International Journal of Communication 12(2018), 3835–3855 1932–8036/20180005

The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda

SARAH MCKUNE
University of Toronto, Canada

SHAZEDA AHMED
University of California, Berkeley, USA

This article focuses on China as the state dedicating the most coordinated, strategic, and consistent efforts to promoting an Internet sovereignty agenda at home and abroad. At its core, the Chinese case for Internet sovereignty envisions the regime's absolute control over the digital experience of its population, with a focus on three dimensions: Internet governance, national defense, and internal influence. Through its guidance of the Shanghai Cooperation Organization and creation of the World Internet Conference, normative collaborations with Russia and other states, and promotion of Internet sovereignty as benefiting developing states in particular, the Chinese government is advocating for global recognition of the norm over the long term. Yet growing international support for Internet sovereignty could undermine multistakeholderism, transparency, accountability, and human rights, sparking new flash points in ongoing contestation over digital norms.

Keywords: Internet sovereignty, China, Russia, human rights, digital norms, legal norms, public opinion guidance, Shanghai Cooperation Organization, World Internet Conference

In current international debates about digital norms, the Chinese government has spearheaded legitimization and adoption of "Internet sovereignty." The Internet sovereignty concept attempts to align the potent international legal norm of state sovereignty with a key authoritarian priority: absolute control by the regime over the digital experience of its population. Such control depends heavily on "public opinion guidance" and the stamping out of digital influence that the regime considers destabilizing. In practice, Internet sovereignty is defined by state participation or intrusion into wide swathes of online activity—for example, online censorship, penalization of online dissent, or data localization requirements for foreign companies. To promote widespread diffusion of the norm, Beijing has characterized Internet sovereignty as a well-accepted premise that will better protect the digital interests of the developing world in particular.

This article examines the development of the Internet sovereignty concept over time, and the venues where the Chinese government has marshalled this concept to promote its core interests concerning Internet governance, national defense, and control of internal influence. We draw on norms literature to assess how Internet sovereignty has emerged as a relatively successful social norm, diffused in both

principle and practice through the regional Shanghai Cooperation Organization (SCO) and China's World Internet Conference (WIC). We argue that the Chinese government may also seek to characterize and diffuse Internet sovereignty as a legal norm, which could undermine international commitments to transparency, accountability, and human rights. We conclude that the many contradictions inherent in Internet sovereignty, as it exists in practice and discourse today, may ultimately limit its diffusion absent further refinement through ongoing norm contestation.

Methods

Our arguments about Chinese diffusion of digital authoritarian principles and their associated practices draw on discourse analysis of English and Chinese texts. We accessed the Internet sovereignty literature in Chinese through keyword searches for this term (网络主权, *wangluo zhuquan*, lit. "network sovereignty") in the China National Knowledge Infrastructure database and the Superstar (Chaoxing) database. The former is run by Tsinghua University and several Chinese government ministries related to science, media, and education, and the latter provides more extensive metrics on articles' readership, downloads, and citations within other Chinese texts. These are two of the most widely used academic databases for Chinese sources, both in China and internationally. We initially drew on more than twenty Chinese texts previously uncited or untranslated in English-language analyses to focus on how Chinese academics, military officials, and regulators have internalized the Internet sovereignty concept, settling on ten sources purposively sampled to capture views across these distinct domains.

Analysis of the SCO and China's international diplomacy surrounding Internet sovereignty relies on review of SCO normative documents; the official SCO and SCO Regional Anti-Terrorist Structure (RATS) websites; United Nations documents; reports by nongovernmental organizations (NGOs) such as Human Rights in China, Freedom House, and the Citizen Lab; and news reports.

Analysis of the World Internet Conferences at Wuzhen draws on domestic Chinese and foreign media coverage from the four years (2014–2017) that the conference has been held and proceedings and other documentation from the official conference website. We retrieved many non-Chinese sources by following Twitter hashtags such as #WuzhenSummit and those relevant to specific years of the conference—for example, #WIC2015.

Internet Sovereignty: Norm Emergence Around China's Digital Authoritarian Practices

Norms related to government use of information controls—including Internet filtering, content removal, and surveillance—have spread internationally, achieving varying levels of acceptance even among democracies (Deibert & Crete-Nishihata, 2012). At the same time, strong international resistance has emerged against conceding that the Internet, which began as an open commons, is the exclusive province of states; such resistance is often accompanied by insistence on a multistakeholder approach to Internet governance (Antonova, 2013). Mueller (2017) describes the concerns numerous stakeholders have raised around Internet fragmentation resulting from opposing approaches to Internet regulation and governance and governments' attempts to impose traditional notions of sovereignty and jurisdiction upon the digital space.

Within this tumultuous global atmosphere, the Chinese government has been a first mover with its own normative proposal of Internet sovereignty. Beijing has characterized Internet sovereignty as a nonthreatening premise by which to address the digital space—both an extension of the well-absorbed norm of state sovereignty and part of a "new model of international relations" that better represents the interests of the developing world (Ministry of Foreign Affairs of the People's Republic of China [MFA] & State Internet Information Office [SIIO], 2017). Although it is only within the past few years—arguably since the first World Internet Conference in 2014—that the concept has drawn significant attention from the wider international community (Bandurski, 2015b), the Chinese government has developed the policy positions enveloped within Internet sovereignty over a much lengthier span of time.

The Chinese Communist Party (CCP) leadership's concept of Internet sovereignty (also referred to as "cyber sovereignty" and, in earlier iterations, "information sovereignty") is a cornerstone of its overarching cybersecurity—and by extension, national security—strategy ("Xi Jinping Leads Internet Security Group," 2014). The Chinese government has outlined three major dimensions as falling within the scope of the Internet sovereignty concept: a *governance* dimension (e.g., states "must participate in international Internet governance on an equal footing"); a *national defense* dimension (e.g., states should not "engage in, condone or support cyber activities that undermine the national security of other states"); and an *internal influence* dimension (e.g., states have the "right to choose their own paths of cyber development, their models for Internet regulation and their public Internet policies" and should not "interfere in other States' internal affairs") (MFA & SIIO, 2017, p. 4).

President Xi Jinping emphasized "respect for cyber sovereignty" in December 2015 at the second World Internet Conference in Wuzhen, and has since then consistently deployed this term in numerous high-level speeches on the broader scope of state planning and international security issues. According to Xi, cyber sovereignty is violated when countries "pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security" (Xi, 2015, para. 10). Xi thus envisions Internet sovereignty as the absolute, exclusive right of the state to control its domestic Internet environment, and its citizens' interaction with that environment. Ye Zheng (2015), a scholar affiliated with the People's Liberation Army (PLA), China's military force, has also described the "the logic of Internet sovereignty as a starting point" for control of cyberspace. He noted that ceded

Internet sovereignty "will result in the loss of control over the guidance of online public opinion, sparking serious unrest and upheaval in society, directly challenging state power" (Bandurski, 2015a, para. 17), threatening the CCP's long-standing priority of public opinion guidance (Bandurski, 2013; ChinaFile, 2013; Wang, 2010).

Evolution of the Chinese Internet Sovereignty Concept Pre-2013

Although the rhetoric of Internet sovereignty has been most closely associated with Xi's tenure, the concept's core tenets circulated in Chinese academic and policy circles as far back as the 1990s (and possibly earlier), when the Internet first became popularized in the country. The CCP's state-centric approach to the Internet stems from long-standing concerns over regime control and domestic stability, both of which information flows deeply affect (McKune, 2015b). This view was not limited to China: Mueller (2017) notes that the related concept of "data sovereignty" gained traction in 2001 when many countries balked at extraterritorial data acquisition privileges the USA PATRIOT Act granted the U.S. government, and again in response to the global expansion of cloud computing in the late 2000s.

In a prescient article from 2000, "Network Security, Sovereignty, and Innovation," top-flight engineer Ji Zhaojun (2000) raised concerns that have since become hallmarks of the current Chinese case for cyber sovereignty: comparison of Internet sovereignty to sovereignty over national airspace and maritime space, the need to raise domestic awareness of Internet sovereignty, the fragility of open global networks running on the U.S.-created TCP/IP protocol, and "resolution of network security and innovation problems from the Internet sovereignty perspective" (p. 20).

Further rooting digital interaction in its material forms, Chen Xueshi (2004) of the PLA-affiliated National University of Defense Technology defined national "information borders" as "the national security-relevant virtual space (and corresponding physical carriers) stored on electronic devices used by a state's infrastructure systems, government, and extra-governmental institutions and individuals" (p. 20). This early definition has not changed substantially in the ensuing decade-plus.

In Beijing's arguments for global acceptance of Internet sovereignty, the concept's consistency is used to assert its legitimacy. A source government officials and scholars alike often provide as evidence that the Chinese government has consistently valued this principle is the 2010 white paper, "The State of China's Internet." In the "Protecting Internet Security" section, this document regarded the Internet as a component of China's infrastructure and stated that the Internet within Chinese borders belonged under PRC sovereignty and jurisdiction (Ye, 2015), crystallizing the leadership's linkage of security, sovereignty, and information controls.

Since 2010, the definitional scope of cyber borders in China has grown to include "Internet infrastructure, wireless technology facilities, and cloud computing infrastructure" (Liu, 2012, p. 65) and the "Chinese Internet's domain names and related public services" (Ye, 2015, p. 29), including the claim that "the financial, telecommunications, transportation, energy, and other . . . core national networked systems, should all be seen as forming a state's national Internet borders" (Liu, 2012, p. 65). There is no definitive,

government-issued statement on the precise parameters of China's cyber borders, yet these explications provide a sense of what might be expected from such a definition.

Post-2013 Shifts in China's Internet Sovereignty Strategy

Mueller (2017) points out that international debates over Internet sovereignty predate Edward Snowden's 2013 revelations about the U.S. National Security Agency's global espionage campaigns—an observation the Chinese literature supports. Post-2013, Chinese writings about Internet sovereignty proliferated, with a focus on how to defend cyber borders. In an article on Internet sovereignty for the journal *China Information Security*, PLA-affiliated authors Ye Zheng and Zhao Baoxian (2014) propose that,

> [Having] grasped the reality that cyber hegemons are more reliant on information networks, and more afraid of their destruction, [we must] develop attack-centered cyber combat measures, and use independently created technology to shape our real combat capabilities. [We have to] use asymmetrical search and destroy policies against enemies [寻求破敌], and build all-new, normalized cyber attack capabilities. (p. 31)

Ye (2015) has also advocated for Chinese citizens to band together while the state

> lead[s] the people to recognize that it is necessary to defend the sovereignty of the state's land, sea, sky, space, and cyberspace . . . as well as to fight a battle for all citizens' defense of Internet sovereignty in the information age. (p. 29)

From the inception of the information sovereignty principle, ideological arguments for its enforcement stemmed from a fear that information transmitted into China from outside its borders would corrode regime stability, whether by chance or by design. A more recent concern is that a lack of control over China's Internet users via highly coordinated online censorship could lead to an outcome similar to the Arab Spring, which some Chinese critics consider a case of ceded Internet sovereignty (Ye & Zhao, 2014). Casting further into the past, another commentator cited the collapse of the Soviet Union as indicative of the loss of control over information within state borders (Ran, 2017). Regime stability is clearly at the forefront of the Internet sovereignty agenda, and it is the most appealing promise of this norm for authoritarian developing states.

Beijing's extraterritorialization of the Internet sovereignty principle is meant to normalize its associated policies. Pre-2013, the Chinese view of Internet sovereignty lacked its current urgency and international character. Mueller (2017) argues that rather than simply fragmenting Internet governance, China instead practices *alignment*: incentivizing other countries to internalize and adopt a model of Internet governance that "re-align[s] control of communications with the jurisdictional boundaries of national states" (pp. 18–19).

Chinese supporters of Internet sovereignty argue that because the United States and Europe were the first to establish and regulate core Internet infrastructure, both these physical systems and power over their use are concentrated in wealthy democracies even though the majority of global Internet users are

from developing countries. The biggest shift in thinking about Internet sovereignty between the 1990s and the post-2013 Chinese literature on the subject marks the emergence of an alignment strategy: the argument that China should combine forces with developing nations around the world to gain international respect for Internet sovereignty and its concomitant digital authoritarian practices—a foundational goal of China's annual World Internet Conference. Some arguments for proportionate representation are much-needed, such as initiatives for more global Internet infrastructure to be built in places with higher concentrations of new Internet users. Yet these ambitions are overshadowed by many of these states' censorship and criminalization of online activism or, more recently, data localization practices that enable local law enforcement to access domestic users' personal data even when hosted by foreign companies. Similar strategies extend to international human rights law, which has not shifted policies within China but which instead the Chinese government is subtly altering.

Contestation and Diffusion of the Internet Sovereignty Agenda

Literature on international norms elucidates patterns of norm emergence, contestation, and diffusion that are helpful for understanding Internet sovereignty's normative evolution. Finnemore and Sikkink (1998) lay out the life cycle of a norm in three stages: *norm emergence* through the efforts of a "norm entrepreneur;" *norm cascade*, when "more countries begin to adopt new norms more rapidly even without domestic pressure for such change" (p. 902); and *norm internalization*, when a norm becomes widely accepted and is viewed as noncontroversial. "No matter how a norm arises, it must take on an aura of legitimacy before it can be considered a norm" (Florini, 1996, p. 365). As more recent literature recognizes, however, "the content of norms is far from static or singular, but rather subject to ongoing contestation" (Krook & True, 2010, p. 110). Such contestation could weaken *or* strengthen a norm over time (Deitelhoff & Zimmermann, 2013, pp. 4–5).

The Chinese government, as the primary norm entrepreneur of Internet sovereignty, has long sought international legitimization of the concept to justify its domestic agenda. After years of Beijing promoting Internet sovereignty, the concept is now widely discussed, though its legitimacy is still critically questioned in international debates. As such, Internet sovereignty is in the norm emergence phase. The content and language of Internet sovereignty has evolved much over the past two decades, reflecting ongoing contestation among states' digital policy prerogatives. Krook and True (2010) describe how norms are dynamic and "may encompass different meanings, fit in with a variety of contexts, and be subject to framing by diverse actors"—actually facilitating diffusion (pp. 104–105). Ben-Josef Hirsch (2014) similarly notes that "norm emergence is a dynamic process in which ideas, practices, and consensus change significantly" (p. 825). Internet sovereignty shows such dynamism, adapting to the evolving objectives and interests of those states that assert it and to shifts in the geopolitical arena that major digital conflicts frequently trigger.

It is no surprise that Internet sovereignty has gained traction alongside China's increasing global prominence and economic clout. Norm contestation is a natural result of rising powers' interest in challenging inadequate representation in international forums and normative content established by prior hegemons (Newman & Zala, 2017). Indeed, China, purportedly speaking on behalf of the developing world, has highlighted insufficient non-Western representation in Internet governance, the dangers of the United States

as an unchallenged "cyber hegemon," and the inapplicability of "Western values" in Internet sovereignty discourse. Beijing has sought to increase its influence in international forums by advancing the Internet sovereignty model as the polar opposite of "Internet freedom," which many governments link to the Arab Spring and efforts at regime change.

In such a contestation scenario, the norm "selected will depend on three factors . . . the relative prominence of each of the contested norms, their relative compatibility or coherence with other prevailing norms, and the extent to which they fit the existing environmental conditions" (Florini, 1996, p. 378). In that sense, the SCO has been crucial to the incubation and strengthening of the Internet sovereignty norm. At the regional level, among SCO members, Internet sovereignty enjoyed the prominence, coherence, and environmental conditions initially absent on the wider international stage. Even so, given the dynamic nature of norms, the ability "to predict which international norms will emerge and which will not survive is limited" (Ben-Josef Hirsch, 2014, p. 825). Normative progress attained thus far, however, suggests that the discourse of Internet sovereignty has staying power in the international community.

The SCO has served as a first staging ground in the norm elaboration and diffusion process, which originally coalesced around "information security." Following the vigorous contestation of norms of information security at the international level, however, it may be that the Chinese government has turned to its Wuzhen Process for a new articulation based on Internet sovereignty.

Through the Shanghai Cooperation Organization

The Shanghai Cooperation Organization, which China and Russia spearhead, is perhaps one of the most successful examples of multilateral embrace of digital authoritarian norms and practices. The original membership roster of the SCO, established in 2001, consisted of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. In June 2017, India and Pakistan joined the SCO as full members. Since its establishment, this regional body has slowly and steadily built up its normative framework and international influence, primarily focusing on security by "combating terrorism, separatism, and extremism" (the "three evils") and on the creation of "a democratic, fair and rational new international political and economic order" (Shanghai Cooperation Organization [SCO], 2001, para. 2)—a significant foray by China into multilateral norm-setting. SCO member state cooperation has coalesced largely around shared interest in maintaining regime stability in the face of feared "color revolutions" and interference from "foreign hostile forces." Security cooperation within the SCO has raised human rights concerns, given the founding member states' propensity to identify ethnic groups and political opposition as security threats combined with the policy harmonization and extradition cooperation that is streamlined through the SCO framework (Human Rights in China [HRIC], 2011). Normative and practical cooperation includes both elements that are specific to the digital space, as well as a broader security apparatus covering the "three evils" that likewise applies to their digital manifestations.

The digital aspects of SCO member state cooperation follow similar patterns in crystallizing member state consensus—here, regarding notions of information security (led by Russia) and Internet sovereignty (led by China)—and extending practical cooperation and policy around such consensus. The SCO's approach to regional security came to include a strong digital component by 2009, when the member states adopted

an Agreement on Cooperation in the Field of International Information Security. That agreement, among others, drew heavily on well-established Russian precedent (McKune, 2015a) and elaborated "main threats" and "main areas of cooperation" (SCO, 2009). More recently, under the 2017 Convention on Countering Extremism, each member state committed to "monitoring the media and the Internet for timely detection and suppression of the spread of extremist ideology" and restricting online access to materials deemed extremist (SCO, 2017).

The Regional Anti-Terrorist Structure, the SCO's operational unit devoted to combating the three evils, has taken steps to mobilize such cooperation, illustrating diffusion of authoritarian practices. Member states have indicated they work together to prevent the use of the Internet to propagate "terrorist, extremist, or separatist" ideologies. RATS maintains its own database of information related to such threats as well as a Unified Investigative Register containing details on people and entities suspected of these acts. Each member state's law enforcement agencies may access or submit information to these databases, potentially duplicating and elevating any due process shortcomings. The same data may possibly be employed in censorship or surveillance efforts.

RATS has also coordinated two SCO Anti-Cyberterror Exercises in Xiamen, China. Reflecting member states' preoccupation with internal influence via digital mediums, the inaugural exercise in 2015 simulated the dissemination of "information inciting terrorism, separatism, and extremism on websites, forums, and social networks within SCO member states, [which] caused extremists hiding out in these SCO member states to launch terrorist attacks" (China Information Security, 2015, p. 70). SCO member state authorities cooperated to locate "the terrorist organizations' instigatory information on websites and social communication platforms," and "discovered information about the posters' identities and locations, arrested them, and finally eliminated the terrorist threat" (China Information Security, 2015, p. 70).

RATS held the second such exercise in December 2017. This time the participants were joined by new member states India and Pakistan (Meng, 2017; "SCO Countries Hold Drill," 2017). The exercise involved a coordinated response to "terrorist groups us[ing] the Internet and social networks to spread terrorism, separatism, and extremism" and "trying to recruit members from the SCO countries" (Meng, 2017, para. 2). Notably, RATS also used technology offered by Chinese digital forensics company Meiya Pico (2018) during the joint exercise. The company indicates that it has provided training (offered with Russian translation) in all six of the original SCO member states. Thus, in what amounts to diffusion by practice of priorities, capabilities, and techniques, SCO member states are normalizing their cooperation regarding targeted online content and discovery of those responsible for that content. The SCO and RATS within it are seeding the field, integrating Chinese prerogatives and even technology within member states' security cooperation.

With regional security mechanisms in place and functional, the SCO has also served as a platform to disseminate member states' digital norms to the international community. SCO member states twice submitted for debate at the United Nations General Assembly an International Code of Conduct for Information Security, once in 2011 and again in 2015 (McKune, 2015a). This effort to create consensus around preferred digital norms reiterated core principles of Internet sovereignty and information security. In March 2017, China built on this effort by proposing an International Cyberspace Cooperation Strategy to

the United Nations Conference on Disarmament, highlighting its predecessor codes proposed by the SCO (MFA & SIIO, 2017). The strategy noted: "We have now seen interference in other countries' internal affairs through the malicious use of ICT and we have seen cybersurveillance activities on a massive scale" (p. 3).

The evolution of China's normative approach, from a reliance on the Russian notion of information security to its own language around Internet sovereignty, is consistent with Ben-Josef Hirsch's (2014) elaboration of "ideational change," which describes

> how the process of norm promotion is actually prompted and preceded by a process of ideational contestation, debate, and discussion that refines and selects the ideas that are associated with the norm's practice, which ultimately come to define an international norm. (p. 813)

The SCO forum and RATS have played an important role in the iterative process of norm emergence in furtherance of regime control: they have facilitated information exchange and comparison of experiences as well as practical law enforcement cooperation. Successful approaches have been adopted, advanced, and refined regionally and internationally. One can appreciate the extent to which the most influential member states—China and Russia—have informed and emboldened each other when comparing information control tactics, some of which were quite novel in their original conception (see Table 1).

The SCO and its patron states China and Russia have effectively carried the water in advancing digital authoritarian norms and practices on the international stage. Yet there are contradictions below the SCO's veneer of harmonization. On the one hand, the SCO has had two key impacts: (a) diffusing security imperatives and concrete modes of cooperation to SCO states, thereby creating a bulwark for regime preservation; and (b) advancing legitimation of SCO norms as a new world order in international diplomacy, regionally as well as at the UN and other international bodies, to reduce criticism and generate acceptance—if not outright imitation—of domestic policies. The fact that India, often touted as "the world's largest democracy" (though recognized as flawed in a number of respects) has now joined the SCO, demonstrates the significant potential for diffusion of authoritarian norms and practices.

On the other hand, in practice, SCO member states ignore notions of sovereignty and noninterference in the digital space when it suits them. For example, China is known to conduct pervasive digital intrusion and espionage against extraterritorial targets, including not only state actors but also the Chinese diaspora, civil society entities, media outlets, and others beyond its borders (Citizen Lab, 2014; McKune, 2015b). Researchers have uncovered China's use of an offensive weapon, co-located with the Great Firewall, to insert malicious content in unencrypted Web traffic to overseas users (Marczak et al., 2015). Moreover, within the broader SCO membership, Russian demands for noninterference in internal affairs strain credulity following its 2016 U.S. election-related operations. Finally, some evidence has emerged suggesting the SCO member states even target *each other* in digital operations (Falcone & Miller-Osborn, 2016; Margolin, 2016; Ray & Falcone, 2016), in contravention of SCO agreements.

Table 1. Trendsetters? Digital Authoritarian Developments in China and Russia.

Digital authoritarian practice	China	Russia
Data localization	Articles 37 and 66 of Cybersecurity Law (June 2017)	Amendments to On Personal Data Law (Federal Laws No. 242-FZ and No. 526-FZ) (September 2015)
Restrictions on VPNs	Ministry of Industry and Information Technology directive to restrict VPN access (July 2017)	Amendments to Information, Information Technology, and Protection of Information Law (Federal Law No. 276-FZ) (November 2017)
Penalties for reposting targeted content	Major domestic media outlets banned from reposting content (2017)	Anti-Extremism Law (2002, with subsequent amendments and additions)
Real-name registration requirements	Article 24 of Cybersecurity Law (June 2017)	Bloggers Law (August 2014); Amendments to Information, Information Technology, and Protection of Information Law (Federal Law No. 241-FZ) (January 2018)
Restrictions on encryption	Article 18 of Counter-Terrorism Law (requiring telecoms and ISPs provide decryption services to assist public and state security in investigating suspected terrorist activities) (January 2016)	Amendments to Anti-Terrorism Law (Federal Law No. 374-FZ) (July 2016) Blocking Telegram encrypted messaging app (April 2018)
Strategic censorship of content deemed threatening to regime	Great Firewall (ongoing development since arrival of Internet in China)	Internet blacklisting coordinated through Roskomnadzor [Federal Service for Supervision of Communications, Information Technology and Mass Media] (launched with passage of 2012 Internet Restriction bill, Federal Law No. 139-FZ)

Through the Wuzhen Process

A second site through which the CCP attempts to diffuse its digital authoritarian practices and alignment strategy is through annual meetings of the World Internet Conference held in Wuzhen, China, since 2014. Convening world leaders, Internet operations figures from the Internet Corporation for Assigned Names and Numbers (ICANN), and the Asia-Pacific National Network Information Centre, top executives from technology firms—including Facebook, Amazon, Google, Apple, Alibaba, and Tencent—and members of think tank and research communities, the WIC showcases the homegrown Chinese tech industry while promoting Internet sovereignty and multilateralism. The WIC's reach is far less pervasive than the SCO's, though the latter set the stage for the increasingly ostentatious WIC by encouraging SCO member states to attend in the hopes of gaining access to companies that may invest in their information technology sectors. All four iterations of the WIC, also called the Wuzhen Summit, have demonstrated the double standards and lack of accountability that have come to typify China's digital authoritarian practices.

Chinese media has portrayed the WIC meetings as representative of a broad international consensus on the direction global Internet regulation should take, which both their outcomes and actual proceedings do not reflect. Nevertheless, Chinese news media regarded the second WIC (December 2015) as a successful instance in which Xi Jinping publicly advocated for Internet sovereignty. His speech on the subject was domestically heralded as "having launched the 'Wuzhen Process' . . . This will be one of China's most important contributions to the world, and marks a major step in the forward march of transforming the global order of cyberspace governance" (Shen, 2015, para. 16). Specifically, former Chinese head of the Cyberspace Administration of China, Lu Wei, cited Xi Jinping's "four principles and five points" as foundational to the Wuzhen Process of reforming Internet governance, including the principle of "respect for Internet sovereignty" (Lu, 2016).

An egregious violation of the Wuzhen Process's own claims of "openness and cooperation" is its creation of a small locus of Internet connectivity that skirts the Great Firewall: foreign participants at all of the Wuzhen conferences could access websites that are blocked in China, while domestic Chinese journalists have not been allowed into the spaces where these Web browsing restrictions were lifted (Horwitz, 2017). Nested within this unblocked zone, however, at least one noteworthy act of censorship transpired.

At the second Wuzhen Summit, Wikipedia founder Jimmy Wales gave an address that was altered in its Chinese translation on the official WIC website. Wales's original comment, "the idea that any one government can control the flow of information of what people know in their territory will become completely antiquated and no longer possible," was translated as "Probably we will see improved machine translation, which will very much enhance person-to-person communication. And also the government could conduct good analysis on people's communication in various relevant areas" (Areddy, 2015, paras. 6–8). Both incidents typify Beijing's lack of accountability in upholding its own purported Internet agenda at home.

Although it was remarkable that Wales and other high-level representatives of online platforms that are blocked in China attended the Wuzhen conferences, some critics have focused on where world leaders who attended the conference come from as indicative of where China's global influence over Internet governance is growing. Seven heads of state attended the 2015 WIC; all hailed from Central and South

Asian countries that stand to benefit from China's One Belt, One Road infrastructure-building investments projects, which include the laying of fiber-optic networks for high-speed Internet connectivity (Timmons, 2015). Six of these states are SCO members and share practices of online censorship similar to China's. While international headlines about the 2017 WIC focused on the attendance of Apple's and Google's CEOs, a major story in the shadows of the summit involved efforts to address developing countries' concerns about Internet infrastructure buildout, poverty alleviation, and closing the digital divide (Ahmed, 2017).

The Wuzhen Process has yet to take off internationally, however, and continues to remain so ill-defined that at least one WIC participant has even characterized it as inching toward multistakeholderism. Writing about the 2016 WIC, Bruce McConnell (2017) of the EastWest Institute noted that Fadi Chehadé, a member of the WIC advisory committee and former ICANN CEO, regarded the committee's closing statement as "a model of [the] participatory process." McConnell highlights the statement's emphasis that "Governments, international organizations, Internet companies, technology communities, civil organizations, academia, and individuals will all take positive actions to safeguard and promote deepening pragmatic cooperation on building the Internet shared and governed by all" (para. 9). At none of the Wuzhen Summits have "civil organizations" partaken in the mostly consultatory role that nongovernment actors such as tech company executives play. Some critics may argue that this exclusion of civil society actors does not differ from how multistakeholder Internet governance has operated since the 1990s (Carr, 2015). It is unsurprising that in China, too, the only efforts domestic NGOs are invited to participate in serve commercial ends, such as the Internet Plus Alliance Alibaba's founder chaired at the 2016 WIC.

As one representative of digital rights NGO Access Now noted on Twitter, it may not be a coincidence that the 2015 WIC was held on the same dates as the 10th meeting of the World Summit on the Information Society. Part diplomatic theater and part high-tech expo, the Wuzhen Summit aims to distract attention away from efforts to secure multistakeholder Internet governance by juxtaposing access to Chinese technology markets, firms, and outbound investment with tacit agreements to replicate the state's Internet governance goals outside its borders.

Assessing Internet Sovereignty From an International Legal Perspective

China has for many years been a staunch proponent of both sovereignty—with particular attention paid to territorial integrity and noninterference in internal affairs—and Internet sovereignty. It has treated the two as intertwined, arguing that Internet sovereignty flows from the nature of sovereignty itself. A deeper dive into the relevance and meaning of the Internet sovereignty concept to the Chinese government is essential to understanding its prospects for diffusion and wider impact. Do the Chinese government and other states consider Internet sovereignty a *social norm*—that is, a voluntary, nonbinding standard of appropriate behavior (with China and Russia as the standard bearers for the developing world)? Or do they see Internet sovereignty as a *legal norm*, rooted in international law and reflecting existing rights and responsibilities of states (thus opening the door to legal consequences for breaches resulting in internationally wrongful acts)? While additional research may clarify these questions further over time, Chinese government and academic rhetoric in domestic and international forums suggests the stronger view that Internet sovereignty amounts to a legal norm based on international law.

Scholars have noted the tendency to confuse the language of legal and social norms in discussions around cybersecurity and governance (Schmitt & Vihul, 2014, pp. 4, 6–9; Tikk & Kerttunen, 2017, pp. 24–27). Conflation of the two may only be natural: Brunnée and Toope (2010) recognize that both social norms and legal norms concern shared social understandings. However, they enumerate additional "criteria of legality" that distinguish legal norms, including (among others) generality, promulgation, clarity, noncontradiction, and constancy over time (p. 206).

While Brunnée and Toope (2010) highlight the interaction between social and legal norms, they clarify that "legal norms arise when shared normative understandings evolve to meet the criteria of legality, and become embedded in a practice of legality" (p. 203). This may take the form of customary international law or treaty law. The benefits of establishing a legal norm through the process of normative contestation reside largely in state perception of their "bindingness," because the "normative power of contestation is ambivalent as long as it cannot be channeled into institutions that bind applicatory discourses to the normative system. Legalizing a norm is a strategy to allow for such an institutionalization" (Deitelhoff & Zimmermann, 2013, p. 9).

Invocation of international law underpins Chinese government engagement on Internet sovereignty issues in international forums. The governments of China and Russia—and the SCO on their behalf—"treat state sovereignty as the defining principle of international law" (Roberts, 2017, p. 292). This approach is apparent in official international policy pronouncements by one or both states dating back for many years, including the Five Principles of Peaceful Coexistence (China, 1953), the Declaration on the Establishment of the SCO (2001, para. 5), the SCO Charter (2002, Art. 2), the Russia-China Joint Declaration (2002), both versions of the International Code of Conduct for Information Security (2011, 2015), the Russia-China Joint Declaration on the Promotion of International Law (2016), and the International Cyberspace Cooperation Strategy (China, 2017). It is therefore unsurprising that China has staked the legitimacy of its digital control apparatus on sovereignty as an incontrovertible legal principle. Characterizing Internet sovereignty as a valid legal norm is a way for the Chinese government to (a) advance its own interpretation of international law while challenging Western hegemony; (b) shield its actions and policies from rights-based criticism; and (c) build pressure against the activities of others that it views as contrary to Internet sovereignty.

As previously noted, the Chinese government's articulation and practice of Internet sovereignty encompass a governance dimension, a national defense dimension, and an internal influence dimension. Yet despite official insistence that Internet sovereignty is rooted in the legal concept of state sovereignty, the internal influence dimension does not appear to adequately exhibit the criteria of legality. It does not meet the requirements of generality, accessibility, clarity, noncontradiction, and constancy over time: Internet sovereignty is too amorphous to define and alert the international community and domestic audiences to the full scope of behavior that violates the norm, leaving interpretation of what constitutes interference with internal affairs entirely to government discretion. Indeed, the Chinese government's public opinion guidance initiatives necessarily fluctuate in response to world events and evolving public narratives. When a norm "maintains space for political assessments," the legality of the norm is weakened "as regards the requirements of generality, clarity and constancy over time" (Brunnée & Toope, 2010, p. 208).

Linking the Internet sovereignty norm to state sovereignty does not cure such shortcomings. In their case study of the emergent "responsibility to protect" norm, Brunnée and Toope (2010) describe how linking the norm to existing legal categories (those of international crime and state responsibility) "ensures the norm's consistency with established international law . . . thereby addressing the requirements of non-contradiction and constancy over time" (p. 206). That "the responsibility to protect concept makes explicit what international law already requires" (p. 207) enhanced its potential to achieve the status of a legal norm.

In the case of Internet sovereignty, however, the opposite is true: international law pertaining to nonintervention in internal affairs, an integral aspect of state sovereignty, contradicts the Chinese government's approach. The perceived threat of internal influence by digital means does not meet international legal standards pertinent to nonintervention. The International Court of Justice (1986), in the case of *Nicaragua v. U.S.*, articulated wrongful intervention as follows:

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. (p. 108)

As the court made clear, coercion by another state is a critical element in identifying a prohibited intervention.

The Chinese government has conveyed its views that the forms of influence made possible through digital mediums intrude on the government's own choices in the political, economic, social, and cultural spheres, and thus amount to interference in its internal affairs. It has referred to the actors behind such influence as "Western anti-China forces," linked them with domestic social movements, and stressed the government imperative of public opinion guidance and ideological control (ChinaFile, 2013)—an approach consistent with threats identified in the SCO Agreement on Information Security and with SCO practice.[1]

Under international law, however, prohibited interventions concern the activities of states rather than private, nonstate actors. Beyond hostile states, protagonists of concern to the Chinese government on the influence front include ICT companies (which Beijing sees as vectors of home state ideologies), journalists, NGOs, foundations, and activists. Not coincidentally, targeted entities closely reflect the composition typically associated with "transnational advocacy networks," which rely heavily on information exchange to promote rights (Keck & Sikkink, 1999, pp. 91–93). The government has targeted these entities with censorship, digital surveillance, foreign funding laws, and other intense regulatory scrutiny and

[1] In elaborating the threat of "dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States," the agreement identifies this threat as emanating "from states, organizations, groups of people or individuals that use the information infrastructure to disseminate [harmful] information" (SCO, 2009, Annex 2, para. 5).

restrictions. As a matter of international law, however, the activity of nonstate transnational advocacy networks does not amount to prohibited intervention (Cassese, 2005, pp. 53–54; Kunig, 2008, para. 8). It is only when activities are attributable to a state itself—for example, when state "organs have co-operated with these entities" (Kunig, 2008, para. 8)—that the activities could be evaluated as potential prohibited interventions. Issues such as U.S. government support for Internet freedom initiatives, or the projection of soft power through media, tech companies, and other entities, may raise questions concerning the extent to which a transnational advocacy network or its participants operates on a state's behalf. A clear and fact-specific nexus would need to exist, however, to credibly assert that these entities' activities are attributable to a state; the blanket approach to non-regime influence adopted within the Internet sovereignty norm is outside the letter of international law on this count.

Moreover, the influence of primary concern within the Internet sovereignty agenda does not amount to coercion under international law. Coercion is "more than mere influence. It involves undertaking measures that deprive the target State of choice" (Schmitt, 2017, p. 8). Online activities targeted by Internet sovereignty thus must exceed standard manifestations of digital influence to qualify as coercion. While subversive propaganda that "aim[s] to foment revolt or civil strife in another State or [is] devoted to assisting illegal and violent activities" may amount to coercion (Kunig, 2008, para. 24), a far wider range of content and activities is restricted on the basis of Internet sovereignty, including expression on historical events or news of public interest. "Not prohibited by the non-intervention principle is criticism of the internal politics of another State, if this criticism is substantiated by facts" (Kunig, 2008, para. 24).

Perhaps most importantly, Internet sovereignty also fundamentally contradicts established international human rights law. It is well understood that China and Russia have subordinated human rights law to principles of sovereignty in their engagement with the international legal framework (Roberts, 2017, pp. 291–293). Even so, the incompatibility of Internet sovereignty and international human rights law requires explicit discussion and understanding, particularly given that the rhetoric employed in promoting the Internet sovereignty concept frequently makes casual but inaccurate, incomplete, or unsubstantiated reference to human rights. As Schmitt and Vihul (2014) elaborate, should states accept an understanding of human rights law "as inconsistent with their need to ensure, for instance, the security of their cyber systems, they may begin to act contrary to the [human rights] norm." Such state practice may, over time, "be viewed by states as legal, such that the original human rights norm will have been modified. Given the novelty of cyber activities, they are particularly vulnerable to this dynamic of customary law" (p. 5).

Not least among such threatened norms is the right to freedom of opinion, which, under international human rights law, is considered an absolute right. This "right to hold opinions without interference also includes the right to form opinions" (Kaye, 2015, p. 8). Internet sovereignty, with its emphasis on "public opinion guidance" online, suggests de facto interference in the right to form opinions.

The Chinese government has gauged the receptivity of the international community to Internet sovereignty by characterizing it as an international legal norm. This tactical approach is evinced by China's hitching of its digital agenda to the notion of sovereignty itself—a notable change from the previous normative discourse around information security. The Chinese government has not masked its intentions; as stated plainly in its International Cyberspace Cooperation Strategy, "China is committed to ensuring

peace and security in cyberspace and, *on the basis of State sovereignty*, establishing a just and coherent international cyberspace order. *It has worked actively to advocate for and build international consensus on this question*" (MFA & SIIO, 2017, p. 6; emphasis added). Successful diffusion of Internet sovereignty as an international legal norm, however, may ultimately depend precisely on its coherence with international law and sovereignty principles.

Conclusion

China has engaged in coordinated, strategic, and consistent efforts to promote an Internet sovereignty agenda at home and abroad. This article has assessed the emergence of Internet sovereignty as an international norm and detailed China's relative success in winning adherents to its normative agenda. The Internet sovereignty concept is of critical significance to the CCP as it advances legitimization of regime control over the digital experience of a population by linking such control to accepted norms of state sovereignty and multilateralism. Core dimensions of China's Internet sovereignty agenda reflect regime priorities regarding Internet governance, national defense, and internal influence.

At the same time, Internet sovereignty, as embraced by the SCO, its member states, and other nations, is full of contradictions. For example, China emphasizes noninterference in states' internal affairs. It asserts the importance of equitable Internet governance as well as international law and international organizations in the formation of norms applicable to the digital space. Yet China has itself relied heavily on extraterritorial digital intrusions to achieve regime goals. It has also consistently rejected meaningful application of international human rights law to its domestic information controls and other digital authoritarian practices (HRIC, 2016), branding rights-based challenges to such practices as politicization or double standards. All of this calls into question whether an Internet sovereignty norm advances international law, noninterference, and win-win cooperation (a preferred term of the Chinese government)—or simply serves as license to control and repress with impunity.

With China's rhetorical and monetary support, however, it appears that Internet sovereignty has achieved emergence as a social norm. Prospects for diffusion among a broader international constituency may be bolstered by the decline of U.S. normative leadership in the international arena and China's growing financial and political influence, including that facilitated through the SCO and the Wuzhen Process. However, Internet sovereignty lacks the criteria of legality that would strengthen its acceptance as a legal norm. While this weakness may undermine diffusion of the norm, the ongoing process of norm contestation surrounding Internet sovereignty could yet result in its further refinement.

References

Ahmed, S. (2017, December 20). Refocusing on the "world" at the World Internet Conference. *China-U.S. Focus.* Retrieved from https://www.chinausfocus.com/political-social-development/refocusing-on-the-world-at-the-world-internet-conference

Antonova, S. (2013). Internet and the emerging global community of rights: The human rights debate at the Internet Governance Forum. *Journal of Philosophy of International Law*, *4*(1), 84–98.

Retrieved from http://www.academia.edu/9063864/INTERNET_AND_THE_EMERGING_GLOBAL_COMMUNITY_OF_RIGHTS_THE_HUMAN-RIGHTS_DEBATE_AT_THE_INTERNET_GOVERNANCE_FORUM

Areddy, J. (2015, December 17). Anti-Wikipedian translation at China's Internet conference. *Wall Street Journal*, China Real Time Report. Retrieved from https://blogs.wsj.com/chinarealtime/2015/12/17/anti-wikipedian-translation-at-chinas-internet-conference

Bandurski, D. (2013, November 5). Guidance of public opinion. *China Media Project*. Retrieved from http://chinamediaproject.org/2013/11/05/guidance-of-public-opinion-舆论导向/

Bandurski, D. (2015a, October 2). Thoughts on "Internet sovereignty." *Medium*. Retrieved from https://medium.com/@cmphku/thoughts-on-internet-sovereignty-ae18a125b89e

Bandurski, D. (2015b, September 28). Two share a boat. *Medium*. Retrieved from https://medium.com/@cmphku/two-share-a-boat-a5a22b60744

Ben-Josef Hirsch, M. (2014). Ideational change and the emergence of the international norm of truth and reconciliation commissions. *European Journal of International Relations*, *20*(3), 810–833.

Brunnée, J., & Toope, S. (2010). The responsibility to protect and the use of force: Building legality. *Global Responsibility to Protect*, *2*, 191–212.

Carr, M. (2015). Power plays in global Internet governance. *Journal of International Studies*, *43*(2), 640–659.

Cassese, A. (2005). *International law*. New York, NY: Oxford University Press.

沈雪石 [Chen Xueshi]. (2004, January). 论信息网络时代的国家安全 [On national security in the information network age]. 国防科技 [National Defense Science and Technology], 20.

ChinaFile. (2013, April 22). *Document 9: A ChinaFile translation*. Retrieved from https://www.chinafile.com/document-9-chinafile-translation

中国信息安全 [China Information Security]. (2015). 上合组织举行首次网络反恐演习 [Shanghai Cooperation Organization conducts first anti-terror exercise]. (December 2015), 70.

Citizen Lab. (2014, November 11). *Communities @ risk: Targeted digital threats against civil society*. Retrieved from https://targetedthreats.net/

Deibert, R., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance*, *18*, 339–361.

Deitelhoff, N., & Zimmermann, L. (2013). *Things we lost in the fire: How different types of contestation affect the validity of international norms* (PRIF Working Paper No. 18). Frankfurt, Germany: Peace Research Institute Frankfurt.

Falcone, R., and Miller-Osborn, J. (2016, January 24). Scarlet mimic: Years-long espionage campaign targets minority activists. *Palo Alto Networks*. Retrieved from http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, *52*(4), 887–917. Retrieved from http://www.ir.rochelleterman.com/sites/default/files/Finnemore_Sikkink_1998.pdf

Florini, A. (1996). The evolution of international norms. *International Studies Quarterly*, *40*(3), 363–389.

Horwitz, J. (2017, December 1). Starting this weekend, China celebrates its "open" Internet after a year of unprecedented censorship. *Quartz*. Retrieved from https://qz.com/1144001/this-weekend-china-celebrates-its-open-internet-after-a-year-of-unprecedented-censorship/

Human Rights in China. (2011, March). *Counter-terrorism and human rights: The impact of the Shanghai Cooperation Organization*. New York, NY: Author. Retrieved from https://www.hrichina.org/sites/default/files/publication_pdfs/2011-hric-sco-whitepaper-full.pdf

Human Rights in China. (2016, November). *The China challenge to international human rights: What's at stake?* New York, NY: Author. Retrieved from http://www.hrichina.org/sites/default/files/hric_upr_mid-term_assessment_11.06.2016.pdf

International Court of Justice. (1986). *Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America)*. Merits, Judgment. I.C.J. Reports 1986, p. 14. Retrieved from http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

嵇兆钧 [Ji Zhaojun]. (2000). 网络安全，网络主权, 网络创新 [Network security, sovereignty, and innovation]. 世界网络与多媒体 [International Networks and Multimedia], *8*(10), 16–20.

Kaye, D. (2015, May 22). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/29/32). UN Human Rights Council.

Keck, M., & Sikkink, K. (1999). Transnational advocacy networks in international and regional politics. *International Social Science Journal*, *51*(159), 89–101. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2451.00179

Krook, M., & True, J. (2010). Rethinking the life cycles of international norms: The United Nations and the global promotion of gender equality. *European Journal of International Relations*, *18*(1), 103–127.

Kunig, P. (2008). Prohibition of intervention. *Max Planck encyclopedia of public international law*. Oxford Public International Law. Retrieved from http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434

刘阳子 [Liu Yangzi]. (2012, November). 对国家网络主权的理解 [An understanding of states' Internet sovereignty]. 中国信息安全 [China Information Security], 65.

鲁炜 [Lu Wei]. (2016, March). 坚持尊重网络主权原则推动构建网络空间命运共同体 [Support respect for the principle of Internet sovereignty, promote construction of a shared destiny for cyberspace]. 中国信息安全 [China Information Security], 36.

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., . . . Paxson, V. (2015, April). *China's Great Cannon* (Research Brief). Toronto, Canada: Citizen Lab. Retrieved from https://citizenlab.ca/2015/04/chinas-great-cannon/

Margolin, J. (2016, December 2). Russia, China, and the push for "digital sovereignty." *Global Observatory*. Retrieved from https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/

McConnell, B. (2017, December 13). China cyber: Stepping into the shoes of a "major power." *The Diplomat*. Retrieved from https://thediplomat.com/2016/12/china-cyber-stepping-into-the-shoes-of-a-major-power/

McKune, S. (2015a, September 28). *An analysis of the International Code of Conduct for Information Security.* Toronto, Canada: Citizen Lab. Retrieved from https://citizenlab.ca/2015/09/international-code-of-conduct/

McKune, S. (2015b). "Foreign hostile forces": The human rights dimension of China's cyber campaigns. In Jon R. Lindsay, Tai Ming Cheung, & Derek S. Reveron (Eds.), *China and cybersecurity: Espionage, strategy, and politics in the digital domain* (pp. 260–293). New York, NY: Oxford University Press.

Meiya Pico. (2018, March). Training. Retrieved from https://meiyapico.com/training/index.html

Meng, Q. (2017, December). SCO joint anti-cyber terrorism exercise held in Xiamen. *CGTN*. Retrieved from https://news.cgtn.com/news/326b7a4d30637a6333566d54/share_p.html

Ministry of Foreign Affairs of the People's Republic of China & State Internet Information Office. (2017). *International Cyberspace Cooperation Strategy.* CD/2092. Retrieved from https://undocs.org/CD/2092

Mueller, M. (2017). *Will the Internet fragment? Sovereignty, globalization and cyberspace*. Cambridge, UK: Polity Press.

Newman, E., & Zala, B. (2017). Rising powers and order contestation: Disaggregating the normative from the representational. *Third World Quarterly*, 1–18. Retrieved from https://doi.org/10.1080/01436597.2017.1392085

Ran, J. (2017, March 15). American unrest proves China got the Internet right. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2017/03/15/american-unrest-proves-china-got-the-internet-right-beijing-great-firewall-censorship-trump/

Ray, V., & Falcone, R. (2016, January 21). NetTraveler spear-phishing email targets diplomat of Uzbekistan. *Palo Alto Networks*. Retrieved from http://researchcenter.paloaltonetworks.com/2016/01/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/

Roberts, A. (2017). *Is international law international?* New York, NY: Oxford University Press.

Schmitt, M. (2017). Grey zones in the international law of cyberspace. *Yale Journal of International Law Online*, *42*(2), 1–21. Retrieved from https://cpb-us-west-2-juc1ugur1qwqqqo4.stackpathdns.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf

Schmitt, M., & Vihul, L. (2014). *The nature of international law cyber norms* (Tallinn Paper No. 5). NATO Cooperative Cyber Defense Centre of Excellence. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf

SCO countries hold drill targeting cyber-terrorism. (2017). *Xinhua*. Retrieved from http://www.xinhuanet.com/english/2017-12/06/c_136806108.htm

Shanghai Cooperation Organization. (2001). *Declaration on the establishment of the Shanghai Cooperation Organization*. Retrieved from https://www.hrichina.org/sites/default/files/PDFs/Reports/SCO/2011-HRIC-SCO-Whitepaper-AppendixA-SCO-Docs.pdf

Shanghai Cooperation Organization. (2009). *Agreement between the governments of the member states of the Shanghai Cooperation Organization on cooperation in the field of international information security*. Unofficial translation by NATO CCDCOE. Retrieved from https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

Shanghai Cooperation Organization. (2017). *Convention of the Shanghai Cooperation Organization on combating extremism.* Retrieved from https://www.rusemb.org.uk/fnapr/6271

沈逸 [Shen Yi]. (2015, December 19). 网络主权：全球网络空间新秩序的中国主张 [Internet sovereignty: China's advocacy for a new order in global cyberspace]. Retrieved from http://tech.qq.com/a/20151219/027794.htm

Tikk, E., & Kerttunen, M. (2017). *The alleged demise of the UN GGE: An autopsy and eulogy.* New York, NY: Cyber Policy Institute. Retrieved from http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

Timmons, H. (2015, December 16). Mapped: The heads of state attending China's "World Internet Conference." *Quartz*. Retrieved from https://qz.com/575180/mapped-the-heads-of-state-attending-chinas-world-internet-conference/

Wang, Chen. (2010, July 13). *Concerning the development and administration of our country's Internet.* Unofficial translation by Human Rights in China. Retrieved from https://www.hrichina.org/en/content/3241

Xi Jinping. (2015, December 16). *President of the People's Republic of China at the opening ceremony of the Second World Internet Conference.* Wuzhen, China: Ministry of Foreign Affairs of the People's Republic of China. Retrieved from http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

Xi Jinping leads Internet security group. (2014, February 27). *Xinhua*. Retrieved from http://www.chinadaily.com.cn/china/2014-02/27/content_17311358.htm

叶征 [Ye Zheng]. (2015, July). 对网络主权的思考 [Thoughts on Internet sovereignty]. 中国信息安全 [China Information Security], 28.

叶征, 赵宝献 [Ye Zheng & Zhao Baoxian]. (2014, January). 关于网络主权、网络边疆、网络国防的思考 [Thoughts on Internet sovereignty, Internet borders, and national network defense]. 中国信息安全 [China Information Security], 28.