social surveillance capacity.[2] It has also taken more direct efforts to suppress anti-government, or pro-liberal, views on Weibo, arresting some well-known opinion-formers on charges of immoral conduct (e.g. entrepreneur Xue Manzi), or banning others from

[1] In concert with the ostensibly defensive Great Firewall China has also developed offensive tools that can be directed against opponents of Chinese Internet censorship. See, for example, the “Great Cannon” (Stevens 2015a).

[2] Interestingly, this kind of censorship on Wechat (the most popular chat app in China) mainly applies to China-based accounts not international accounts. As a result, it “creates a ‘one app, two system’ model of censorship” (Ruan *et al.* 2016).

using social media accounts (e.g. scholar Zhang Lifan) (South China Morning Post 2013, 2014). At the same time, local government has adopted Weibo as a means of engaging with citizens as part of broader social management policies (Schlæger and Jiang 2014). Central government has similarly used Weibo and other platforms to monitor public sentiment, shape domestic policy and government information activities, and to 'neutralize potential threats' (Sullivan 2014, 31). As Noesselt (2014) points out, social media, Weibo in particular, have been integrated into the regime's social management strategy in an attempt to enhance its legitimacy.

In the meanwhile, driven by its regime insecurity, China has also taken impressive efforts in adopting ICT to strengthen its domestic surveillance (Zeng 2016a). Its "social credit system", for example, has put forward an ambitious blueprint to digitalize its individual archives, in which it records the digital presence activities of every single citizen (Clover 2016; Yap and Wong 2015). Since 2015, Internet sovereignty has also been embedded in China's national security law as a part of renewed efforts to secure the one-party system in China in the face of growing political opposition (Agence France-Presse 2015).

In short, historical and contemporary concerns over regime insecurity are played out in Chinese government attempts to strengthen its control over domestic cyberspace. This domestic regime security concern is often less noticed when discussing China's rise. For example, it is completely missing in Mearsheimer's (2014) offensive realist analysis of China's rise. However, it plays a crucial role in deciding China's foreign policy. One characteristic of this diverse landscape is a "more assertive authoritarianism at the international level" (Deibert 2015, 70). In this context, Internet sovereignty has been promulgated at the global level to legitimise Beijing's domestic social management of cyberspace and its wider attempts at Internet governance. It also forms a part of China's political marketing strategy to build soft power for the authoritarian regime.

Moreover, China is calling for support in asserting national sovereignty in cyberspace. In the global arena, there is a wider debate in global cyber governance over whether cyberspace should be globalized or subordinated to national and territorial concerns. To some, the current cyberspace is US-centric and thus problematic in many ways. The case of the US National Security Agency's PRISM clandestine surveillance programme, for example, exposed the problem of information and network security in this US-centric cyberspace (Greenwald and MacAskill, 2013). PRISM facilitated the collection of personal and commercial data from American Internet companies including Google, Facebook, Yahoo, Apple and Microsoft. Its surveillance targets included entities of interest not only in China and Russia but also US allies such as the EU and its member-states. To many, the case of PRISM shows that the US is taking advantage of existing Internet governance mechanisms in favour of its own national interests (Lu 2014; Shen 2013). Specifically, these arguments allege that, while promoting 'Internet freedom' and a tacit acceptance of cyberspace as a global commons beyond the sovereignty of any state, the US has abused the notion of public goods so provided (Leavitt 2012; Lukasik 2000).

In this regard, some would prefer a sovereign, nationally partitioned cyberspace. Thus, countries including Russia, Brazil, South Africa, and Iran have taken a similar position with China to support a more traditional state-centric, sovereignty-oriented regime (Stevens 2015b). This position on state's sovereign rights in cyberspace is based on conventional readings of territorial rights and obligations, rather than on "Western" narratives of global information flows across an “open” Internet or global cyber commons (Nocetti 2015). To some extent, China’s World Internet Conference in Wuzhen since 2014 has served as a summit for those countries to openly align themselves against the current global and private sector-led regime promoted and dominated by the US. This again reflects China’s importance and leadership credential in contesting the US-dominated international order.

Indeed, even before its first World Internet Conference, China actively took the lead in various regional governance bodies to assert the principle of Internet sovereignty and reshape existing cyber norms. In September 2011, for example, China along with other five members of Shanghai Cooperation Organization (Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) submitted a document “International Code of Conduct for Information Security” to the United Nations in order to formalize new rules and norms in cyber governance. According to the then director of the United Nations Institute for Disarmament Research, it was “rather vehemently rejected by the United States and most Western states, who see the effort as aimed at establishing a strict national sovereignty model over content flow over the Internet and potentially a tool of oppressive regimes” (Hitchens 2014). After this initiative failed to win global support, an updated Code of Conduct was submitted to the UN in January 2015. Despite its controversy, the notion of Internet sovereignty remains a crucial component of this updated version (Rõigas 2015).

As the following sections will show, while China is taking the lead to promote Internet sovereignty, it does not yet have a firm conceptualisation or consistent definition of what Internet sovereignty is or entails.

Methods and Formation of Political Ideas in China

In order to understand the Chinese discourse of Internet sovereignty, this article surveys the Chinese language literature on this topic, including Chinese academic journals, newspapers and policy documents. We searched China National Knowledge Infrastructure, the largest journal database in China, for two key words “Internet/cyber” (*wang luo*) and “sovereignty” (*zhu quan*). All articles with these two words in their titles are included in our database, which focuses inevitably on articles published after 2012, when the term “Internet sovereignty” began to emerge in explicit fashion. Our pilot study first briefly read through all the articles found through key word search and then identified the key themes in the Chinese debate. Afterwards, we analysed those articles with a focus on the disagreement and consensus among those key themes.

The nature of the database means that we were unable to examine internal policy documents or the views of dissidents. The former are not available for public research and the latter have little policy relevance. We also do not claim that this academic discussion translates directly into policy in China; far from it. Nevertheless, it can play a significant role in shaping emerging policies. This influence is related to how political ideas develop in China, as mentioned before. When Chinese top leaders put forward new political ideas, they are often not clearly defined, serving more as guidelines (if not slogans) for policy than as precise blueprints (Zeng, Xiao and Breslin 2015). The subsequent process of imbuing these concepts with meaning and substance often occurs in an incremental manner. Academic and political discussions play key roles in steering and shaping the development and emergence of these policy ideas. Recent examples under Xi Jinping's leadership include diplomatic initiatives like "New Type of Great Power Relations" and "One Belt, One Road"'.

When Xi Jinping first proposed to establish the so-called "New Type of Great Power Relations" in 2012, it was a loosely articulated diplomatic initiative targeting Sino-US relations, specifically how to manage potential conflicts within this bilateral relationship. Yet, the subsequent development of this concept, informed by different interpretations and uses by the Chinese academic and policy community, has extended it into a much broader initiative (Zeng 2016b). It now refers not only to China's bilateral relations with the US but also with other major powers like the European Union (Zeng and Breslin 2016). Similarly, 'One Belt, One Road' – the Silk Road Economic Belt and the 21st-century Maritime Silk Road – has evolved from China's periphery diplomacy in 2013 into a broad global strategy that even targets countries like Australia and Brazil that have little to do with China's ancient Silk Road (Zeng 2017).

We argue that this is also the case for Internet sovereignty. When Xi Jinping promoted this concept in Wuzhen in 2015, he did not elaborate on its specifics. Xi asserted that sovereignty matters in cyberspace affairs and that the state should exercise some form of control over cyberspace within the context of the international system of state sovereignty. As will be demonstrated below, Chinese scholars recognise its conceptual elasticity and seek to improve its clarity and applicability in order to influence Chinese policy.[3]

The Chinese Search for Internet Sovereignty

Despite the concept of Internet sovereignty being brought to wide public attention by Xi Jinping's address in 2012, the emphasis on national sovereignty is not entirely novel. Beyond the relatively new Internet industry, this emphasis on sovereignty has a long historical pedigree in China's communications infrastructure industry. As early as the late Qing dynasty, Chinese nationalists had struggled to secure national independence against Western hegemony in industrial communication and transportation. The Qing dynasty's weak military strength forced it to let Britain, Denmark and Russia take full control over this industry until 1899 (Pitt, Levine, and Yan 1996). The struggle to be rid of foreign influence prompted domestic uprisings, not least the "Railway Rights Protection Movement" in the second decade of the twentieth century. The Qing dynasty's attempted suppression of this movement triggered a revolutionary uprising that eventually ended two millennia of Chinese imperial rule (Rankin 2002).

As a result of this bitter early experience, the Chinese government tends to view telecommunications as a matter of "high politics" intertwined with national strategy and military value, rather than "social or economic benefit" (Pitt, Levine, and Yan 1996). This perception has shaped a highly conservative telecommunications policy with strict control over foreign investment (Pitt, Levine, and Yan 1996; Yan 2002).

[3] There are many channels through which they can achieve this. Leading scholars are invited to lecture officials at all levels of government, from local institutions to central ministries, and even the politburo, the most powerful organ of central government, attended by the top 25 Chinese leaders (Tsai and Dean 2013). State research councils and governmental organizations also fund social science projects that will generate policy advice. Indeed, the general character of Chinese scholarship on politics and international relations is one of policy advice, rather than theoretical development, as demonstrated by previous studies (Zeng 2016; Zeng, Xiao, and Breslin 2015; Zeng 2015, 96-114).

When it comes to cyberspace, the nationalistic emphasis on sovereignty has long underpinned China's Internet policy. The avoidance of foreign manipulation has always been one of the most important goals of China's Internet policy. As discussed before, in contemporary China the regime has developed various national projects – such as the Great Firewall of China – to secure its Internet information and networking since the late 1990s. Nonetheless, China had not actively promoted these domestic Internet policies on the global stage in order to reshape global discourses of cyber governance until Xi Jinping took power. Xi's high-profile promotion of Internet sovereignty openly articulates China's desire to contest the existing multistakeholder model of Internet governance promoted by the US. This involves traditional states and international organizations, as well as a range of new institutions, non-state actors, non-governmental organizations (NGOs), technical advisory bodies, civil society, and private entities, arrayed and operating in distributed and networked fashion (DeNardis 2014:23).

China has sought, for example, to participate in and reform the Internet Corporation for Assigned Names and Numbers (ICANN), the US-hosted non-profit organisation that manages and maintains Internet "namespace" (Mueller 2011). This ambition is listed as an explicit goal of China's Information Development Strategy (State Council of China 2016). China and its allies sought to counter perceived US influence over ICANN by forcing the US Department of Commerce to abandon a contract with ICANN that China and others consider deleterious to global cybersecurity. China has worked since the early 2000s to this end. For example, China hosted ICANN meetings in 2002 and 2013, and Chinese Internet giants such as Alibaba and Tencent, the Ministry of Industry and Information Technology, and the Internet Society of China, have participated actively in ICANN's affairs in the multi-stakeholder model that structures ICANN's activities and networks. At the same time, China and Russia have worked tirelessly in regional fora like the Shanghai Cooperation Organization and international organizations like the International Telecommunications Union to undermine the American position. In October 2016, the US government severed its formal ties with ICANN, a decision perceived widely as a victory for China and Russia (Kessler 2016). The Deputy Director of the National Internet Information Office called the handover a progressive step in global cyber governance and a valuable attempt to "bridge the digital divide between developing and developed countries" (Li 2016).

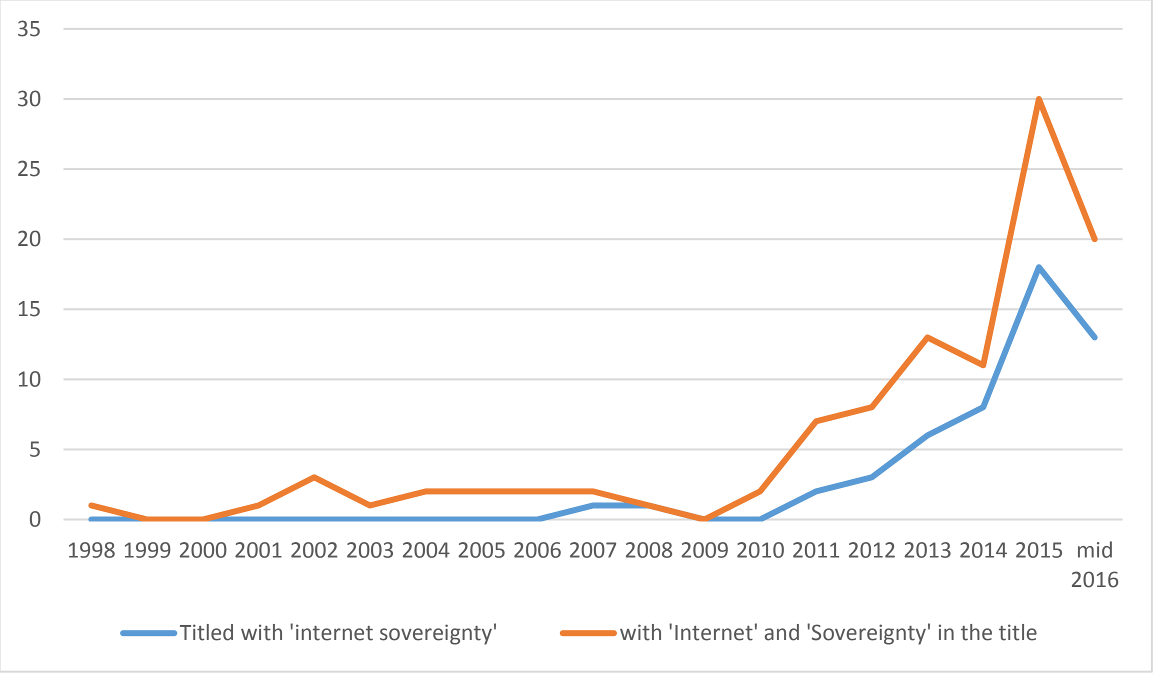
In the context of Internet sovereignty, China's move was less a displacement of the US than an attempted entrenchment of state prerogatives in global Internet governance. China and its allies pursued the ICANN issue in order to reimpose multilateralism on multistakeholderism. Whilst it is important not to over-state the influence of states on the day-to-day technical management of the Internet (Van Eeten and Mueller 2012), Internet sovereignty of the Chinese kind implies strongly that states should have the final say in determining global Internet policy (Han 2016).

This undercuts the more pluralistic visions of multistakeholderism and is consistent with China's position on other issues of global governance. From a Western perspective, global governance is informed by neoliberal imperatives that allow for the incorporation of international organizations, NGOs and civil society in decision-making if this improves the circulation of capital. This "governance without government" model (Rosenau and Czempiel 1992; Held *et al.* 1999) is at odds with a Chinese state that can no more allow for such distributed governance abroad than it can at home. The CCP still plays the central role in internal socioeconomic affairs and the development of NGOs and civil society is highly controlled. In this regard, China's global governance efforts downplay the role of non-state actors for domestic reasons as much as international ones.

The following discussion will focus on China's contemporary search for Internet sovereignty. As Figure 1 shows, academic discussions about the relationship between national sovereignty and the Internet date back to at least 1998. Since then, Chinese scholars have engaged actively with the challenges brought by the Internet and new technologies to China's national sovereignty. Not surprisingly, its impact on the political system is a key focus. It is argued, for example, in an article published in 1998, that the US may take advantage of its "information hegemony" in cyberspace to promote regime change in developing countries (Lao and Xiao 1998:29). This is to say, even if the concept of Internet sovereignty had not been explicitly used, the preliminary idea – that sovereignty applies in cyberspace – has deep historical roots in Chinese academic discussions. Given the aforementioned contested origins of Chinese telecommunication industry and the concern over regime security, this is hardly surprising.

Scroll forward to today's China and a very different focus of debate on Internet and sovereignty was evident when Xi Jinping proposed to respect Internet sovereignty. While the current academic debate still emphasises the challenges posed by the Internet to sovereignty and, more specifically, to one-party rule, new agendas have gradually come to the fore. Early debate prioritised analysis of these challenges but current discussions aim to provide specific and policy-related solutions to those challenges in the form of Internet sovereignty. The desire to legitimize China's normative position on cyberspace has driven Chinese scholars to elaborate the idea of Internet sovereignty and how it can be put into practice, as we shall discuss in the following sections.

Figure 1: Number of articles in Chinese language literature with "Internet sovereignty" or "Internet" and "sovereignty" in the title



Source: Data collected on 23 May 2016 from China National Knowledge Infrastructure, www.cnki.net/.

Consensus

At the outset, it is important to note the concept of Internet sovereignty does not enthuse *all* Chinese elites, especially those of a liberal persuasion. To them, the instigation of this policy represents an attempt to condone state control of people's rights to access and use the Internet and impinges upon freedom of speech (e.g. Dong 2015; Fu 2015; Li 2015; Yu 2015). They argue that citizens' Internet rights extend to, one, the freedom to access the Internet and, two, the freedom to share content on the Internet. The state has a responsibility to ensure the former and not to censor or otherwise interfere with the latter. In both cases, the state should not discriminate between Internet users; their rights, as understood, are absolute, not relative or contingent.

It is further suggested in this literature that the World Internet Conference (2015), at which Xi Jinping proposed the idea of Internet sovereignty, was something of a "joke": it was "a gathering of 'third-rate countries' picking a quarrel with advanced (liberal) countries" (Li 2015). The only purpose in promoting this idea was to try and block foreign information and thus enable the government to better "deceive the public" (Yu 2015). Needless to say, this sort of dissenting voice often spreads online with little impact on actual policy, not least as these opinions are disbarred from appearing in official academic journals.[4] This article will focus on academic studies that attempt to define Internet sovereignty in a policy context, as well as discussing how to put this concept into practice.

Among those academic studies, there is consensus on two aspects of Internet sovereignty. First, it is a relatively new concept and its definition is therefore unclear. Precisely because of this, the academic articles we examine aim and call for developing the theory of Internet sovereignty (e.g. Gao and Chen 2016; Liu 2012). As identified previously, when new ideas are put forward by Chinese leaders they are often not defined clearly. There follows a process of imparting meaning and substance to policy ideas, in which academic and other discussions play key roles. This is also the case with Internet sovereignty, which is why consideration of academic debates is important in this context. The second broad consensus affirms that, despite the imprecision of the term, China should seek to protect and promote its Internet sovereignty, *contra* the opinion of many online dissenters (e.g. Wang 2012; Wang 2013; Yu 2012). Internet sovereignty is therefore framed as one means through which to defend and preserve China's national interests.

Disagreements

Consensus therefore exists about the imprecision yet importance of Internet sovereignty but there are significant disagreements about three issues that arise from its consideration: the relationship between Internet sovereignty and "information sovereignty"; the origins of the

[4] This kind of irony against official language is not unique to "Internet sovereignty" but exists widely in subverting other official concepts (e.g. Nordin and Richaud 2014).

term, Internet sovereignty; and the problem of how and where to define “network frontiers”. We address each in turn.

Internet Sovereignty and Information Sovereignty

The first area of disagreement concerns the fundamental applicability of the concept of Internet sovereignty. As noted above, some reject it on ideological grounds, as it promotes the essential right or obligation of the state to restrict freedom of expression. In contrast, the scholars under consideration here accept the state should exert control over the Internet: why should cyberspace be exempt from state control, given that few other environments are so excluded? Within this group of scholars, however, there is disagreement over whether Internet sovereignty is the optimal term to describe this political endeavour.

Indeed, before the term “Internet sovereignty” was widely accepted in China, academic discussions often referred to “information sovereignty” (Du and Nan 2014; Guo 2010; Ren 2007; Yang 2006, 2012; Yu 2003, 33). To Yang Zewei, a professor in law, for example, information sovereignty refers to sovereign states’ rights to autonomy and independence (Yang 2006, 2012). A sovereign state has the rights to (a) control transboundary information, (b) to regulate and manage how information flows in and out of a country as well as jurisdiction over disputes arising in this context, and (c) to share information based on international cooperation (Yang 2006, 2012). This definition is adopted in major textbooks of law and communication in China (Guo 1999, 251-252; Yu 2003, 33).

Some argue that information sovereignty reflects national sovereignty in cyber activity (Guo 2010; Ren 2007, 74). It is the state capacity to “protect”, “manage” and “regulate” information (Kong 2000; Liu and Chang 2005; Ren 2007, 72). In other words, the word “information” in this “information sovereignty” concept *only* refers to information in cyberspace. In this sense, as “information sovereignty” already reflects national sovereignty in cyberspace, why is there a need to introduce a new concept like Internet sovereignty to refer to the same thing?

Others argue that the two concepts are not equivalent (Du and Nan 2014). Information exists outside of cyberspace and also pre-exists the Internet. Information sovereignty is therefore not a new concept and has a similarly long history to, for example, political sovereignty and cultural sovereignty (Du and Nan 2014).[5] Internet sovereignty, on the contrary, is a new concept developing only with the emergence of Internet. In addition, Internet sovereignty not only refers to information “within” cyberspace but also the platforms that produce, transmit and share that information. Therefore, Internet sovereignty is a broader yet more accurate concept than information sovereignty when considering the implications of cyberspace for national sovereignty (Du and Nan 2014).[6]

[5] Indeed, the Chinese debate on governing cyberspace is closely related to the sense of ‘cultural sovereignty’ (Cornish 2015).

[6] We do not explore here the conceptual and practical links between certain conceptualizations of information sovereignty and the insurgent term, “data sovereignty”, defined as governments’ “exclusive authority and control over all virtual public assets” (Irion 2012, 41), although they are clearly related.

Notably, “information sovereignty” was used by Xi Jinping in 2014 to refer to what he now means by Internet sovereignty. According to Xi:

> Although the Internet is highly globalized, the sovereignty of the information of all countries should be respected. No matter how developed a country’s Internet technology is, it must not violate the information sovereignty of others (People’s Daily, 2014).

This suggests that the two terms are being conflated in official discourse. The evidence does not allow us to determine if this is a function of unfamiliarity with relatively novel ideas, or if it betokens the eventual substitution of Internet sovereignty for information sovereignty. This is an evolving discourse on the relationship between sovereignty and the Internet and key terms have yet to stabilise in use and meaning. Other foundational terms like “cyberspace” are similarly fluid in their characterisation and application. This is hardly unique to the Chinese case alone, the global terminological appeal to “cybersecurity”, for example, generally being “often elastic in definition and elusive in practice” (Stevens 2016, 23).

Origins of Internet Sovereignty

A second disagreement concerns the origins of the idea of Internet sovereignty itself. Some consider it a Chinese invention. Ye Zheng, a senior director of the Chinese Academy of Military Sciences, finds that Internet sovereignty is a specifically Chinese innovation in the theory of political sovereignty, expressly intended to support Chinese national security (Ye 2015). To Zhi Zhenfeng, a scholar based in the Chinese Academy of Social Sciences, it is a Chinese solution for improving global Internet governance and reflects China’s intention to be a responsible Internet power (Chen 2015).

Others argue that Internet sovereignty is the product of multilateral cooperation, or is at least supported by groups of like-minded nations. Two differing perspectives on the multilateral origins of Internet sovereignty are represented within this group of scholars. One identifies Internet sovereignty with the balancing actions of less-developed countries against more highly-developed nations; the other traces its roots to Western applications of sovereignty to cyberspace.

In the first case, Internet sovereignty is conceived as the outgrowth of collective actions by less-developed countries to defend their national interests against more developed countries (An 2016; Lu 2014; Zhang and Ren 2016). According to Lu Chuanying, a scholar on cyberspace and global governance based at Shanghai Institute of International Studies, states divide into three categories of ‘Internet power’, according to the distribution of power and influence in cyberspace: developed Internet powers, emerging Internet powers, and developing Internet powers (Lu 2014). Developed Internet powers, the US in particular, argue that the Internet is a global commons, over which no state may lay claim on the basis of national sovereignty. If other states do not constrain US activities in cyberspace, this assists implicit US hegemonic claims over the global Internet and furthers US national interests. However, it is also argued that the US is practicing a double standard (Gao and Chen 2016; Lu 2014). Domestically, the US has strengthened its supervision and state surveillance, as well as its transnational surveillance and intelligence practices and capabilities, as illustrated by the case of Edward Snowden, but also captures the intensification of US domestic surveillance in the aftermath of the terrorist attacks of 11 September 2001. Indeed, some Western commentators suggest that the official Chinese push to formalise Internet sovereignty is a direct response to the Snowden disclosures of 2013 (Livingston 2015).

Emerging Internet powers like Russia and China have some strength in Internet technology and capacity (Lu 2014). Unlike developed Internet powers, they argue that state sovereignty should be respected in cyberspace affairs. They also adopt a more defensive position in terms of national (cyber) security and position themselves against the prospects of US Internet monopoly or hegemony. Thus, this group of countries are active promoters of Internet sovereignty. According to Lu (2014), this group includes Russia and China, but the identities of other members of this grouping are unclear. For example, do Brazil and India belong to this group, not least as both have been vocal in criticising US actions in cyberspace? (Ebert and Maurer 2013).

Lu (2014) considers developing Internet countries as the weakest category of countries, in that they have to accept the relevant Internet technology and standards developed by the previous two groups. States in this group have to rely on and work with emerging Internet powers in order to better secure their national interests. Although the reasoning is left unstated, from the broadly Marxist perspective of these commentators the cooperation between developing and emerging Internet powers is a means of challenging and, ultimately, diminishing US hegemony.[7] Thus, Lu (2014) argues that to promote Internet sovereignty is one way of fostering equality and justice in cyberspace.

The second angle sees Internet sovereignty as an originally Western creation. As briefly mentioned above, it is argued that the US has actively promoted domestic supervision and state surveillance through Internet technologies. In this regard, the US is "the pioneer and leader" of Internet sovereignty (Lu 2014). This idea can also be traced to the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, published under NATO auspices in 2013 (Cui 2013; Gao and Chen 2016; Yuan 2016a; Yuan 2016b). The product of a working group of international lawyers drawn from NATO member-states, this document does not mention Internet sovereignty specifically but endorses the applicability of state sovereignty to cyberspace. According to Rule 1,

> A state may exercise control over cyber infrastructure and activities within its sovereign territory… Accordingly, cyber infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace is subject to the sovereignty of the territorial State. (Schmitt 2013, 15-16)

This principle is frequently used by Chinese scholars to legitimize China's position on Internet sovereignty (e.g. Cui 2013; Zhu 2015). In this sense, it is the US rather than China that initiated the principle of national sovereignty in cyberspace. Thus, there should be no reason for the US to oppose China's normative position on Internet sovereignty, which is merely a restatement of that principle.

Some Chinese scholars are critical of the Tallinn interpretation, a critique that is closely bound up with practical considerations about how and to define the boundaries of the Internet (Chen 2014; Yuan 2016a; Yuan 2016b). In order to operationalise Internet sovereignty, there

[7] Zhang Chunhou (2012), a professor at Yan'an University, uses a more explicitly Marxist term, "network colonization", to describe hegemonic powers who attempt to overthrow foreign regimes.

must be more precise identification of where “network frontiers” or “network borders” lie, so as to be able to project sovereignty over the spaces within those frontiers or borders, howsoever defined. Network frontiers do not map directly to geographical borders, as indicated by the argument that it is unfair to use the geographic locations of cyber infrastructure, *per* the Tallinn Manual, as the sole criterion to define network frontiers (Yuan 2016a; Yuan 2016b). If we applied this rule, much of the Internet would be in American territory and subject to US sovereignty, as most Internet root servers and many enterprise servers are located there (Yuan 2016a; Yuan 2016b).

Similarly, neither is it equitable to define Internet borders by the quantity of information resources, population of netizens, or the economic scale of national networks, according to Yuan Yi, a scholar based in the People's Liberation Army’s Academy of Military Sciences (Yuan 2016a; Yuan 2016b). As most information on the Internet is available in English, China could lay claim only to a very small portion of Internet “territory” if integuments were determined by the relative size of information resources (Yuan 2016a; Yuan 2016b). The only favourable way would perhaps be by population of netizens, which would grant China the largest share by some margin. Nonetheless, we find little support for this principle in China. Debate has therefore turned to how best to define network borders/frontiers in respect of Internet sovereignty.

Defining Network Frontiers

As identified previously, there is no simple correlation between geographical borders and the borders of the state in cyberspace (see also, Johnson and Post 1997). There are at least three contrasting perspectives on this issue in Chinese literature, all of which are concerned with how best to define borders as a means of implementing Internet sovereignty in practice.

The first leverages the Tallinn interpretation outlined above and uses the geographic locations of cyber infrastructure to determine where network frontiers lie (Liu 2012; Wang 2012). As such, the responsibility for regulating certain behaviours in cyberspace lies with the state within whose conventional territorial borders those activities originate (Liu 2012; Wang 2012). Following this logic, this applies even to those situations in which, for example, an actor in country A attacks country B using the resources of country C. Country C would still be responsible at some level for those actions and should regulate to control such actions.

Proponents of this view are fully aware of its potential consequences, as it may benefit countries like the US that possess developed network technologies at the expense of those that do not. The latter may suffer from cyberattack conducted in countries which have better technology. In this sense, the opposite argument is also valid: that more developed countries can be used by actors in less-developed countries to launch attacks, although this is not noted in the relevant literature. Nonetheless, it is argued that this may motivate less-developed countries to prioritise network defence technologies and physical facility protection (Liu 2012). In this regard, the efficiency with which network frontiers can be determined is considered more important than fairness.

The second view moves the debate forward by developing the idea of “non-physical network frontiers”. Two types of network frontier are proposed: tangible and intangible (Ye and Zhao 2014; Yuan 2016a; Yuan 2016b). Tangible network frontiers include national network infrastructure and core network systems such as finance, telecommunication, transportation, and energy, as described by the *Tallinn Manual.* Intangible network frontiers consist in, for example, top-level Internet domain names like .cn or .uk. These are counted as national territory and those Internet locations that take these domain names exist within these intangible but sovereign “borders”.

Alternatively, Hao Yeli, a retired major general, retains “tangible network frontiers” but introduces a new term, “flexible frontier”, to replace “intangible network frontiers”. According to Hao, there are three layers of network frontiers (Hao 2015). The outermost layer is also the so-called “flexible frontier” (also referred by Hao as “capability frontiers”). It refers to the range of a country’s national Internet capacity. The middle layer refers to the geographical border including cyber infrastructure and domestic public opinion field. Here, it transcends the tangible network as it includes the public opinion field. In the Chinese context, more specifically, to defend this border means the government needs to actively resist the “invasion” of Western liberal ideas like democracy that might challenge the current one-party system. Lastly, the innermost layer refers to the core circle of the CCP regime. Needless to say, this model is heavily inflected with regime security concerns. Compared with the first view outlined above, it is, of course, much harder to decide where these borders lie and what lies within them.

The third view uses levels of network access to define where network borders lie. Similar to the categorisation of maritime delimitation, i.e. international waters, territorial waters, exclusive waters, it is argued that cyberspaces could be divided into public networks, territorial networks and exclusive networks (Yuan 2016a; Yuan 2016b). Public networks are similar to international waters of the global commons that are not restricted by internal borders, although they are negatively defined by external borders. Everyone in the world has free access to those public networks, regardless of nationality. Similar to territorial land, water and airspace, territorial networks include networks that are isolated from the outside world such as government and military intranets. Access is only granted to authorised actors and unauthorised access is treated as a violation of Internet sovereignty. Exclusive networks are analogous to exclusive waters, and share information with external locations but operate strict controls over access, such as business, finance and e-government services (Yuan 2016a; Yuan 2016b). An everyday example would be online banking services that are only available to authorised banking customers.

Concluding Remarks

This preliminary analysis has explored academic contributions to the emerging debate about Internet sovereignty in China. There exists significant consensus that Internet sovereignty is a proper concern for the Chinese government and that China’s interests are well-served by pursuing Internet sovereignty as a matter of formal policy. At the same time, there are several areas of disagreement amongst scholars able to participate in these discussions. The first is an unresolved discussion about the relative merits of the terms, “information sovereignty” and “Internet sovereignty”, and whether they are cognate or not. There are hints that Internet sovereignty may replace information sovereignty as the official term of choice, although the evidence is insufficient to make a strong case for this. If this terminological and policy shift occurs, it may represent a broadening of the concept of sovereignty with respect to information communications technologies. This argument is further substantiated by considering that the alternative translation of *wangluo zhuquan* is ‘cyber’ sovereignty. The use of ‘cyber’ elsewhere in the world, particularly in the West, is often deliberately non-specific and acts as a broad rubric under which all manner of ICT-related activities can be grouped, regardless of their affinities and relationships (Stevens 2016, 3-4). This presents opportunities for the extension of sovereign power and control where previously these were limited (Dunn Cavelty 2007). “Cyber”, and to a certain extent, “Internet”, are far more politically useful terms than “information” alone.

The second area of disagreement is a more abstruse debate over the origins of the term ‘Internet sovereignty’ itself. Some authors identify its origins in China alone, others in a multilateral drive to balance US hegemony. There is also recognition that Western powers, particularly through the NATO-sponsored Tallinn Manual process, have already articulated a form of Internet sovereignty, inasmuch as they recognise a state’s sovereignty over cyber infrastructure and activities within its sovereign borders. In this case, the West should not protest too much about China’s very similar argument as to the validity of Internet sovereignty as a principle upon which international ‘cyber’ relations should be founded. The problem, however, is precisely how and where to draw those sovereign borders, as the third area of debate around ‘network frontiers’ illustrates. In keeping with the role of Chinese academics as advisors on practical implementation as well as policy refinement, this is a more technical discussion about where sovereignty applies and how to define its limits.

These debates follow the conventional pattern of policy development in China. Concepts and policy ideas are expressed in initially inexact fashion by high-level officials, in this case President Xi, and are elaborated through consultation and negotiation, re-emerging later as China’s policy narratives. The preliminary empirical inquiry presented here is but a snapshot of the early stages of this process and it is unclear precisely what form of Internet sovereignty will ultimately exist in official policy and China’s global stance, although its broad parameters are clear and form an identifiable facet of current Chinese domestic and foreign policy. The question remains, then, as to the political functions of Internet sovereignty now and in the immediate future.

As identified previously, Chinese Internet policies have both domestic and international aspects, each of which is intimately tied to concerns about regime security. From the perspective of the CCP, threats to regime security derive from both domestic sources and from external influence, the latter particularly mediated by the Internet. Domestic Internet censorship is therefore geared both to suppressing indigenous political dissent and to restricting the influx of foreign ideas corrupting of the Chinese populace, either of which, or both in combination, could lead to the delegitimisation of the CCP and the destabilisation of the Chinese state. In this context, the pursuit of Internet sovereignty is both a justification of its domestic policies and an attempt to ward off foreign interference both ‘hard’ and ‘soft’.

In the latter register, Internet sovereignty serves an important international function, as China attempts to shape international norms around inter-state behaviour in cyberspace and the nature of statehood in the informationalised 21st century. A group of countries have already aligned with China’s normative positions in cyber governance, which are antagonistic to those promoted by the US and its allies. In this regard, China has elevated its leadership status by providing an alternative to Western cyber governance.

At the same time, this attempt to reshape cyber norms also helps to improve the CCP’s domestic legitimacy and improve regime security. In this way, Internet sovereignty serves both domestic and foreign policy goals, united by a fundamental concern with the maintenance of the Chinese state. In the global arena, however, the relevant discourse is not yet sufficiently developed to be either convincing or practical, let alone widely applied in governing global cyberspace. This has no doubt significantly restricted China's capacity to challenge existing cyber norms. Without a more rigorous and practical theory of Internet sovereignty and global cyber governance, China can hardly transform itself from a norm taker to a norm shaper, not to mention a norm maker.

About the Authors

Jinghan Zeng is Lecturer in the Department of Politics and International Relations at Royal Holloway, University of London. His research lies in the field of Chinese politics with more specific interests in the study of China's authoritarian politics, political communication, political economy and foreign policy. He is the author of *The Chinese Communist Party's Capacity to Rule: Ideology, Legitimacy and Party Cohesion* (Palgrave, 2015).

Tim Stevens is Lecturer in Global Security in the Department of War Studies, King's College London. He has published on cybersecurity and related issues in a wide range of media and peer-reviewed journals. His recent book is *Cyber Security and the Politics of Time* (Cambridge University Press, 2016) and he is the co-author of *Cyberspace and the State* (Routledge, 2011). He is a Fellow of the Royal Geographical Society, London.

Yaru Chen is Research Fellow at the Warwick Business School, University of Warwick. Her research interests include public management and governance in the UK and China.

References

FRANCE-PRESSE, AGENCE. 2015. "China Passes New National Security Law Extending Control Over Internet." 1 July. Accessed on January 30, 2017. Available online at https://www.theguardian.com/world/2015/jul/01/china-national-security-law-internet-regulation-cyberspace-xi-jinping

AGNEW, JOHN. 2009. *Globalization and Sovereignty*. Lanham, MD: Rowman & Littlefield.

AN, JING. 2016. 网络主权原则是全球网络治理的必然选择 (Internet sovereignty is a necessary choice of global cyber governance), *红旗文稿 (Red Flag Manuscript)* 4: 30-31.

BARLOW, JOHN PERRY. 1996. "A Declaration of the Independence of Cyberspace." Accessed on January 26, 2017. Available online at https://www.eff.org/cyberspace-independence

BETZ, DAVID J., and TIM STEVENS. 2011. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge for the International Institute for Strategic Studies.

BRANTLY, AARON FRANKLIN. 2014. "The Cyber Losers." *Democracy & Security* 10 (2): 132-155. Accessed on 30 January, 2017. Available online at http://www.tandfonline.com/doi/abs/10.1080/17419166.2014.890520

BRESLIN, SHAUN. 2012. “China and the Arab Awakening.” *ISPI Analysis* 140: 1-8, Accessed on January 30, 2017. Available online at http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_140_2012.pdf

BROUSSEAU, ERIC, MERYEM MARZOUKI, and CÉCILE MÉADEL, eds. 2012. *Governance, Regulation and Powers on the Internet*. Cambridge: Cambridge University Press.

CARTER, LIZ. 2015. *Let 100 Voices Speak: How the Internet is Transforming China and Changing Everything*. London: I.B. Tauris.

CHINA INTERNET NETWORK INFORMATION CENTER. 2016. 中国互联网络发展状况统计报告 (Report of China’s Internet Development).

CHEN, LEI. 2015. 全球互联网治理 “中国方案”解读 (Interpret “Chinese solution” to global cyberspace governance), *法制日报(Legal Daily)*.

CHEN, QI. 2014. 网络安全、网络战争与国际法术——从《塔林手册》切入 (Cyber security, cyber war and international spells), *政治与法律 (Political Science and Law)* 7: 147-160.

CLOVER, CHARLES. 2016. “China: When Big Data Meets Big Brother.” *Financial Times*, January 19. Accessed January 30, 2017. Available online at http://www.ft.com/cms/s/0/b5b13a5e-b847-11e5-b151-8e15c9a029fb.html#axzz40G2n0kmE

COHEN, JEAN L. 2012. *Globalization and Sovereignty: Rethinking Legality, Legitimacy, and Constitutionalism*. Cambridge: Cambridge University Press.

CORNISH, PAUL. 2015. “Governing Cyberspace through Constructive Ambiguity.” *Survival* 57 (3): 153-176. Accessed on January 30, 2017. Available online at http://www.tandfonline.com/doi/abs/10.1080/00396338.2015.1046230

CUI, WENBO. 2013. 《塔林手册》对我国网络安全利益的影响 (The Influence on Chinese Cyber Security Interest of Tallinn Manual), *江南社会学院学报 (Journal of Jiangnan Social University)* 15 (3): 22-26.

DEIBERT, RONALD J. 2010. “The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace.” In *Routledge Handbook of Internet Politics*, edited by Andrew Chadwick and Philip N. Howard. London: Routledge. 323-336.

DEIBERT, RONALD J. 2015. “Cyberspace Under Siege.” *Journal of Democracy* 26 (3): 64-78. Accessed on January 30, 2017. Available online at https://muse.jhu.edu/article/586479

DEIBERT, RONALD J., JOHN G. PALFREY, RAFAL ROHOZINSKI, and JONATHAN ZITTRAIN, eds. 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: The MIT Press.

DEMCHAK, CHRIS, and PETER DOMBROWSKI. 2013. “Cyber Westphalia: Asserting State Prerogatives in Cyberspace.” *Georgetown Journal of International Affairs*, special issue, International Engagement on Cyber III: State Building on a New Frontier, 29-38.

Accessed on January 30, 2017. Available online at http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13003_Demchak-CYBER-III.pdf

DENARDIS, LAURA. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

DIAMOND, LARRY. 2010. “Liberation Technology.” *Journal of Democracy* 21 (3): 69-83. Accessed on January 30, 2017. Available online at https://muse.jhu.edu/article/385959/summary

DICKSON, BRUCE. 2011. “No ‘Jasmine’ for China.” *Current History* 110 (737): 211-216. Accessed on January 30, 2017. Available online at http://search.proquest.com/openview/018cd5e2ad4d49b5e43697fa528ec637/1?pq-origsite=gscholar&cbl=41559

DONG, BULIANG. 2015. 网络主权是个什么东西 (what is Internet Sovereignty?) blog post. Accessed on 30 January 2017. Available online at http://hk.on.cc/cn/bkn/cnt/commentary/20151220/bkncn-20151220000319783-1220_05411_001.html

DU, ZHICHAO, and YUXIA NAN. 2014. 网络主权与国家主权的关系探析 (Analysis of the relationship between Internet sovereignty and national sovereignty), *西南石油大学学报（社会科学版） Journal of Southwest Petroleum University（Social Sciences Edition）*16 (6): 79-84.

DUNN CAVELTY, MYRIAM. 2007. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon and New York: Routledge.

EBERT, HANNES, and TIM MAURER. 2013. “Contested Cyberspace and Rising Powers.” *Third World Quarterly* 34 (6): 1054-1074. Accessed on January 30, 2017. Available online at http://www.tandfonline.com/doi/abs/10.1080/01436597.2013.802502

FU, CHUANHENG. 2015. 习近平互联网大会剑指网络自由——一场注定要失败的战争 (Xi Jinping’s sword points to cyber freedom – a doomed war) blog post. Accessed on 1 February, 2017. Available online at http://blog.boxun.com/hero/201601/xinwenmingluntan/1_1.shtml

GAO, QIQI, and JIANLIN CHEN. 2016. 中美网络主权观念的认知差异及竞合关系 (Cognitive Differences and Competitive and Cooperative Relations in Understanding Internet Sovereignty between the US and China), *国际论坛 (International Forum)* 18 (5): 1-7.

GOURLEY, STEPHEN K. 2014. “Cyber Sovereignty.” In *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, edited by Panayotis A. Yannakogeorgos and Adam B. Lowther. Boca Raton, FL: Taylor and Francis. 277-290.

GREENWALD, GLENN, and EWAN MACASKILL. 2013. “NSA PRISM Program Taps In to User Data of Apple, Google and Others.” *The Guardian*, 7 June. Accessed on January 30, 2017. Available online at https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

GUO, QINGGUANG. 1999. *传播学教程 (Journalism & Communication)*, Beijing: Renmin University Press

GUO, YUJUN. 2010. *网络社会的国际法律问题研究 (Studies on international law in network society)*, Wuhan: Wuhan University Press

HAN, XIANYANG. 2016. 中国在互联网全球治理中发挥重要作用 (China plays an important role in global cyber governance), *光明日报 (Guangming Daily)*, 9 November. Accessed on 30 January 2017. Available online at http://news.gmw.cn/2016-11/09/content_22892833.htm

HAO, YELI. 2015, 大国网络战略博弈与中国网络强国战略 (Strategy Game of Cyber Power and China's Cyber Power Strategy), *国际关系研究 (Journal of International Relations)* 3: 3-15.

HELD, DAVID, ANTHONY MCGREW, DAVID GOLDBLATT and JONATHAN PERRATON. 1999. *Global Transformations: Politics, Economics, and Culture*. Stanford, CA: Stanford University Press.

HITCHENS, THERESA. 2014. Speech for High-Level Seminar "Cybersecurity: Global responses to a Global Challenge". 21 March, Madrid.

HUGHES, CHRISTOPHER, and GUDRUN WACKER, eds. 2003. *China and the Internet: Politics of the Digital Leap Forward*. London: Routledge.

INKSTER, NIGEL. 2015. *China's Cyber Power*. London: Routledge for the International Institute for Strategic Studies.

IRION, KRISTINA. 2012. "Government Cloud Computing and National Data Sovereignty." *Policy & Internet* 4 (3-4): 40-71. Accessed on January 30, 2017. Available online at http://onlinelibrary.wiley.com/wol1/doi/10.1002/poi3.10/full

JIANG, MIN. 2010. "Authoritarian Informationalism: China's Approach to Internet Sovereignty." *SAIS Review of International Affairs* 30 (2): 71-89. Accessed on January 30, 2017. Available online at https://muse.jhu.edu/article/403440

JOHNSON, DAVID R. and DAVID G. Post. 1997. "The Rise of Law on the Global Network." In *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, edited by Brian Kahin and Charles Nesson. Cambridge, MA: The MIT Press. 3-47.

KEOHANE, ROBERT O. 2002. "Ironies of Sovereignty: The European Union and the United States." *JCMS: Journal of Common Market Studies* 40 (4): 743-765. Accessed on January 30, 2017. Available online at http://onlinelibrary.wiley.com/doi/10.1111/1468-5965.00396/abstract

KESSLER, GLENN. 2016. "Cruz's Claim that ICANN's Transition Will Empower Foes to Censor the Internet." *The Washington Post*, 21 September. Accessed 26 January 2016. Available online at https://www.washingtonpost.com/news/fact-checker/wp/2016/09/21/cruzs-claim-that-icanns-transition-will-empower-foes-to-censor-the-internet

KING, GARY, JENNIFER PAN, and MARGARET E. ROBERTS. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107 (2): 326-343. Accessed January 30, 2017. Available online at https://doi.org/10.1017/S0003055413000014

KONG, XIAOWEI. 2000. 全球化进程中的信息主权 (Information Sovereignty in the process of globalization), *国际论坛 (International Forum)* 2 (5): 13-17.

KRASNER, STEPHEN D. 2001. "Abiding Sovereignty." *International Political Science Review* 22 (3): 229-251. Accessed on 26 January, 2017. Available at https://www.jstor.org/stable/1601484

LAO, LIU and XIAO XIANG.1998. 网络与国家主权 (Internet and national sovereignty), *资料通讯 (Information Communication)* 12.

LEAVITT, SANDRA R. 2012. "Problems in Collective Action." In *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, edited by Scott Jasper. Washington, DC: Georgetown University Press. 23-39

LI, DANDAN. 2016. 国家网信办：中方欢迎美国向 ICANN 移交管理权 (The National Internet Information Office: China welcomes the US' handover of management right to ICANN), *新京报(The Beijing News)*, 12 October. Accessed on January 30, 2017. Available online at http://www.bjnews.com.cn/news/2016/10/12/419563.html

LI, MINGTAO. 2015. 主张"互联网主权"的实质是。。。(the essence of asserting internet sovereignty is…), published on Wechat public account 七思而在 (qi si er zai)

LINDSAY, JON R., and DEREK S. REVERON. 2015. "The Rise of China and the Future of Cybersecurity." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron. New York: Oxford University Press. 333-352.

LIVINGSTON, SCOTT D. 2015. 'Beijing Touts "Cyber-Sovereignty" in Internet Governance.' *China File*, 19 February. Accessed on January 30, 2017. Available online at https://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-internet-governance

LIU, XIAOQIAN, and FUYANG CHANG. 2005. 信息时代的国家主权 (State Sovereignty in the Information Age), 江南社会学院学报 (Journal of Jiangnan Social University) 7 (3): 15-19.

LIU, YANGZI. 2012. 对国家网络主权的理解 (Understanding of national internet sovereignty), *中国信息安全(China's information security)* 11: 62-66.

LIU, YU, and DINGDING CHEN. 2012. "Why China Will Democratize" *The Washington Quarterly* 35 (1): 41-63. Accessed on January 30, 2016. Available online at http://dx.doi.org/10.1080/0163660X.2012.641918

LU, CHUANYIN. 2014. 主权概念的演进及其在网络时代面临的挑战 (The evolution of sovereignty and its challenges in the era of Internet), *国际关系研究 (Studies on International Relations)* 1.

LUKASIK, STEPHEN J. 2000. "Protecting the global information commons." *Telecommunications Policy* 24 (6-7): 519-531. Accessed 26 January, 2017. Available online at http://www.sciencedirect.com/science/article/pii/S0308596100000380

LYNCH, MARC. 2011. "After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State." *Perspectives on Politics* 9 (2): 301-310. Accessed on January 30, 2017. Available online at https://doi.org/10.1017/S1537592711000910

MACKINNON, REBECCA. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* New York: Basic Books.

Mearsheimer, John. 2014. "Can China Rise Peacefully?." *The National Interest*, 25 October. Accessed on January 30, 2017. Available online at http://nationalinterest.org/commentary/can-china-rise-peacefully-10204

MOROZOV, EVGENY. 2011. *The Net Delusion: How Not to Liberate the World*. New York: Public Affairs.

MUELLER, MILTON L. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

MUELLER, MILTON L. 2011. "China and Global Internet Governance: A Tiger by the Tail." In *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, edited by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA: The MIT Press. 177-194.

MUELLER, MILTON L. 2017. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge: Polity.

NOCETTI, JULIEN. 2015. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91 (1): 111-130. Accessed January 30, 2017. Available online at http://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12189/abstract

NOESSELT, NELE. 2014. "Microblogs and the Adaptation of the Chinese Party-State's Governance Strategy." *Governance* 27 (3): 449-468. Accessed on January 30, 2017. Available online at http://onlinelibrary.wiley.com/doi/10.1111/gove.12045/full

NORDIN, ASTRID, and LISA RICHAUD. 2014. "Subverting Official Language and Discourse in China? Type River Crab for Harmony." *China Information* 28 (1): 47-67. Accessed on January 30, 2017. Available online at http://journals.sagepub.com/doi/abs/10.1177/0920203X14524687

NYE, JOSEPH S., Jr. 2014. *The Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance Paper Series 1. Global Commission on Internet Governance: Waterloo, ON and Chatham House: London. Accessed on January 30, 2017. Available online at https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

PEOPLE'S DAILY. 2014. 弘扬传统友好 共谱合作新篇 (Full text of Xi Jinping's talk on "Carry forward traditional friendship and compose a new chapter of cooperation"), accessed on 30 January 2017. Available at http://news.xinhuanet.com/world/2014-07/17/c_1111665403.htm; English translation from Michael D. Swaine. 2014. "Xi Jinping's Trip to Latin America." *China Leadership Monitor* 45. Accessed on 14 July 2016. Available online at http://www.hoover.org/research/xi-jinpings-trip-latin-america

PIEKE, FRANK N. 2012. "The Communist Party and Social Management in China." *China Information* 26 (2): 149-165. Accessed on January 30, 2017. Available online at http://journals.sagepub.com/doi/abs/10.1177/0920203X12442864

PITT, DOUGLAS, NIALL LEVINE, and XU YAN. 1996. "Touching Stones to Cross the River: Evolving Telecommunication Policy Priorities in Contemporary China." *Journal of Contemporary China* 5 (13): 347-365. Accessed on January 30, 2017. Available online at http://www.tandfonline.com/doi/abs/10.1080/10670569608724259

POWERS, SHAWN M., and MICHAEL JABLONSKI. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana, Chicago and Springfield, IL: University of Illinois Press.

PU, XIAOYU. 2012. "Socialisation as a Two-Way Process: Emerging Powers and the Diffusion of International Norms." *The Chinese Journal of International Politics* 5 (4): 341-367. Accessed on January 30, 2017. Available online at https://academic.oup.com/cjip/article/5/4/341/394716/Socialisation-as-a-Two-way-Process-Emerging-Powers

RAMZY, AUSTIN. 2011. "State Stamps Out Small 'Jasmine' Protests in China." *Time*, 21 February. Accessed on January 30, 2017. Available online at http://content.time.com/time/world/article/0,8599,2052860,00.html

RANKIN, MARY BACKUS. 2002. "Nationalistic Contestation and Mobilization Politics: Practice and Rhetoric of Railway-Rights Recovery at the End of the Qing." *Modern China* 28 (3): 315-361. Accessed on January 30, 2017. Available online at https://www.jstor.org/stable/3181336

REIDENBERG, JOEL R. 1997. "Governing Networks and Rule-Making in Cyberspace." In *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, edited by Brian Kahin and Charles Nesson. Cambridge, MA: The MIT Press. 84-105.

REN, MINGYAN. 2007. 互联网背景下国家信息主权问题研究 (Studies on information sovereignty in the context of Internet), *河北法学 (Hebei Law Science)*, 25 (6): 71-74 & 94.

RÕIGAS, HENRY. 2015. "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?" Accessed on January 30, 2017. Available online at https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html

ROSENAU, JAMES and ERNST-OTTO CZEMPIEL. 1992. *Governance without Government: Order and Change in World Politics*. Cambridge University Press.

RUAN, LOTUS, JEFFREY KNOCKEL, JASON Q. NG, and MASASHI CRETE-NISHIHATA. 2016. "One App, Two Systems: How WeChat uses one censorship policy in

China and another internationally." Accessed on January 30, 2017. Available online at https://citizenlab.org/2016/11/wechat-china-censorship-one-app-two-systems/

SARAN, SAMIR. 2016. "Striving for an International Consensus on Cyber Security: Lessons from the 20th Century." *Global Policy* 7(1): 93-95. Accessed on January 27, 2017. Available online at http://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12317/full

SASSEN, SASKIA. 1996. *Losing Control? Sovereignty in the Age of Globalization*. New York: Columbia University Press.

SCHLÆGER, JESPER, and MIN JIANG. 2014. "Official Microblogging and Social Management by Local Governments in China." *China Information* 28 (2): 189-213. Accessed on January 30, 2017. Available online at http://journals.sagepub.com/doi/abs/10.1177/0920203X14533901

SCHMITT, MICHAEL N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

SHEN, YI. 2013. "GG2022 – Developing a Code of Conduct for Internet Governance." *Global Policy*, 5th December. Accessed on January 30, 2017. Available online at http://www.globalpolicyjournal.com/blog/05/12/2013/gg2022-%E2%80%93-developing-code-conduct-internet-governance

SHEN, YI. 2016. "Cyber Sovereignty and the Governance of Global Cyberspace." *Chinese Political Science Review* 1 (1): 81-93. Accessed on January 30, 2017. Available online at https://link.springer.com/article/10.1007/s41111-016-0002-6

SOUTH CHINA MORNING POST. 2013. "'I Am Like a Ghost Now', Says Censored Outspoken Scholar Zhang Lifan." 14 November. Accessed on January 30, 2017. Available online at http://www.scmp.com/news/china-insider/article/1355832/i-am-ghost-now-says-censored-outspoken-scholar-zhang-lifan

SOUTH CHINA MORNING POST. 2014. "Four Months After Prostitution Arrest, Influential Investor Charles Xue Remains Uncharged." 11 January. Accessed on January 30, 2017. Available online at http://www.scmp.com/news/china-insider/article/1403009/four-months-after-prostitution-arrest-influential-investor

STATE COUNCIL OF CHINA. 2016. 国家信息化发展战略纲要 (National Information Development Strategy Outline). Accessed on January 30, 2017. Available online at http://www.gov.cn/zhengce/2016-07/27/content_5095336.htm

STEVENS, TIM. 2012. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33 (1): 148-170. Accessed on January 30, 2017. Available online at http://www.tandfonline.com/doi/abs/10.1080/13523260.2012.659597

STEVENS, TIM. 2015a. "Roar of China's 'Great Cannon' Heard Across the Internet." *The Conversation*. 15 April. Accessed on 26 January, 2017. Available online at https://theconversation.com/roar-of-chinas-great-cannon-heard-across-the-internet-40201

STEVENS, TIM. 2015b. "BRICS Set Out Vision for International Information Security." *Thesigers*, 1 July. Accessed on January 30, 2017. Available online at http://thesigers.com/analysis/2015/7/3/brics-set-out-vision-for-international-information-security

STEVENS, TIM. 2016. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.

STEVENS, TIM. 2017. "Cyberweapons: An Emerging Global Governance Architecture." *Palgrave Communications* 3 (16102). Accessed on 26 January 2017. Available online at http://www.palgrave-journals.com/articles/palcomms2016102

STRANGE, SUSAN. 1996. *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge: Cambridge University Press.

SULLIVAN, JONATHAN. 2014. "China's Weibo: Is Faster Different?" *New Media & Society* 16 (1): 24-37. Accessed on January 30, 2017. Available online at http://journals.sagepub.com/doi/abs/10.1177/1461444812472966

TSAI, WEN-HSUAN, and NICOLA DEAN. 2013. "The CCP's Learning System: Thought Unification and Regime Adaptation." *China Journal* 69: 87-107. Accessed on January 30, 2017. Available online at http://www.journals.uchicago.edu/doi/abs/10.1086/668806

VAN EETEN, MICHEL J.G. and MILTON L. MUELLER. 2012. "Where is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720-736. Accessed on January 30, 2017. Available online at http://journals.sagepub.com/doi/abs/10.1177/1461444812462850

WALTON, GREG. 2001. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Montreal: International Centre for Human Rights and Democratic Development. Accessed on January 30, 2017. Available online at http://open.canada.ca/vl/en/doc/publications-421743

WANG, CHINGLUN. 2012. 倡导网络主权极其重要 (To promote Internet Sovereignty is extremely important), 光明日报 (Guangming Daily), 28 April. Accessed on January 30, 2017. Available online at http://epaper.gmw.cn/gmrb/html/2012-04/28/nw.D110000gmrb_20120428_2-03.htm

WANG, JUN. 2013. 筑牢网络边疆的防护墙 (To build a protective wall of Internet border), 中国国防报 (China National Defense News), 24 June.

WU, TIMOTHY S. 1997. "Cyberspace Sovereignty? The Internet and the International System." *Harvard Journal of Law and Technology* 10 (3): 647-666. Accessed on January 30, 2017. Available online at http://heinonline.org/HOL/Page?handle=hein.journals/hjlt10&id=657

XINHUA NEWS. 2015. 习近平在第二届世界互联网大会开幕式上的讲话 (Xi Jinping's talk in the second World Internet Conference). 16 December. Accessed on January 30, 2017. Available online at http://news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm

YAN, XU. 2002. "China's Accession to the WTO and Its Implications for Foreign Direct Investment in Chinese Telecommunications." *Communications and Strategies* **45**: 17-31

YANG, GUOBIN. 2009. *The Power of the Internet in China: Citizen Activism Online*. New York: Columbia University Press

YANG, ZEWEI. 2006. *主权论—国际法上的主权问题及其发展趋势研究 (Sovereignty: studies on the issue of sovereignty in international law and the development trends)*. Beijing: Peking University Press.

YANG, ZEWEI. 2012. *国际法析论 (Analysis of International Law)*. Beijing: Renmin University Press.

YAP, CHUIN-WEI, and GILLIAN WONG. 2015. "China Wants to Tap Big Data to Build a Bigger Brother." *The Wall Street Journal*, 6 November. Accessed on January 30, 2017. Available online at http://blogs.wsj.com/chinarealtime/index.php?p=28059&preview=true

YE, ZHENG. 2015. 网络主权已成为国家主权的全新制高点 (Internet Sovereignty has become the new commanding heights of national sovereignty), *中国青年报 (Newspaper of Chinese Youth*). Accessed on 14 July 2016. Available online at http://zqb.cyol.com/html/2015-07/10/nw.D110000zgqnb_20150710_4-09.htm

YE, ZHENG, and BAOXIAN ZHAO. 2014. 关于网络主权，网络边疆，网络国防的思考 (Thoughts on Internet Sovereignty, Internet Frontier and Internet Defense), *中国信息安全 (China's information security)* 1: 28-31.

YU, LI. 2012. 如何认识与维护互联网主权 (How to understand and protect Internet sovereignty), People's Daily, 2 February.

YU, MINGCAI, ed. 2003. 国际法专论 (Studies in International Law), Beijing: Citic Publishing House.

YU, TANFEI. 2015. 网络主权：一枚弱民弱国的护身符(Internet Sovereignty: An amulet of the weak state and the weak people). 20 December. Accessed on January 30, 2017. Available online at https://commondatastorage.googleapis.com/letscorp_archive/archives/99243

YUAN, YI. 2016a. 网络空间的国界在哪 (Where are the national border of cyberspace?)，*学习时报 (Study Times)*. 19 May. Accessed on January 30, 2017. Available online at http://www.studytimes.cn/zydx/KJJS/JUNSZL/2016-05-19/5690.html

YUAN, YI. 2016b. 如何为网络空间划分国界 (How to define national border in cyberspace?) *中国信息安全 (China Information Security)* 9: 28-29.

ZENG, JINGHAN. 2015. *The Chinese Communist Party's Capacity to Rule: Ideology, Legitimacy and Party Cohesion.* London: Palgrave Macmillan.

ZENG, JINGHAN. 2016a. "China's Date with Big Data: Will It Strengthen or Threaten Authoritarian Rule?" *International Affairs* 92 (6): 1443-1462. Accessed on January 30, 2017. Available online at http://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12750/full

ZENG, JINGHAN. 2016b. "Constructing a 'New Type of Great Power Relations': The State of Debate in China (1998-2014)." *British Journal of Politics and International Relations* 18 (2): 422-442. Accessed on January 30, 2017. Available online at http://journals.sagepub.com/doi/abs/10.1177/1369148115620991

ZENG, JINGHAN. 2017. “Does Europe Matter? The Role of Europe in Chinese Narratives of ‘One Belt One Road’ and ‘New Type of Great Power Relations’.” *JCMS: Journal of Common Market Studies,* forthcoming.

ZENG, JINGHAN, and SHAUN BRESLIN. 2016. “China’s ‘New Type of Great Power Relations’: a ‘G2’ with Chinese Characteristics?” *International Affairs* 92 (4): 773-794. Accessed on January 30, 2017. Available online at http://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12656/abstract

ZENG, JINGHAN, YUEFAN XIAO, and SHAUN BRESLIN. 2015. “Securing China’s Core Interests: The State of Debate in China.” *International Affairs* 91 (2): 245-266. Accessed on January 30, 2017. Available online at http://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12233/abstract

ZHANG, CHUNHOU. 2012. 全球化和互联网时代的国家主权、民族国家与网络殖民主义 (National sovereignty, nation-state and cyber colonialism in the era of globalization and Internet), 马克思主义与现实 (Marxism and Reality) 4: 32-41.

ZHANG, XINBAO and YAN REN. 2016. 网络主权的理论与网络空间法治 (The theory of Internet Sovereignty and rule of law in cyberspace), *法制日报 (Legal Daily)*, 28 September.

ZHENG, YONGNIAN. 2007. *Technological Empowerment: The Internet, State, and Society in China*. Stanford, CA: Stanford University Press.

ZHU, LIXIN. 2015. 聚焦《塔林手册》透视网络战规则 (Focusing on “Tallinn Manual”), *中国信息安全 (China’s information security)* 10.

Acknowledgements

We are grateful for the valuable feedback provided by five anonymous referees of *Politics and Policy*.