The Ohio State Technology Law Journal

CYBER SOVEREIGNTY AT ITS BOLDEST: A CHINESE PERSPECTIVE

ANQI WANG*

CONTENTS

* Candidate for MSc in Social Science of the Internet, Oxford Internet Institute at the University of Oxford. The author is deeply indebted to professor Han Liu at Tsinghua Law School for his invaluable guidance and comments. This paper benefitted from helpful feedback provided by Lianrui Jia, Anda Wang and Wenlong Li. The author is particularly grateful to the editors of the *Ohio State Technology Law Journal* for their professional editorial support.

I. Introduction

At the initial stage of Internet development during the 1990s, cyberspace was hailed as a borderless, decentralized and open world of free-flowing information. The term *Internet sovereignty* was developed by early eminent engineers, scholars and Internet exceptionalists inspired by the New Left Movement of the 1960s and the New Social Movement of the 1970s and 1980s.[1] In the eyes of these Internet pioneers, cyberspace should be operated without systematic control from any authoritative entity or regulatory arbitrage.[2] The core nature of the Internet is to advance the dissemination of knowledge and to achieve personal freedom through a self-governance mechanism. Accordingly, cyber sovereignty was democratically interpreted as a utopian concept exempted from governmental control and free of cooperation constraints; it is essentially about granting users' rights and empowering users with shared resources to govern themselves.

However, with the U.S. government's reign over root servers in the late 90s, the noble fantasy of cyber-utopianists was officially bankrupted. Entering into the 21st century, commercialization has made the Internet an artificial, man-made network that operates within geographical borders.[3] Nowadays, the subject of Internet sovereignty has shifted from governing users to governing states. Cyber sovereignty has become synonymous with states endeavoring to impose control over the intangible cyberspace within territorial borders. Governments, whether democratic or nondemocratic, imbue

---

[1] Liu Han (刘晗), *Yuming Xitong, Wangluo Zhuquan Yu Hulianwang Zhili: Lishi Fansi Jiqi Dangdai Qishi* (域名系统、网络主权与互联网治理：历史反思及其当代启示) [DNS, Cyber Sovereignty and Internet Governance: A Historical Reflection and its Contemporary Legacy], 28 Peking Uni. L. J. (中外法学) 518, (2016).

[2] *See*, *e.g.*, David Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996); Timothy S. Wu, *Cyberspace Sovereignty?* 10 HARV. J. L. & TECH. 467 (1997).

[3] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 58-59 (2006).

the Internet with regulatory law and policies. The motivations for these practices range widely; from concerns over national security, copyright protection, and protection of social values, to the protection of economic monopolies. For China, although Internet sovereignty is a relatively new concept, it follows the entrenched core rationale of its assertive Internet stance, that is, to exert extensive control in order to maintain its social stability and regime legitimacy.

The Chinese idea of cyber sovereignty is a high-profile declaration of intent to fragment the Internet with its jurisdiction.[4] It was firstly introduced in a Chinese manifesto on the Internet, "The Internet in China," published by the Chinese State Council Information Office in 2010.[5] This white paper characterizes the "Internet sovereignty of China" as "within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty" and proclaims that "the Internet sovereignty of China should be respected and protected."[6] Its emphasis on noninterference and equal participation can be understood in conformity with China's regulatory tone of foreign policy; according to President Xi, cyber sovereignty conveys "respecting each country's right to choose its own Internet development path, its own Internet management model [and] its own public policies on the Internet."[7]

This concept has been increasingly prevalent in Chinese official discourse since 2014. In 2014, President Xi Jinping called for other countries to "respect sovereignty on the Internet" at the First World Internet Conference. In the following year, he proposed the "four principles" and "five-point advocacy," with the first principle emphasizing respect for "cyber sovereignty."[8] During the third

---

[4] INFO. OFFICE OF THE STATE COUNCIL OF CHINA, INTERNET IN CHINA 2 (2010).
[5] *Id*.
[6] *Id*. at 11.
[7] Bruce Sterling, *Respecting Chinese and Russian Cyber-Sovereignty In The Formerly Global Internet,* WIRED (Dec. 22, 2015), https://www.wired.com/beyond-the-beyond/2015/12/respecting-chinese-and-russian-cyber-sovereignty-in-the-formerly-global-internet/ [https://perma.cc/TE46-ZSDH].
[8] Catherine Shu, *China Tried to Get World Internet Conference Attendees To Ratify This Ridiculous Draft Declaration*, TECH CRUNCH (Nov. 14, 2014, 12:52 PM), https://techcrunch.com/2014/11/20/worldinternetconference-declaration

Wuzhen World Internet Conference in November 2016, Xi called for "more fair and equitable" governance of the global web and stated that China would work to uphold "cyber sovereignty."[9] In 2017, cyber sovereignty became the "key in China's vision of internet development" in Xi's speech at the 19th Party Congress.[10]

This concept has attracted both domestic and international attention and elicited controversial debates. Advocates, mostly Chinese scholars, warmly embrace the idea of cyber sovereignty. They believe that this idea contributes to the protection of national security,[11] as well as ideology security.[12] Western observers tend to reduce China's cyber

---

[https://perma.cc/44N5-UUSV] ("We should respect each country's rights to the development, use and governance of the Internet, refrain from abusing resources and technological strengths to violate other countries' Internet sovereignty, and build an Internet order to equality and mutual benefit." "Third, jointly safeguard cyber security. We should actively cope with challenges to cyberspace security and reject all forms of cyber-attacks and Internet theft. We should work together to fight cyber-crimes, protect individual privacy and information security, and safeguard the legitimate rights and interests of citizens.").

[9] Cao Yin & Zhang Zhihao, *Xi: Share Internet Governance,* CHINA DAILY ASIA (Nov. 16, 2016, 5:30 PM), https://www.chinadailyasia.com/nation/2016-11/16/content_15527097.html [https://perma.cc/ZF6E-K42N].

[10] Mark Schiefelbein, *Chinese President Xi Jinping delivers a speech at China's 19th Party Congress,* ABC NEWS (Dec. 3, 2017, 4:23 AM), http://www.abc.net.au/news/2017-12-03/chinese-president%C2%A0xi%C2%A0jinping%C2%A0delivers-a-speech/9221698.

[11] *See*, *e.g.*, Liu Yangyue (刘杨钺) & Yang Yixin (杨一心), Wangluo Kongjian "Zaizhuquanhua" Yu Guoji Wangluo Zhili de Weilai ("网络空间"再主权化" 与国际网络治理的未来) [*The Re-territorialization of Cyberspace And The Future of International Internet Governance*], 15 INT'L F. (国际论坛) 1, 4 (2013); Wu Hequan (邬贺铨) & Ni Guangnan (倪光南), Meiyou Wangluo Anquan Jiu Meiyou Guojia Anquan (没有网络安全就没有国家安全) [*National Security Cannot Live Without Cyber Security]*, QIU SHI (Oct. 15, 2015), http://www.qstheory.cn/dukan/qs/2015-10/15/c_1116807805.htm.

[12] *See, e.g.*, Du Yanyun (杜雁芸), Meiguo Wangluo Baquan Shixian de Lujing Fenxi (美国网络霸权实现的路径分析) [An analysis on how America achieved its cyber-hegemony] 24 TAIPINGYANG XUEBAO (太平洋学报) 65, 75 (2016).

sovereignty to censorship, and cry foul against it accordingly.[13] They insist upon the multi-stakeholder 'Internet freedom' theory.[14] Under this vision, China's conception of cyber sovereignty appears uncongenial and untenable.[15] This tit-for-tat debate forms a conventional framework of Internet governance model, a state-centric agenda represented by China versus an information freedom agenda represented by the Western observers.

There has been a growing body of literature framing China's cyber sovereignty through the lens of such an Internet governance model. Sarah Mckune and Shazeda Ahmed warned that China's advocacy for Internet sovereignty could undermine multi-stakeholderism and its associated values, including transparency, accountability, and human rights.[16] Zhang Xinbao and Xu Ke countered the censorship argument and criticized the hegemonic perspective of multi-stakeholderism.[17] Kristen Eichensehr contrasted China's state-centric multilateralism with America's bottom-up multi-stakeholderism, shedding light on how China and its cyber ally Russia attempt to dominate cyberspace as

---

[13] *See,* e.g., Amy Chang, *How the Internet with Chinese Characteristics Is Rupturing the Web*, HUFFPOST (Feb. 14, 2015, 1:52 PM), https://www.huffingtonpost.com/amy-chang-/china-internet-sovereignty_b_6325192.html [https://perma.cc/4KCM-YMUY]; Nick Lynall, *Cyber Sovereignty: The Sino-Russian Authoritarian Model,* FOREIGN BRIEF (Sep. 15, 2017), https://www.foreignbrief.com/tech-society/cyber-sovereignty-sino-russian-authoritarian-model/ [https://perma.cc/ZC83-M2G4]; Scott Livingston, *Beijing Touts "Cyber-Sovereignty" In Internet Governance: Global Technology Firms Could Mine Silver Lining*, CHINA LAW BLOG (Feb. 19, 2015), https://www.chinalawblog.com/2015/02/beijing-touts-cyber-sovereignty-in-internet-governance-global-technology-firms-could-mine-silver-lining.html [https://perma.cc/74LU-JBFH].

[14] Internet Freedom, U.S. DEP'T OF STATE, https://www.state.gov/internet-freedom/.

[15] Scott Shackelford & Frank Alexander, *China's Cyber Sovereignty: Paper Tiger or Rising Dragon?* ASIA & PACIFIC POL'Y SOC'Y (Jan. 12, 2018), https://www.policyforum.net/chinas-cyber-sovereignty/ [https://perma.cc/2FCP-WRHK].

[16] Sarah Mckune & Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. OF COMM. 3835, 3836 (2018).

[17] Zhang Xinbao (张新宝), Xu Ke (许可), *A Study on Cyberspace Sovereignty* (网络空间主权研究), 4 CHINA LEGAL SCI. 33 (2016).

a part of territory where censorship could happen.[18] Hong Shen has pointed out that the inadequacy of this framework lies in its failure to examine the multifaceted power interactions among powerholders, perpetuating China's state-centric authoritative image.[19] This literature has made valuable contributions to our understanding of cyber sovereignty, but seems to limit discussions within the scope of Internet governance.

Building upon Hong Shen's argument, this article argues that such frameworks indeed reveal the most salient feature of China's cyber sovereignty and its most fundamental difference from western cyber norms, but that it can also be misunderstood because it exonerates attempts made by Western governments to govern the Internet and limits China's cyber sovereignty within the scope of censorship. If we understand China's cyber sovereignty solely within this framework, the question becomes "whether the government should impose sovereign control on cyberspace"—which suggests the answer that China should not gain that control. But the real question is no longer about whether nations should exert sovereign control over the Internet, or which country has the legitimate right to do so. Scholars have recognized that even nations with the most "information freedom" also exert sovereign control.[20] The crux of the question this paper tries to address is *how much* control is being exercised by China and how China's approach evolves into a different, arguably bolder version when compared with other countries.

---

[18] Kristen Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J., 317, 329-335 (2015).

[19] Hong Shen, *China and Global Internet Governance: Toward an Alternative Analytical Framework,* 9 CHINESE J. OF COMM. 304, 306 (2016).

[20] Harold Koh, *International Law in Cyberspace* (September 18, 2012), https://20092017.state.gov/s/l/releases/remarks/197924.htm (comments at the USCYBERCOM Cyber Law Conference); James Lewis, *Piecemeal Measures Regulate Cyberspace,* CIPHER BRIEF (Feb. 26, 2017), https://cyberstability.org /news/piecemeal-measures-regulate-cyberspace/ [https://perma.cc/7VY6-799D] ("No country, except perhaps China, outright says it is extending sovereign control over the internet, and this lack of explicit pronouncements helps preserve the illusion that the internet is free and open. Instead, countries impose regulations for data protection and localization, to restrain hate speech or intellectual property theft, creating a piecemeal extension of sovereignty.").

To deconstruct this conventional framework and deepen our understanding of China's cyber sovereignty, this article locates this concept within the wider scope of China's social relations and political mechanisms. It aims to provide a systemic account of China's unique interpretation of cyber sovereignty, unpacking conventional mythology to understand what China really means by that concept. It will contribute to the current literature by understanding this concept beyond the dichotomies of multi-stakeholderism and multilateralism; information freedom theory and authoritarian regimes; the liberal market; and state-nation constraints. To this end, it will apply Benckler's framework of the three-layer principle, examining how China regulates the physical, logical, and content layer of the Internet.[21] It argues that China's long-standing cyber strategies of network security ("Wangluo Anquan") and information sovereignty ("Xinxi Zhuquan") are embodied at the physical layer and the content layer respectively, and a more recent cyber-norm multilateralism agenda is advocated at the logical layer. Overall, cyber sovereignty is a combination of the network security at the physical layer, the information sovereignty at the content layer and the state-centric multilateral approach at the logical layer.

Benckler's framework is selected because China's laws and legal documents demonstrate a layered regulatory design: the telecommunications department of the State Council and public security departments are assigned to maintain cybersecurity protection and supervision, which embodies the physical layer;[22] the Ministry of Industry and Information Technology is responsible for regulating domain name services, which comprises the logical layer;[23] and the

---

[21] *See infra* Section IV.

[22] Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) [hereinafter Cybersecurity Law], http://www.cac.gov.cn/2016-11/07/c_1119867116.htm [https://perma.cc/7QTX-MXPQ].

[23] (中国互联网域名管理办法) [Measures for the Administration of Internet Domain Names of China], (promulgated by Ministry of Industry & Information Technology,

Cyberspace Administration of China is authorized to manage content regulation, which is the content layer. This three-layer analysis allows insight into how, and to what extent, China's version of strong cyber sovereignty differs from other forms of weak cyber sovereignty.[24] Through the three-layer analysis, this article argues that in the eyes of Chinese officials, the Internet is essentially a state-owned communication tool with economic benefits: the political and ideological security of the government is the basic foundation of associated economic activities operated on the Internet. The concept of cyber sovereignty was employed to strike the right balance between the Internet as the property of a political party-state and its commercial activities; unlike other or weaker forms of cyber sovereignty in democratic countries. China instrumentalizes the concept of cyber sovereignty to impose strict control upon the physical, logical and content layers to maintain national and ideological security, while trying to maximize the growth of digital economy.

This article will proceed as follows. First, it will describe three dimensions of cyber sovereignty: its physical and ideological contribution to national security, its economic protection to domestic tech-companies, and how it was contested between advocates and skeptics on an international level. This article argues that these three dimensions corroborate the conventional framework of Internet governance, a state-centric agenda represented by China opposed by an information freedom agenda represented by Western society.[25] In order to present clear, complete and representative views from both sides, this article selects articles from academic journals, Chinese government-sponsored media and American government-assisted

---

Sep. 30, 2000), at art. 3 [hereinafter Measures].

[24] The comparison of "weak cyber sovereignty" and "strong cyber sovereignty" derives from Dana Polatin-Reuben & Joss Wright, who define weak data sovereignty as "private sector-led data protection initiatives with an emphasis on the digital-rights aspects of data sovereignty" and strong data sovereignty as favoring "a state-led approach with an emphasis on safeguarding national security. See Dana Polatin-Reuben & Joss Wright, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet*, paper presented at 4th USENIX WORKSHOP ON FREE AND OPEN COMMUNICATIONS ON THE INTERNET (FOCI 14) 1, 2 (2014).

[25] Hong Shen, *supra* note 19, at 2.

think-tanks. This article contends that the conventional framework is built upon partial facts presented by each side, and attempts to connect these narratives to deepen understanding for cyber sovereignty.

Secondly, this article will discuss the technological, political and legal context of China's Internet development. Specifically, it will introduce the regulatory mechanism of the Internet in each developmental period and the establishment of the Cyberspace Administration of China (CAC).[26] Thirdly, it will discuss a three-layer scheme and investigate how the Chinese conception of cyber sovereignty is composed by three layers of the Internet—the physical layer, the logical layer, and the content layer. It will argue that China imposes strict control upon the physical, logical and content layers to maintain political stability, while trying to minimize its chilling effect on the growth of the digital economy. Ideological and political conflicts that occur at the content layer are the key that sheds light on vital differences between China and other states. Overall, with its ongoing efforts to strengthen Internet infrastructure security and content censorship, China has applied a narrow and controlling version of cyber sovereignty that censors Internet expression and activities.

II. Three Dimensions of Cyber Sovereignty

This section will unfold three major dimensions that lie beneath the concept of cyber sovereignty: cyber sovereignty contributes to ensure Internet security at the *infrastructural* and *ideological* dimension, provides a form of economic protectionism to Chinese high-tech industries at the *economic* dimension, and faces raising concerns from international community who questioned such concept would compromise universal values like information security and freedom of speech at the *international* dimension. Through exhibiting representative narratives from Chinese and Western scholars for each dimension, this paper identifies that the conventional framework is built upon partial facts presented by each side. This section attempts to reveal the limitation of this framework and connect these partial narratives to deepen understanding of cyber sovereignty.

---

[26] *See infra* Section II.C.

a. Infrastructure and Ideological Security

The Internet was initially conceived by the United States during the Cold War; nowadays the key information infrastructure is still dominated by the U.S. During the initial adoption of the Internet in third-world countries, scholars raised concerns about technological dependence. Some worried that infrastructural monopoly would create unequal distribution and a digital divide, leading to asymmetric disadvantages for smaller, less connected developing countries.[27]

China was, and still remains, one of these developing countries. While China might consider foreign infrastructure ownership an opportunity to attract foreign investment and accelerate economic prosperity, it always sees U.S. technical ascendency as a potential threat. The fact that the majority of root servers are located in the United States is emphasized by Chinese scholars as a legitimate reason to attain cyber sovereignty.[28] They also worry that the U.S. entities registered the most popular mainstream domain names under the current IPv4 system. Under the current Internet governance model, even though the U.S. government does not directly regulate the Internet naming system, the active participation of private corporations and civil

---

[27] *See e.g.*, Juli L. Gittinger, *Is There Such a Thing as 'Cyberimperialism?,'* 28 COMM. J. MEDIA & CUL. STUD. 509, 511 (2014); Linda Main, *The Global Information Infrastructure: Empowerment or Imperialism?,* 22 THIRD WORLD Q. 83, (2001). It suggests that although Global Information Infrastructure created a global information market and narrowed the poverty gap, the U.S.-driven market is in risk of moving towards a two-tier technology society that perpetuates the old distinction between North and South, due to inadequate capacity and particular regional issue such as "the lack of regional, social and economic integration found in the USA" and "deep political, linguistic and cultural divisions that do not exist in the USA." *Linda Main, supra* note 28, at 83.

[28] Chi Dongyang & Liu Quan (赤东阳&刘权), "Cong Wangluo Kongjian Guoji Hezuo Zhanlve Kan Woguo Weihu Wangluokongjian Zhuquan de Silu" (从《网络空间国际合作战略看我国维护网络空间主权的思路》看我国维护网络空间主权的思路) [Thoughts of Maintaining Cyberspace Sovereignty from China's "International Cooperation Strategy of Cyberspace"] Z1 CYBERSPACE SECURITY (网络空间安全) 1, 2 (2017).

society representatives who have technical advantages in designing the Internet infrastructure still largely represent U.S. interests.[29]

As America's technological hegemony struck fear among Chinese leadership, the imperative to improve the capacity of China's own core Internet infrastructure was constantly emphasized. In 2016, President Xi pointed out that "Internet core technology is the greatest 'vital gate,' and the fact that core technology is controlled by others is our greatest hidden danger."[30] Developing core Internet infrastructure not only advances infrastructural security, it is also closely tied to economic development. he *Report on China Internet Development* 2017 states that "[n]etwork infrastructure has become a new type of public infrastructure that promotes economic and social development." [31] The rapid development of basic infrastructure underlines the central leadership's fervent pursuit for technological independence.

The Chinese emphasis on infrastructure independence has an ideological dimension as well. Paul Cornish recognizes that the cyber sovereignty debate in the PRC goes deeper than physical expression such as trade-offs and procedures; a more enduring aspect is cultural respect.[32] While Western representatives argued that delegitimizing

---

[29] Sandeep Joshi, *India to Push for Freeing Internet from U.S. Control*, HINDU (Dec. 7, 2013, 11:55 PM), http://www.thehindu.com/sci-tech/technology/internet/india-to-push-for-freeing-internet-from-%20us-control/article5434095.ece.; Kristen Eichensehr, *supra* note 18, at 347 ("Although the United States supports the multistakeholder model at least in part for freedom of expression reasons, the bottom-up governance model also serves U.S. interests because many of the nongovernmental voices that the model amplifies, including technology companies and nongovernmental actors, have ties to the United States or share its values.")

[30] Xi Jinping, *Speech at The Work Conference for Cybersecurity and Informatization*, CHINA COPYRIGHT & MEDIA (Apr. 19, 2016), https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization [https://perma.cc/3J3B-2KFX].

[31] CORPORATE AFFAIRS COMMISSION, REPORT ON CHINA INTERNET DEVELOPMENT (2017), http://www.wuzhenwic.org/download/ReportonChinaInternetDevelopment2017overview.pdf.

[32] Paul Cornish, *Governing Cyberspace through Constructive Ambiguity*, 57

the free flow of information is employed to justify censorship,[33] Chinese scholars see malicious intentions behind the U.S. advocacy for "information freedom." Chinese authorities fear that the Internet would erode Chinese ideological security[34] if the Western conception of Internet freedom prevails,[35] and that importing Western values would contribute to cultural imperialism.[36] The exposure of the PRISM project reinforced that vision: that information freedom is a hypocritical diplomatic language to cover true intent; tearing down the

---

SURVIVAL: ST. POWER & CLIMATE CHANGE 153, 164 (2015).

[33] DEAN CHENG, CYBER DRAGON: INSIDE CHINA'S INFORMATION WARFARE AND CYBER OPERATIONS, 1, 60 (2017) ("[B]y delegitimizing the free flow of information, Chinese authorities would justify efforts to control what information can flow across state boundaries and could even seek assistance from other states in constricting that flow.").

[34] Xu Qiang (徐强), Zengqiang Zhongguo Wangluo Wenhua Ruanshili (增强中国网络文化软实力) ["To better advancing the soft power of China's Internet culture"], QIUSHI (Jan. 11, 2018), http://www.qstheory.cn/dukan/hqwg/201801/11/c_1122243467.htm.

[35] Michael Swaine, *Chinese Views on Cybersecurity in Foreign Relations*, 42 LEADERSHIP MONITOR 1, 7 (2013)(pointing out that "the 'ideological' dimension of cybersecurity usually refers to the defense and expansion of "socialist ideology and culture." Both civilian and military officials and observers assert that to protect China's sovereignty and the authority of the PRC government, the Internet in China must reflect socialist "cyber culture" and resist "ideological infiltration and political instigation.").

[36] See, *e.g.*, Yin Xiaorong (殷晓蓉), "Meijie Diguo Zhuyi" he "Shuzi Honggou"—Gainian Neihan Jiqi Shidai Yiyi de Fenxi Bijiao ("媒介帝国主义"和"数字鸿沟"—概念内涵及其时代意义的分析比较) [a comparative analysis on the conception and significance of "media imperialism" and "digital divide"], ZHONGGUO CHUANBOXUE LUNTAN (中国传播学论坛) (2003) (pointing out that in the 60s and 70s, the battle around information freedom cropped up between the United States and developing countries who had Soviet Union's back. At that time, when facing criticism on media imperialism, America used the idea of information freedom to defend itself and oppose developing countries' inquiry to develop a new order for communications and journalism.); Du Yanyun (杜雁芸), *supra* note 10 (noting that Chinese scholars see the U.S. actively advocate for Internet freedom, harboring malicious intentions to establish an ideology hegemony by selling its so-called universal value of information freedom.).

digital border of other countries while immunizing its own.[37]

Instead of shaping a free-flowing communication environment, proponents of cyber sovereignty believe that promoting a "positive energy" ideology ("zheng neng liang"), will allow the cultivation of a harmonious online environment. Min Jiang characterizes China's cyber sovereignty as "authoritarian informationalism" that combines capitalism, authoritarianism, and Confucianism.[38] The Confucianism Jiang proposes is reflected in the national call to build a "clear environment on cyberspace" and "harmonize the Internet." Employed to develop a cohesive, socialist nation, positive energy connotes a variety of meanings, including "patriotism," "loyalty to the communist party," "dedication to one's work," "honesty," "filial piety," and other culturally normative virtues.[39] By reviving these Confucian values in cyberspace, Jiang suggests that the Party hopes to legitimize party rule and promote social order. President Xi's remark in a CAC group meeting echoes this viewpoint. He stated that "we must . . . strengthen positive online propaganda, foster a positive, healthy, upward and benevolent online culture, use the Socialist core value view and the excellent civilizational achievements of humankind to nourish people's hearts and nourish society."[40]

Therefore, cyber sovereignty should not be viewed simply as a brand new concept isolated from historical perspectives: the infrastructural and ideological concerns behind Internet sovereignty have been held long before the age of Internet.[41] The Chinese worry that ideological and infrastructural American hegemony would allow the U.S. to pose a

---

[37] Michael Swaine, *supra* note 33, at 7.
[38] See Min Jiang, *Authoritarian Informationalism: China's Approach to Internet Sovereignty,* 30 SAIS REV. INT'L AFF. 71, 72 (2010).
[39] Derek Hird, *Smile Yourself Happy: Zheng Nengliang and The Discursive Construction of Happy Subjects*, in CHINESE DISCOURSES ON HAPPINESS (Gerda Wielander & Derek Hird eds, 2018).
[40] Xi Jinping, *Xi Jinping Gives Speech at Cybersecurity and Informatization Work Conference*, CHINA COPYRIGHT & MEDIA (April 19, 2016).
[41] *See generally*, Wenxiang Gong, *Information Sovereignty Revisited,* XIV INTERCULTURAL COMM. STU. 119, 120 (2005).

double standard [42] in their Internet strategy, establishing the U.S. hegemony with an Americanized Internet. Cyber sovereignty helps China both allocate critical Internet resources and resist American hegemony in terms of the spread of Internet freedom ideology. The Chinese authorities have always tried to utilize Western communication technologies, but at the same time curb its socio-political and ideological impacts.

b. Economic Empowerment Of Chinese Companies

While China's Internet-related business is developing increasingly quickly with broadband construction, many foreign companies left China due to strict data localization regulations and the censorship issue. Reports show that the Great Firewall has an adversarial impact on U.S. companies based in China.[43] Only 5 percent of respondents answered that "internet controls do not hinder my business in any way."[44]

---

[42] Yu Li (余丽), *Meiguo Hulianwang Zhanlve Jiqidui Zhongguo Zhengzhi Wenhua Anquan de Yingxiang* (美国互联网战略及其对中国政治文化安全的影响) [*American Internet Strategy and its Influences on Chinese Political and Cultural Agenda*], 2 GUOJI LUNTAN (国际论坛) [INT'L FORUM] 1 (2012). (Stating that the massive surveillance the American government implemented after enforcing the Patriot Act after 9/11 incident demonstrated the double standard the United States exercised); Zhang Yuan (张媛), *Wangluo Kongjian Huodong Xushoudao Zhuquan Yuanze Zhipei* (网络空间活动须受到主权原则支配) [Cyber Activities must be Dominated by the Sovereignty Principle], LEGAL DAILY (July 23, 2015, 8:36 AM), http://www.legaldaily.com.cn/rdlf/content/2015-07/23/content_6184990.htm?node=34014 [http://perma.cc/8UKL-AT7F] (stating that Li Zhong (李忠), the Director of the Institute of Law in the Chinese Academy of Social Sciences suggested that the PRISM project and documents revealed by WikiLeaks has created a delirious climate for the Internet, and that most countries cannot pretend nothing happened and not take measures to regulate the Web based on their territories).

[43] Paul Mozur & Carlos Tejada, *China's 'Wall' Hits Business*, WALL ST. J. (Feb. 13, 2013, 9:07 PM), https://www.wsj.com/articles/SB10001424127887323926104578277511385052752 [http://perma.cc/RHM7-TFLX].

[44] *Id*.

The departure of foreign companies left their Chinese domestic tech counterparts in a preponderant position to secure the Chinese market. For instance, a domestic company, Baidu, quickly grew to become Google's substitute after its exit from mainland China in 2010: when it left China, Google controlled 40 percent of the Chinese search market, and Baidu accounted for roughly 65 percent of the Chinese search engine market in 2018.[45]

Google is not the only foreign Internet platform provider that reeled from China's regulatory hurdles. American dotcoms such as YouTube, Twitter, and Facebook all fell prey to the censorship mechanism. With the external competitors leaving, the internal companies thrived. Similar services were offered by Chinese-indigenous dotcoms, such as Sina Weibo, a Chinese-equivalent of Twitter, Youku, a Chinese-homegrown alternative to YouTube, and WeChat, which successfully replaced Facebook and WhatsApp. Protectionist sentiment also has spilled into the 3G network arena.[46] The rapid growth of China's own tech superpowers leaves its global tech counterparts with an awkward dilemma—either adapt to China's laws, or quit.

Domestic companies did not remain content with a demographic dividend with the world's largest e-commerce market. Three tech giants, Baidu, Alibaba, and Tencent, also known as the BAT league, have attempted to move into "advanced industries" of cyber business, including semiconductors, chip materials, robotics, aviation equipment, and satellites.[47] McKinsey Global Institute counts China as the top three in the world for venture-capital investment in key types of digital technology; including virtual reality, autonomous vehicles,

---

[45] Search Engine Market Share China: Mar 2019-2020, STATCOUNTER, http://gs.statcounter.com/search-engine-market-share/all/china/ [http://perma.cc/XWK8-N56M].

[46] YU HONG, NETWORKING CHINA: THE DIGITAL TRANSFORMATION OF THE CHINESE ECONOMY 88 (2017).

[47] Michael Brown & Pavneet Singh, *China's Technology Transfer Strategy*, DEFENSE INNOVATION UNIT EXPERIMENTAL (DIUX) (2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

3-D printing robotics, drones, and artificial intelligence (AI).[48] Their active exploration in artificial intelligence with Internet-based technologies have been supported by national policies, such as Internet Plus and Internet Power dream. By promoting innovations in Internet-based commercial and management models to shape an Internet Plus ecosystem, these plans aim to integrate the Internet with traditional industries to realize another round of industrial and economic upgrading.[49] Yu Hong suggested that China is revved up for "an upgraded digital capitalism" through Internet Plus, which also empowers private domestic companies to gain considerable political influence.[50]

In the eyes of Beijing, these domestic government-registered actors are more politically reliable than their foreign counterparts. Since the early stage, Zhao identified that the media has to dance between the party line and the bottom line.[51] Min Jiang and Rongbin Han extend the dance analogy into the Internet business landscape: compared to their international rivals, domestic companies or information providers have shown a "discontented compliance to eschew discussion of censorship out of fear of losing license."[52] This political compliance has cultivated a symbiotic relationship between the state and Chinese Internet companies.[53] On the one hand, domestic companies take advantage of

---

[48] Jonathan Woetzel et al., MCKINSEY GLOBAL INSTITUTE, *China's Digital Economy: A Leading Global Force* 2-3 (2017), https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/China/Chinas%20digital%20economy%20A%20leading%20global%20force/MGI-Chinas-digital-economy-A-leading-global-force.ashx.

[49] *Internet Plus: Premier Li's New Tech Tool*, The St. Council The People's Republic of China (Mar. 13, 2015, 9:54 PM), http://english.gov.cn/premier/news/2015/03/13/content_281475070887811.htm [http://perma.cc/M5XK-C3SP].

[50] Yu Hong, *Pivot to Internet Plus: Modeling Chinas Digital Economic Restructuring?,* 11 INT'L J. OF COMM. 1486, 1499 (2017).

[51] YUEZHI ZHAO, MEDIA, MARKET, AND DEMOCRACY IN CHINA: BETWEEN THE PARTY LINE AND THE BOTTOM LINE (1998).

[52] RONGBIN HAN, CONTESTING CYBERSPACE IN CHINA: ONLINE EXPRESSION AND AUTHORITARIAN RESILIENCE 140 (2018); Min Jiang, *Internet Companies in China: Dancing Between the Party Line and the Bottom Line*,ASIE.VISIONS, JAN. 2012, at 31.

[53] Min Jiang & King-Wa Fu, *Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?,* 10 POL'Y & INTERNET 372, 384 (2018).

national subsidies and investments for the high-tech industry to maximize economic gains. On the other hand, domestic companies have to be deferential to relevant governmental laws and regulations, maximizing political stability. Min Jiang and King-Wa Fu raised the social credit system to illuminate this relationship.[54] While the state claims the system is used to rate the trustworthiness of citizens and business sectors, it can also be an instrumental tool for social control through surveillance of data. The domestic firms gather personal data that contribute to their businesses. With this data, the government can monitor and regulate individual behavior to maintain social stability.

Interestingly enough, although power centralization and censorship is at an unprecedented level, the digital trade is also hitting its liberal potential. As the Chinese government seeks to spread global influence, Chinese Internet companies have been actively participating in economic flows of the global market. Lianrui Jia and Dwayne Winseck found extensive foreign investor ownership stakes in Baidu (7.5%), Alibaba (40%) and Tencent (45%), arguing that they have increasingly integrated into the global capital market.[55] Moreover, in contrast to many fears driven by the data localization rule, Yu Hong noted that China-based centers welcome externally originated, cross-border data flows. Paraphrasing the president of China Unicom, the clients for which China Unicom runs data centers include foreign clients, such as Amazon, Google, and Microsoft.[56] In addition, postponement of the strict cross-border transportation of data rule in the CSL also reflects China's effort to preserve economic participation in the global market. Multinational countries worried that the incoming data localization rule would be detrimental to their businesses. China eventually decided to postpone the rule's enforcement for 18 months, to December 31, 2018.[57] Triolo, the political risk consultant for Eurasia

---

[54] *Id*.

[55] Lianrui Jia & Dwayne Winseck, *The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization,* 80 INT'L COMM. GAZETTE 30, 54 (2018).

[56] Hong, *supra* note 47, at 144.

[57] Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Firms Guessing*, N. Y. TIMES (May 31, 2017), https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html [http://perma.cc/T9NT-NCXN].

Group, commented that "getting the cross-border data flow issue right is a prerequisite for Beijing's efforts to promote economic globalization" and that "China is eager to avoid being seen as stifling digital trade."[58] Therefore, although China would not abandon its data localization and censorship strategy due to political stability concerns and benefits to domestic companies from this economic protectionism, it is not entirely accurate to characterize the economic consequence of cyber sovereignty as pure foreign exclusion.

c. Critics From Information Freedom Theory

China's cyber sovereignty has received an especially negative international reception. However, China remains intransigent about exercising greater influence on cyber norms under the onslaught of international critics. Chinese officials have constantly raised UN documents to substantiate its cyber sovereignty claim. In 2015, President Xi, at the opening ceremony of the Second World Internet Conference, cited the principle of sovereign equality in the "Charter of the United Nations" to illustrate why "we should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies."[59] Lu Wei, the former head of the General Office of the Central Leading Group for the Cyberspace Administration of China, writes that the spirit of the Charter of the United Nations entails the Internet's governing approach.[60] It is of pertinence to cyberspace, and this is

---

[58] *Id*.

[59] Rogier Creemers, *Speech at the 2nd World Internet Conference Opening Ceremony,* CHINA COPYRIGHT AND MEDIA BLOG (Dec. 16, 2015), https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/ [http://perma.cc/JGV2-4GSK].

[60] Lu Wei (鲁炜), Jianchi Zunzhong Wangluo Zhuquan Yuanze Tuidong Goujian Wangluo Kongjian Mingyun Gongtongti Zengqiang Zhongguo Wangluo Wenhua Ruanshili (坚持尊重网络主权原则 推动构建网络空间命运共同体) [Adherent to Cyber Sovereignty Principle and Build a Community of Common Future in Cyberspace], Qiushi (Feb. 29, 2016), http://www.qstheory.cn/dukan/qs/2016-02/29/m_1118164592.htm [http://perma.cc/QE9T-UAP6].

where Internet sovereignty arises.[61] It is not only the Chinese government that pushes hard on the Internet sovereignty multilateral governance approach internationally; Chinese scholars also spare no effort in emphasizing state sovereignty and territorial integrity.[62]

As much as Chinese officials and scholars like to cite the UN Charter,[63] the UN's Group of Governmental Expert (GGE) documents,[64] and the Tallinn Manual to advance its Internet sovereignty claims,[65] Western scholars have suggested that it is

---

[61] *Id*.

[62] *See infra* Section IV.B.2; *see, e.g*., Bai Hao (白皓), Wangluo Kongjian AnquanZzhili de Zhongguo Zhuzhang—Yi Zhuquan Yuanze Wei Shijiao (网络空间安全治理的中国主张—以主权原则为视角) [China's viewpoint on Internet security governance based on territorial sovereignty principle], 4 Information Security And Communications Privacy (信息安全与通信保密) (2017) (raising the idea that the group of government experts (GGE) came to consensus that international law, and especially the UN Charter, applies to state activity in cyberspace. Two years afterward, the same group proposed "four peacetime norms": states should not interfere with each other's critical infrastructure; they should not target each other's computer emergency response teams; they should assist other nations investigating cyber-attacks; and they are responsible for actions that originate from their territory. It also states that "the nation-state principle which is also the fundamental principle of international law should apply to the cyberspace, with some adjustments that make it more compatible with particular characteristics of the Internet.").

[63] Lu (鲁), *supra* note 57.

[64] Bai (白), *supra* note 59. Chinese scholars often use GGE documents to support their pro-cyber sovereignty arguments. The GGE documents suggest that "state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory." U.N. Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 27, U.N. Doc. A/70/174 (July 222, 2015).

[65] Chi & Liu (赤&刘), *supra* note 26; Fang Binxing (方滨兴), Zou Peng (邹鹏) & Zhu Shibing (朱诗兵), *Wangluo Kongjian Zhuquan Yanjiu* (网络空间主权研究) [Research On Cyber Sovereignty], 18 STRATEGIC STUD. CHINESE ACAD. ENGINEERING (中国工程科学) 1, 4 (2016).

essentially self-contradictory for the UN to incorporate China's proposal.[66] Mainstream media outlet publicities are tempted to view Russia and China's quest for information sovereignty "as yet another stab at censorship and control."[67] Democratic countries who value more personal freedom than collective interests in cyberspace, reflect their divergence with China's sovereignty assertion. For instance, the U.S. observed that China's emphasis on asserting sovereignty over "citizens and organizations within their borders" is "a diverging perspective from the United States," who "is highly protective of individual freedom of speech and other individual liberties, and views state efforts to control online content as 'inappropriate'."[68] In addition, the rest of the UN Charter, which sheds light on the importance of protecting basic human rights and freedom of speech, is inherently incongruous with cyber sovereignty and censorship.[69] Information freedom theorists worry this concept would allow the government to regulate the Internet more unscrupulously. Human rights organizations like Chinese Human Rights Defenders (CHRD) have made an appeal to the international community to demand that the government "amend relevant laws and regulations to remove restrictions on freedom of expression and the press, including for information on the Internet and sent through instant-messaging apps, that are not in accordance with the International Covenant on Civil and Political Rights and the

---

[66] Adam Segal, *The Development of Cyber Norms at The United Nations Ends in Deadlock. Now What?,* COUNS. ON FOREIGN REL. BLOG (June 29, 2017), https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what [http://perma.cc/EKS3-64NV] (observing that "[C]hinese officials have consistently stressed the UN Charter and the importance of sovereignty without mentioning the rest of international law," and "Beijing has never liked the idea that international law applies to cyberspace;" and also mentioning that China's representative proposed to "take out all references to international law in the upcoming report" during the 2015 meeting of the UN group.) *Id.*

[67] Evgeny Morozov, *Who Is the True Enemy of Internet Freedom - China, Russia, Or The US?,* GUARDIAN (Jan. 4, 2015, 7:04 P.M.), https://www.theguardian.com/commentisfree/2015/jan/04/internet-freedom-china-russia-us-google-microsoft-digital-sovereignty [http://perma.cc/Z5K2-CZNA].

[68] Cornish, *supra* note 30, at 155.

[69] Shannon Tiezzi, *China's 'Sovereign Internet,'* DIPLOMAT (June 24, 2014), https://thediplomat.com/2014/06/chinas-sovereign-internet/ [http://perma.cc/5797-6NN3].

Universal Declaration on Human Rights."[70]

It is worth noticing that in the eyes of information freedom theorists, restricting the Internet to protect the security of cyber infrastructure is not unacceptable, but it "must go hand-in-hand with respect for the human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights."[71] They worry that because China's Internet censorship is essentially antithetical to the freedom of speech, China's attempt to codify its version of Internet sovereignty into international law might spread censorship. To the West, China's pursuit of cyber sovereignty cannot simply be viewed as an act to implement cyber laws based on territorial borders; rather, it is an attempt to implement surveillance, heighten online speech censorship, and invade users' privacy within Chinese territory.[72] As commentators have put it, "if its philosophy of cyber sovereignty is even more widely enacted, many of us could one day find ourselves living behind the equivalent of the Great Firewall of China."[73]

---

[70] *Xi Jinping's "Cyber Sovereignty" Fast Eroding Space For Free Expression,* China Human Rights Defenders (Apr. 19, 2018), https://www.nchrd.org/2018/04/xi-jinpings-cyber-sovereignty-fast-eroding-space-for-free-expression/ [http://perma.cc/7ERC-UXFT].

[71] Tiezzi, *supra* note 66.

[72] Livingston, *supra* note 11 ("[B]ut China's conception of cyber-sovereignty is nothing less than a sharp realignment of the traditional conception of the Internet promoted in the developed world, from an open platform regulated by a diverse array of stakeholders, to one fragmented by national boundaries and regulated piecemeal by national governments. Under the Chinese conception of "'cyber-sovereignty" all forms of national censorship are equivalent."); Bethany Allen-Ebrahimian, *The 'Chilling Effect' of China's New Cybersecurity Regime*, FOREIGN POL'Y (July 10, 2015, 3:27 P.M.) http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/ [http://perma.cc/BX85-NTT5] (quoting the Chinese Director at Human Rights Watch, Sophie Richardson, as stating "Other provisions increase surveillance of the Internet for overly broadly defined security reasons without establishing effective privacy protections, increase requirements for companies to censor online speech, heighten a demand for companies to require real-name registration by users, and stipulate that user data must be stored in China;" and "one of the only means available to people in China to seek accountability or transparency from the state, or to peacefully communicate without threat of reprisal, is at grave risk."); Eichensehr, *supra* note 18.

[73] Shackelford & Alexander, *supra* note 13.

However, Chinese leaders have been refusing to interpret cyber sovereignty as authoritarian control for three reasons. Firstly, in regard to Internet content censorship, they hold that China only censors malicious comments, but welcomes insightful criticism. In Xi's speech at the Symposium on Cybersecurity and IT Application, he recognized the value of "kind criticism" contributing to the healthy development of the online environment. He stated that "to build a well-functioned Internet public sphere is not to censor all negative comments and only endorse a single perspective; it is to welcome, investigate, and learn lessons from the kind criticism but reject those comments which turn things upside down, mix the black with the white, spread rumors with malicious intentions, commit crimes[,] and override the Constitution." It remains unclear how to draw a bright line between "kind criticism" and malicious comments, which could leave the decision to the whim of government officials.

Secondly, China seems to embrace economic freedom in cyber cooperation. President Xi reiterated the necessity of "open Internet" ("Hulianwang Kaifang") in his talk, stating that "the development of the internet knows no national or sectoral boundaries."[74] It is imperative to recognize that the "open Internet" to which China refers does not share a similar meaning as in the traditional Western context of freedom of speech and information flow; rather, the Chinese understanding of "open Internet" encapsulates economic openness. Chinese leaders see the international cooperation to govern and develop the Internet based on a multilateral approach that requires participation from various governments as a form of "open Internet." For example, China initiated the Digital Silk Road project, as a core component of the "Belt and Road Initiative," to promote the construction of basic Internet infrastructure and international communications connectivity in major Eurasian and African nations.[75]

---

[74] FANG BINXING, CYBER SOVEREIGNTY: REFLECTIONS ON BUILDING A COMMUNITY OF COMMON FUTURE IN CYBERSPACE 172 (217).

[75] Nat'l Development & Reform Commission, *Vision and Actions on Jointly Building Silk Road Econ. Belt and 21st Century Mar. Silk Road,* BELT & ROAD PORTAL (Mar. 30, 2015, 6:30 P.M.), https://eng.yidaiyilu.gov.cn/qwyw/qwfb/1084.htm

Based on the broadband expansion and digital transformation, China deployed its major e-commerce players like the BAT, to encourage e-commerce cooperation and "create a transparent digital economy" in the international ecosystem.[76]

Thirdly, e-Government projects provide a venue for governmental officials to hear voices from the grassroots. China experimented with several e-participation trials to improve transparency during the digital age, from the "Government Online Project" that was established in the early stage, to the recent government petition forums and social media accounts that represent local governments. Scholars demonstrate that the e-Government projects do not simply fulfill window-dressing purposes, but instead have substantial influence on the improvement of government policies.[77] Through analyzing the *Local Leader Message Board* (LLMB), which is a petition forum launched by the central media to allow citizens registering complaints to government leaders in their localities, researchers have found that lower-class citizens from rural districts, who comprised a substantial share of the LLMB petitions, have affected governmental policies, such as the Minimum Living Standard Guarantee Scheme (dibao).[78] Moreover, criteria for censoring these online petitions seem to be more lenient. In an interview researchers conducted with LLMB staff, the staff disclosed that censorship mostly applies to personal attacks on top Chinese authorities and that "99.9% of the petitions are displayed exactly the way they were written."[79]

By discussing three main characteristics of China's cyber sovereignty, this article describes a conventional cyber sovereignty framework: while the Chinese government believes that cyber sovereignty

---

[https://perma.cc/75EC-JYEA].

[76] Winston Ma, *The Digital Silk Road for the Next Billion Users*, MILKEN INST. (June 30, 2018), http://www.milkenreview.org/articles/the-digital-silk-road-for-the-next-billion-users [http://perma.cc/W72T-LUQQ].

[77] See Junyan Jiang, Tianguang Meng & Qing Zhang, *From Internet to Social Safety Net: The Policy Consequences of Online Participation in China, 32*GOVERNANCE 531, (2019).

[78] *Id*. at 534.

[79] *Id*. at 6.

advances national security and conforms to international law, international critics attack such concepts, positing that these concepts exclude international business competition and challenge international standards of human rights. This framework reveals some important perspectives of China's cyber sovereignty, but has its limitations. It confines China's cyber sovereignty to a single authoritative image without addressing how much control China asserts within the principle of cyber sovereignty. This paper will propose a three-layer analysis to showcase the Chinese vision on cyber sovereignty infra in section IV. Before presenting this analysis, however, it is imperative to examine how regulatory apparatuses were transformed with the development of the Internet.

III. The Centralization Of Regulatory Institutions

Common wisdom regarding China's Internet development was that it occurred in three stages: the electric media revolution (1994-2000), the digital media age (2000-2014), and the age of Internet of Things (starting from 2014).[80] Specific landmarks may vary, but the general existence of each stage is largely agreed upon. This section will discuss the three stages, and further illustrate how laws and associated political apparatuses evolved in the different periods. A review of China's Internet history is necessary because it can 1) show how regulatory bodies centralized with the development of the Internet, and 2) analyze the vital differences in the Internet's early development between China and the West. Unlike in the United States, where the Internet's ability to spread knowledge without borders was

[80] This paper sets 2000 and 2014 as years of separation because China embarked on content regulation in 2000 and set up the CAC since 2014. Different sources use other years to mark the three stages. *See*, *e.g.*, Hong Shen, *supra* note 19; Zhou Hanhua (周汉华), *Xijinping Hulianwang Fazhi Sixiang Yanjiu* (习近平互联网法制思想研究) [*On Xijinping's Thoughts of the Internet and Relevant Laws*] 3 ZHONGGUO FAXUE (中国法学) 5, 14 (2017); GIANLUIGI NEGRO, THE INTERNET IN CHINA: FROM INFRASTRUCTURE TO A NASCENT CIVIL SOCIETY, 115 (2017); Wang Rong (王融), *Zhongguo Hulianwang Jianguan Ershinian* (中国互联网监管二十年) [*Twenty Years of Internet Regulation in China*], TENCENT RES. INST. (2017), http://www.tisi.org/4944_58 [http://perma.cc/ZHH4-GKYM].

championed, the main role China assigned to the Internet was to facilitate economic development. This long-standing instrumentalist view of the Internet sheds light on how China balances political stability and economic interoperability through the contemporary notion of cyber sovereignty.

a. An Evolving Conception of the Internet in China

Chinese authorities embraced the Internet as a technological means to promote industrial development when it first arrived in China.[81] An electronic media revolution was launched concomitant with the massive development of industrialization and informationization projects between the 1980s and the 1990s. Especially after the mid-1990s, the arrival of the Internet has promoted communications products and a liberalized market. Chinese authorities understood the Internet as nothing more than an efficient means of communication; great efficiency of transportation promotes great volumes of information traffic, which entails economic restructuring. They saw the Internet as an economically advantaged asset and leveraged policies to spur the development of Information Communication Technologies and National Information Infrastructure ("CNII").[82] With the privatization of telecommunications and the liberalization of the market, construction for network projects became a pillar for the national economy.

During this electric revolution, Chinese leaders paid more attention to the Internet's technological impacts than its socio-cultural impacts.[83] Not only were substantial national investments made in infrastructural

---

[81] See FAY SUDWEEKS & CELIA ROMM, DOING BUSINESS ON THE INTERNET: OPPORTUNITIES AND PITFALLS 238 (2012) (mentioning that Hu Qili, Electronic Minister, pointed out on 14 June 1994 that"[p]romoting information services and integrating them with industrialization will greatly enhance the quality of China's national economy.").

[82] ERIC HARWIT, CHINA'S TELECOMMUNICATIONS REVOLUTION, 45, 38-40 (2006).

[83] Fang Xingdong (方兴东), Zhongguo Hulianwang Zhilimoshi de Yanjin yu Chuangxin (中国互联网模式的演进与创新) [The evolvement and innovation of China's Internet model]3 PUB. GOVERNANCE (公共治理)56, 66 (2016).

construction, legislation was also focused on preserving the security of these infrastructural developments.[84] The safety of the Internet infrastructure and computer information systems is the top priority in cyberspace. Between 1994 and 2000, a series of laws and regulations[85] were promulgated addressing the infrastructural security issue. The first Internet regulation in China, published by the State Council in 1994, designated the Ministry of Public Security to "supervise, inspect and guide security protection" and "investigate online criminal activities."[86] The major goal of this regulation, as Article 1 describes, was to "protect the safety of computer information systems, [and] promote the application and development of computers."[87] Although some provisions[88] mentioned content regulation, scholars tend to understand content regulation at this stage as a digital extension of traditional law and, therefore, as not particularly responsive to the

---

[84] Wang Rong (王融), *supra* note 80.

[85] Including "Measures for Security Protection Administration of the International Networking of Computer Information Networks," "National People's Congress Standing Committee's Decision on Safeguarding Internet Security (全国人民代表大会常务委员会关于维护互联网安全的决定)," Measures on the Management of Internet Information Services (互联网信息服务管理办法)," "Computer Information System Security Protection Ordinance of the People's Congress Standing Committee's Decision on Strengthen the Network Information Protection (全国人民代表大会常务委员会关于加强网络信息保护的决定)," and other rules.

[86] (中华人民共和国计算机信息系统安全保护条例) [Regulations of the People's Republic of China for Safety Protection of Computer Information Systems] (promulgated by the State Council, Feb. 2, 1994), http://lawinfochina.com/display.aspx?lib=law&id=12136&CGid= [https://perma.cc/L538-9UJP].

[87] *Id*. at art. 1.

[88] (音像制品管理条例) [Regulations of the People's Republic of China on the Administration of Audio-Visual Products] (promulgated by the State Council, August 25, 1994, effective Oct. 1, 1994); (电影管理条例) [Regulations on Administration of Film] (promulgated by the State Council, June 19, 1996, effective July 1, 1996), http://www.asianlii.org/cn/legis/cen/laws/roaof382/; (广播电视管理条例) [Regulations on Broadcasting and Television Administration] (promulgated by the State Council, Aug. 11, 1997).

development of the Internet.[89]

The heavy national investment in Internet architecture in the '90s underlies the prosperity of China's Internet commercialization sector entering into the millennium. With the rapid commercialization of Internet-related sectors, Chinese officials expressed their optimism for the Internet's capacity in promoting economic growth.[90] Unlike the single-minded emphasis on physical infrastructure development in the initial stage, the social media stage saw the mushrooming of a variety of Internet services, including social networking, photo sharing, video and microblogging services, and other profit-generating cultural and social products. Instant messaging and communication platforms were among the ones nurtured the most aggressively.

Meanwhile, the content delivered by the Internet began to alarm Chinese authorities. The Internet was no longer merely a delivery service: it started to form and perpetuate public spheres. Guobin Yang argued that the trade economy and government-supported policies have laid the vital conditions for the rise of the public sphere in China.[91] TV shows, online discussion boards, and broadcasting programs with political influences are being accessed nation-wide. Chinese collective identity is arguably being shaped over the Internet with two major forces: cyber-nationalism[92] and grassroots social media resistance.[93] But either applauding the rise of China as the Little Pinks[94] do, or criticizing the local government on issues regarding

---

[89] Wang Rong (王融), *supra* note 80.

[90] *See, e.g.*, YONGMING ZHOU, HISTORICIZING ONLINE POLITICS: TELEGRAPHY, THE INTERNET, AND POLITICAL PARTICIPATION 137 (2006); Yuezhi Zhao, *Caught in The Web, in the Public Interest and the Battle for Control of China's Information Superhighway*, 2 INFO 41 (2000).

[91] Guobin Yang, *The Internet and Civil Society in China: A Preliminary Assessment*, 12 J. CONTEMP. CHINA 453, 473 (2010).

[92] Christopher Hughes, *Nationalism in Chinese Cyberspace,* 13 CAMBRIDGE REV. INT'L AFF. 195, 203 (2000) (suggesting that by far the most popular campaigns in Chinese cyberspace to date have been linked to nationalist themes).

[93] GUOBIN YANG, THE POWER OF THE INTERNET IN CHINA: CITIZEN ACTIVISM ONLINE 28-31 (2009).

[94] The Little Pinks are a unique generation that has witnessed China's economic boom in a peaceful age and growth in the Internet age. Unlike the one-way

migrant workers, their vigorous Internet expressions and offline collective actions potentially inherent, pose challenges to the coercive communication regulation and the authority of governmental propaganda institutions.[95]

In response, the Chinese government implemented censorship mechanisms to cope with this intricate online environment. The year 2000 can be identified as the watershed between the first electric stage and the second social media stage; during this year, China published the first regulation specifically targeted at Internet content.[96] This was preceded by a decision[97] issued by the Standing Committee of the National People's Congress which included ideological security more noticeably than the infrastructural construction it emphasized in the previous stage. China gradually published regulations in the forms of "stipulations" ("Guiding"), "management measures" ("Guanli Banfa"), and "notices" ("Tongzhi"), which censor "subversive," "harmful," and "obscene" content as "endangering to national security."[98] Internet news publications also began facing higher levels of restriction.[99] Additionally, regulations related to Internet-based commercial activities such as Internet protocols,[100] e-commerce,[101] and public

---

propaganda machine, the Little Pinks are a walking propaganda group that has genuine faith in the Central Committee of the Communist Party of China (CCP).

[95] Gary King, Jennifer Pan & Margaret Roberts, *How Censorship in China Allows Government Criticism but Silences Collective Expression,* 107 AM. POL. SCI. REV. 1, 2 (2013).

[96] (互联网信息服务管理办法) [Regulation on Internet Information Service of the People's Republic of China] (promulgated by the State Council, Sep. 25, 2000).

[97] (全国人民代表大会常务委员会关于维护互联网安全的决定) [Decision of the Standing Committee of the National People's Congress Regarding Safeguarding Internet Safety] (promulgated by the Standing Committee of the National People's Congress, Dec. 28, 2009), http://www.cac.gov.cn/2000-12/29/c_133158942.htm [https://perma.cc/UMF6-H6S9].

[98] YUEZHI ZHAO, COMMUNICATION IN CHINA 28 (2008).

[99] (互联网站从事登载新闻业务管理暂行规定) [Interim Provisions of the Information Office of the State Council and the Ministry of Information Industry on the Administration of Internet Websites' Engaging in News Publication Services], (promulgated by the State Council, Nov. 17, 2000).

[100] Measures, *supra* note 23.

health[102] were promulgated in response to the staggering growth of Internet applications.

Moving into the current age of Internet of Things ("IoT"), the Internet has allowed an explosive expansion of applications with a higher level of digital penetration; the e-commerce sector experienced exponential growth, from less than 1% of the global e-commerce market to 42% in ten years.[103] Communication platforms have equipped consumers not only with a place to chat, but also a hub for education, information services, entertainment, e-commerce, and social interactions. The number of financial technology unicorns in China is growing competitively in the global market with their active exploration of financial areas including consumer finance, online personal financial investment, online insurance, and so on. The Internet economy has expanded from building telecommunication networks in the previous stage to proprietary platforms.[104] Cyberspace became a unique ecological field inhabited by national military missions, traditional offline industries, high-tech innovation businesses, with all existing previous stages embedded.

Like the two previous stages, the way the Chinese government

---

[101] (财政部关于印发《互联网销售彩票管理暂行办法》的通知) [Notice of the Ministry of Finance on Issuing the Interim Measures for the Administration of Sales of Lottery via Internet], (promulgated by Ministry of Finance, Sep. 26, 2010); (国家食品药品监督管理局关于加强互联网药品信息服务和互联网药品交易监督管理工作的通知)[Notice of the State Food and Drug Administration about Strengthening the Supervision and Administration over the Drug Information Services on the Internet and Drug Transaction Services on the Internet] (promulgated by the State Food and Drug Administration, Aug. 22, 2006).

[102] (互联网医疗保健信息服务管理办法) [Administrative Measures for Internet Medical and Health Information Services] (promulgated by Ministry of Health, May. 1, 2009, effective July 1, 2009).

[103] Rob Smith, *42% Of Global E-Commerce Is Happening in China. Here's Why*, WORLD ECON. F. (April 10, 2018), https://www.weforum.org/agenda/2018/04/42-of-global-e-commerce-is-happening-in-china-heres-why/ [https://perma.cc/DZ7F-PDQV].

[104] Jun Xia, *Convergence and Liberalization in China's ICT Sector: New Market and New Ecosystem,* 40 TELECOMM.POL'Y 81, 82-84 (2016).

responded to technological change has transformed along with the development of the technology itself. In response to the booming market, the Internet was liberalized, with the government showing tolerance, which allowed digital companies some space to experiment before enacting laws and regulations. However, being supportive does not mean the authorities were satisfied with the fact that there was only one law[105] designed for the Internet until 2014. The Chinese authorities understood the Internet space as a novel and separated domain: a political, military, and ideological battlefield as well as a booster for economic growth. Cyberspace is the "fifth domain" after Land, Sea, Air, and Space, which calls for rigorous regulations.[106] China further publishes various administrative laws ("Xingzheng Fagui"), normative documents ("Guifanxing Wenjian"), and departmental rules ("Bumen Guiding") to mediate Internet business activity[107] and relevant media publicity.[108] These strict regulations and measures reflected the fact that China has been paying particular attention to cyber security and content regulation in order to preserve the operations relied on in the ecosystem. This article closely investigates these regulations *infra* in

---

[105] Zhonghua Renmin Gongheguo Dianzi Qianming Fa (中华人民共和国电子签名法) [Law of the People's Republic of China on Electronic Signature], (promulgated by the Standing Comm. Nat'l People's Cong., Apr. 1, 2005).

[106] OFFICE OF THE CENTRAL LEADING GROUP FOR CYBERSPACE, NATIONAL CYBERSPACE SECURITY STRATEGY PART I 182 (2018) ("Cyberspace has become a new area for important human activity of equal importance to land, sea, air and space, state sovereignty has extended and stretched into cyberspace, sovereignty in cyberspace has become an important component part of state sovereignty.").

[107] *See, e.g.*, (外国机构在中国境内提供金融信息服务管理规定) [Provisions on Administration of Provision of Financial Information Services in China by Foreign Institutions] (promulgated by the State Council Information Office, Ministry of Commerce and State Administration for Industry and Commerce, Apr. 30, 2009, effective June 1, 2009); (规范互联网信息服务市场秩序若干规定) [Several Provisions on Regulating the Market Order of Internet Information Services] (promulgated by the Ministry of Industry and Information Technology, Dec. 29, 2011, effective Mar. 15, 2012).

[108] (互联网新闻信息服务管理规定) [Provisions for the Administration of Internet News Information Services] (promulgated by the Cyberspace Administration of China, May 2, 2017, effective June 1, 2017).

Section IV.

b. The Problem of "Nine Dragons Tamed the Flood"

Even as laws were being promulgated, an overarching supervisory body was missing.[109] Before 1998, regulatory frameworks were mainly oriented to the protection of cyber security on the infrastructural level by four sets of state apparatus: the Ministry of Posts and Telecommunications ("MPT"), the Ministry of Electronics Industry ("MEI"), the State Education Commission ("SEC"), and the Chinese Academy of Sciences ("CAS").[110] They were functioning together to represent decision-making on a national level. Additionally, other Ministries and departments managed Internet-related operations within each traditional sector. For instance, although the State Administration of Press and Publication did not share executive power with those four organs, it was responsible for managing Internet-publishing newspapers and magazines.[111]

Scholars pointed out two major problems with the bureaucratic framework. First, bureaucratic cooperation among government Ministries was observed to be inefficient. Milton Mueller and Zixiang

---

[109] The supervisory function was designated to non-exclusive governmental entities. For example, relevant laws granted the Ministry of Public Security the supervising duties and the office of Leading Group for Information Technology Advancement in 1994 and 1998 respectively. See State Council, (中华人民共和国计算系统安全保护条例) [The Regulations of the People's Republic of China for the Safety Protection of Computer Information Systems] (promulgated by the State Council, Feb. 18, 1994), art. 17, and (中华人民共和国计算机信息网络国际联网管理暂行规定实施办法) [Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China] (promulgated by the State Council, Feb. 13, 1998), art. 5.

[110] (中华人民共和国计算机信息网络国际联网管理暂行规定) [Interim Regulations of the People's Republic of China on Management of International networking of Computer Information] (promulgated by the State Council, May. 20, 1997), art. 7.

[111] *New Regulations on Newspapers and Magazines Go Into Effect December 1*, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA (Jan. 4, 2006), https://www.cecc.gov/publications/commission-analysis/new-regulations-on-newspapers-and-magazines-go-into-effect-december [https://perma.cc/DAR3-BZ79].

Tan identified the MPT's loss of control over telecommunications policy early on, when its proposal to draft a telecommunications law in consultation with other Ministries was quashed in 1995.[112] They observed that "the MPT has never been able to get out of the stage of producing drafts; other Ministries, notably MEI, keep vetoing them."[113] Scholars also noted that the rivalry between the MPT and MEI "had become intense" and "services provided by the two government agencies almost completely overlapped." [114] Some attributed this phenomenon to China's administrative structure and general institutional environment.[115] They suggested that due to the self-reliance within each ministry, "department heads had every incentive to expand their own empires and little incentive to contract out for services that could be provided by others."[116]

The second problem was that Internet infrastructure issues usually went beyond the capacity of those four state entities. For example, when the rivalry between the MPT and MEI bogged down in stalemate, the chief administrative authority, China's State Council, was often expected to step in and mediate disputes. The power to negotiate key national plans was limited and therefore often escalated to political levels above the MPT due to "the importance attached to the information superhighway."[117] The first problem—the failure to confer within the four governmental entities—revealed the weakness inside and triggered the second problem, which required opinions from a more centralized entity outside.

Stepping into the digital media age, China recognized the weakness of this dispersed institutional structure and started to centralize the media system by spinning off governmental organs regulating the Internet. The National Informationization Leading Group, founded in 2001, was the first Internet-related Leading Group operated under the directives

---

[112] MILTON MUELLER & ZIXIANG TAN, CHINA IN THE INFORMATION AGE: TELECOMMUNICATIONS AND THE DILEMMA OF REFORM 61-62 (1997).
[113] *Id*. at 62.
[114] SUDWEEKS & ROMM, *supra* note 81, at 242.
[115] MUELLER & TAN, *supra* note 112.
[116] *Id*. at 47.
[117] *Id*. at 54.

of the Party, compared to previous leading groups organized by the State Council. This bureaucratic upgrade allowed the government to conduct top-down administrative orders more directly. Moreover, in 1998, the MPT and the MEI were merged into a newly designed Ministry of Information Industry ("MII") to "reduce the fragmentation of China's information industry."[118] The new department mainly administered industry and commerce relevant to the Internet. In 2008, the new Ministry of Information Industry and Technology ("MIIT") was established to replace and continue the functions of the MII and the Information Office of the State Council. In 2011, China set up the State Internet Information Office ("SIIO"), which is responsible for managing Internet content. The SIIO is the original form of the super-office Cyberspace Administration of China ("CAC"). The MIIT and the SIIO worked together with the Ministry of Public Security, which regulates online criminal activities,[119] constituting three major forces which empower China's top leaders to oversee the Chinese cyberspace. This bureaucratic reshuffling not only reflects a deeper level of centralization, it also implies that Internet regulation at this stage mainly focused on the enterprise units and political stability.

The white paper *Internet in China* characterizes the Internet as "an engine promoting the economic development of China."[120] National plans have set the goal of "using IT to propel industrialization" and "pushing forward national economic informationization by vigorous development of the Internet industry."[121] Exponential growth in Internet penetration accelerated the online entertainment industry such as online games, music downloads, and news updates. Driven by market pressure, the MII promulgated regulations regarding wireless networks, information goods, and commodification trading through the Internet.

---

[118] NEGRO, *supra* note 80, at 26.

[119] (计算机信息网络国际联网安全保护管理办法) [Computer Information Network and Internet Security, Protection and Management Regulations] (promulgated by Ministry of Public Security, Dec. 11, 1997, effective Dec. 30, 1997), art. 3.

[120] INFO. OFFICE OF THE STATE COUNCIL OF CHINA, *supra* note 4, at 4.

[121] *Id*. at 2.

Increasing concerns about political and ideological stability were reflected by the creation of new regulatory departments that were required to stake out and censor sensitive Internet content. Multiple traditional agencies designed relevant branches that were given specific purview over Internet content regulation. For instance, the State Council General Office launched the Internet Information Management Bureau in early 2000, which was responsible for coordinating national Internet news publication.[122]

Previous problems in cooperation extended to these new entities. That is, the assignment of responsibility to regulatory bodies was fragmented by sector, but functionally overlapping. As such, conflicts between Ministries had become increasingly intense since the establishment of the MII.[123] For instance, Jack Qiu noted that the core of China's media control system was steered by stakeholders who uphold Leninist principles and "may not think in line with MII technocrats."[124] Unlike the MII, some core agencies such as the CCP Central Propaganda Department, State Council Information Office, Ministry of Public Security ("MPS"), State Secrecy Bureau ("SSB"), and the People's Liberation Army ("PLA") prioritize the promotion of a positive image of CCP leaders and a harmonious China over developing the national economy.[125] Departments following different lodestars could result in compromised efficiency. The Chinese named this phenomenon "Nine Dragons Tamed the Flood;" many dragons working collaboratively could manage the flood, but in the end, they failed due to inefficient cooperation.[126]

A case involving an imported video game illustrated this dilemma.[127]

---

[122] Yuezhi Zhao, *The State, the Market, and Media Control in China*, *in* WHO OWNS THE MEDIA: GLOBAL TRENDS AND LOAL RESISTANCE 179, 180 (Pradip Thomas & Zohram Nain ed., 2004).
[123] NEGRO, *supra* note 80.
[124] Jack Qiu, The Internet in China: Data and Issue, 1, 11 (Oct. 1, 2003) (unpublished manuscript).
[125] *Id*.
[126] YA-WEN LEI, THE CONTENTIOUS PUBLIC SPHERE: LAW, MEDIA, AND AUTHORITARIAN RULE IN CHINA, 175 (2017).
[127] 当"魔兽"遇上"行政审批," 网络游戏到底归谁管？[*When "Warcraft" Meets*

The Ministry of Culture, State Administration of Press, Publication, Radio, Film and Television ("SARFT"), and General Administration of Press and Publication all directly supervise the import of foreign Internet video games. However, their disagreements about importing the video game *World of Warcraft* remain unresolved. On one hand, the Ministry of Culture issued a provision in 2003, Article 15 of which stipulated that "the import of Internet cultural products shall be conducted by operational Internet cultural entities which have obtained an Internet Culture Business Permit issued the cultural administrative departments."[128] On the other hand, in 2004, the SARFT hosted a game management and importation workshop to discuss whether to publish "World of Warcraft." It published a series of laws written to protect minors from addiction to video games, to regulate gambling with video games, and to publish Chinese ethical video games.[129] The ill-functioned, overlapping role was inimical to the importing process.

Once again, the State Council played the role of mediator. It published a notice[130] which transferred the functions of "animation and network

---

"Administrative Approval," who cares about online games?], TMT POST (Jun. 6, 2016), http://www.tmtpost.com/1901818.html [https://perma.cc/94ZT-MVQV].

[128] Hùliánwǎng wénhuà guǎnlǐ zhàn háng guīdìng (互联网文化管理暂行规定) [Interim Provisions on the Administration of Internet Culture] (promulgated by Ministry of Culture, May 10, 2003, effective July 1, 2003).

[129] *See* Guānyú shíshī "zhōngguó mínzú wǎngluò yóuxì chūbǎn gōngchéng" de tōngzhī (关于实施"中国民族网络游戏出版工程"的通知) [Notice Regarding the Implementation of the Chinese Nationality Online Game Publication Project], (issued by SAPPRFT, Aug. 3, 2004); Guānyú bǎohù wèi chéngnián rén shēnglǐ jiànkāng shíshī wǎngluò yóuxì fáng chénmí xìtǒng de tōngzhī (关于保护未成年人身心健康实施网络游戏防沉迷系统的通知) [Notice on Protecting the Physical and Mental Health of Minors and Implementing the Online Game Anti-addiction System], (promulgated by SAPPRFT, MIIT and six other departments of the State Council, Apr. 13, 2007).

[130] Guówùyuàn bàngōng tīng guānyú yìnfā wénhuà bù zhǔyào zhízé nèi shè jīgòu hé rényuán biānzhì guīdìng de tōngzhī (国务院办公厅关于印发文化部主要职责内设机构和人员编制规定的通知) [Notice of the General Office of the State Council on Issuing the Provisions on the Main Functions, Internal Bodies and Staffing of the Ministry of Culture] (promulgated by the General Office of the State Council, July

game administration and related industrial planning, industrial bases, project construction, trade fairs and market supervision of the SARFT" to the Ministry of Culture, but not the required pre-approval for the online publishing of network games. The pre-approval for publishing network games was reserved for the SARFT.[131]

These notices did not seem to settle the dispute. After obtaining the green light from the Ministry of Culture, but not from the SARFT, "World of Warcraft" was launched by NetEase, one of the largest websites in China. The SARFT expressly announced that without pre-approval for publishing network games, it was not legitimate to launch the game simply based on permission from the Ministry of Culture. In the end, *World of Warcraft* resumed operation several days after "website maintenance." It is not publicly known how NetEase officers managed to persuade the SARFT.

c. The Birth of the Cyberspace Administration of China

After the chaotic events created by the dragon problem, power consolidation reached its pinnacle with the launch of Cyberspace Administration of China ("CAC"), also known as the Office of the Central Cyberspace Affairs Commission, in 2014. Cyber sovereignty was born at a time when the Internet industry exhibited increasing technological complexity and challenges, which contributed to the consolidation of legislative and executive power into one super-office, the CAC. This article analyzes two aspects of the CAC. First, unlike state-led organizations in the electric age in which authorities' attention was pinpointed on a single focal area of infrastructural

---

11, 2008).

[131] *See generally* Guówùyuàn bàngōng tīng guānyú yìnfā guójiā xīnwén chūbǎn zǒng shǔ (guójiā bǎnquán jú) zhǔyào zhízé nèi shè jīgòu hé rényuán biānzhì guīdìng de tōngzhī (国务院办公厅关于印发国家新闻出版总署(国家版权局)主要职责内设机构和人员编制规定的通知) [Notice of the General Office of the State Council on Printing and Distributing the Provisions on the Main Functions and Institutions of the State Administration of Press and Publication (National Copyright Administration)] (promulgated by the General Office of the State Council, July 11, 2008).

development, and equally unlike other central leading groups in the social media age who employed multi-dimensional regulation, for the first time, the CAC expanded its regulation into various explosively growing sectors and encompassed a wide range of regulatory areas. Second, the CAC is entitled to an unprecedented power to coordinate among other bureaucratic organizations, which provides an institutional environment that can resolve the "Nine Dragon Tamed the Flood" problem.

The Central Leading Group for Cybersecurity and Informatization, renamed as the Office of the Central Cyberspace Affairs Commission in 2018, is the most recently refurbished central "Leading Group" designed for Internet development. However, it is not the first. During the initial infrastructural development stage, the State Council established the first state organization in charge of the Internet in 1982: the "Leading Group on Computers and Large-Scale Integrated Circuits," which was led by former Vice Prime Minister, Wan Li. To underline THIS unified leadership, in 1984 the State Council decided to upgrade the organization to the "leading group office of the rejuvenation of [the]electronic information industry," with the primary responsibility of steering nationwide work on infrastructural development. Shifting into China's modernization and industrialization age, the "State Council Informatization Leading Group" and "National Informatization Leading Group" were established to supplant their predecessors in 1999 and 2001, respectively. As their names signify, their primary responsibilities included generating policy proposals and coordinating strategic implementation for China's informatization security and economic development. Therefore, for the issuance of significant policies relevant to the authority of Ministries and committees, various temporary organizations like "leading groups" were established to operate pertinent issues or policies.[132] Every time the key area of Internet development shifted - from physical circuits to infrastructural development, or from electronic information industry to informatization - we not only see a further leadership consolidation,

[132] *See* ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD REVIEW OF INNOVATION POLICY: CHINA (2008).

but also a shift in policymaker focus.

Unlike previous leading groups which mainly undertook techno-infrastructure and economic perspectives, the CAC committed itself to newly-refined responsibilities that encompass duties performed by previous ones, such as infrastructure security, online content regulation, and new areas like e-commerce and data protection.[133] The broad range of responsibilities incorporating related sectors that never appeared in cyberspace until the social media age reflect the fact that Chinese authorities have expanded their understanding of the Internet. The Internet is no longer simply a technological tunnel to deliver information; Chinese officials have started to identify the Internet as a technology whose content can be altered by influencing the physical tunnel.[134] The reason why content regulation did not appear until the birth of CAC is not because government officials never intended to build a centralized governmental entity; it is because the formation of each Central Leading Group is reflective of the Internet's trend towards social development. The dynamics of e-commerce, online activism, and content regulation were not adequately developed to cross over by the governmental officials until the age of Internet of Things.

The CAC's second feature is its unprecedented authority in coordinating state institutions. Compared to other Leading Groups, the CAC is more centralized. If necessary, the CAC is able to coordinate government entities, such as the National People's Congress, the Central Committee of the Communist Party, and other Ministries; previously, this was difficult to accomplish. The CAC did not replace the dragons; relevant departments still manage and supervise their online practices. Rather, the CAC functions to coordinate across

---

[133] Weishan Miao &Wei Lei, *Policy Review: The Cyberspace Administration of China,* 12 GLOBAL MEDIA AND COMM. 337, 338 (2016).

[134] Marshall McLuhan coined the phrase "the medium is the message," which means the nature of the medium can alter the content being transported within the medium. MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN PART I, 7 (1964). In this regard, the Chinese authorities started being aware of how the physical tunnel of the Internet started to transform activities conducted through the Internet.

multiple government entities. At the helm of President Xi Jinping, this top-level supra-ministerial regulatory body primarily oversees Chinese cyberspace operations and executes policies. The *Cyber Security Law* ("CSL") was hitherto the most significant law it has promulgated.[135]

The CAC's consolidating power is authorized by Article 8 of the Cyber Security Law. Article 8 stipulates that "the national cyberspace administration shall be responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration." As for the Nine Dragons, the State Council's telecommunications department, public security departments, and other relevant authorities mentioned before, "shall be responsible for cybersecurity protection, supervision and administration within the scope of their respective functions in accordance with the provisions of this Law and other relevant laws and administrative regulations."[136] Other legal documents and official opinions underline that the CAC performs with a uniform function and an authoritative work mechanism "on a centralized basis."[137]

Although the CAC has been given unprecedented oversight power, Ministries and departments are still the main administrative bodies

---

[135] Cybersecurity Law, *supra* note 22.

[136] *Id*. at art. 8.

[137] Zhōngyāng wǎngluò ānquán hé xìnxī huà lǐngdǎo xiǎozǔ bàngōngshì, guójiā zhìliàng jiāndū jiǎnyàn jiǎnyì zǒngjú, guójiā biāozhǔnhuà guǎnlǐ wěiyuánhuì guānyú jiāqiáng guójiā wǎngluò ānquán biāozhǔnhuà de ruògān yìjiàn (中央网络安全和信息化领导小组办公室、国家质量监督检验检疫总局、国家标准化管理委员会关于加强国家网络安全标准化的若干意见) [Several Opinions of the Office of the Central Leading Group for Cyberspace Affairs, General Administration of Quality Supervision, Inspection and Quarantine and the Standardization Administration of the People's Republic of China on Strengthening National Cybersecurity Standardization Work] (promulgated by the Office of the Central Leading Group for Cyberspace Affairs, Aug. 12, 2016) (suggesting that "[a] uniform and authoritative work mechanism of national standards shall be established. The cybersecurity standardization work shall adhere to uniform planning and deployment… and the support of relevant competent cybersecurity departments, uniformly undertake the technical aspects of national cybersecurity standards on a centralized basis, and uniformly organize the application in relation to such standards.").

performing tasks in relevant sectors.[138] The next section will apply Benckler's framework of the three-layer principle, which analyzes how administrative bodies regulate based on the physical layer, the logical layer, and the content layer.

IV. Reconceptualizing Chinese Cyber Sovereignty: A Three-Area Analysis

Yochai Benkler developed a three-layer model of Internet architecture. Fundamental Internet infrastructures operate at the physical layer, software servers and TCP/IP Protocols and standards make up the logical layer, and data and content transactions occupy the content layer.[139] This article analyzes the CSL and its supporting explanatory documents through the lens of how China wields cyber sovereignty on each layer in the age of Internet of Things. It argues that through installing hefty responsibilities on critical network operators to cooperate and to defend cyber-attacks, China intends to gain network security at the physical level. Based on its persistent efforts to terrorize cyberspace, China tries to tout the idea of cyber sovereignty and the multilateral model to the international community at the logical layer. Finally, for the content layer, although China allows Internet content providers to make occasional violations of the law through the administrative development of the "interview mechanism," central control of online content production to ensure information sovereignty demonstrates a strong incentive to cement political stability. In short, cyber sovereignty is the combination of network security at the physical layer, the multilateral model at the logical layer, and information sovereignty at the content layer.

---

[138] Cybersecurity Law, *supra* note 22, at art. 8 (stating that "[t]he national cyberspace administration shall be responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration. The competent telecommunications department of the State Council, public security departments and other relevant authorities shall be responsible for cybersecurity protection, supervision and administration within the scope of their respective functions in accordance with the provisions of this Law and other relevant laws and administrative regulations.").

[139] Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 848 (2004).

a. Infrastructural Perspectives of Cyber Sovereignty

Technological infrastructure, like a data center or root server, operates at the physical layer. As such, technological infrastructure is localized at one place - For instance, if Microsoft sets up a data center in Mainland China, this data center cannot go elsewhere. This physical exclusivity entails territory sovereignty.[140] The *Tallinn Manual 2.0* characterizes the physical layer of cyberspace as "self-evidently" confined to states' sovereignty.[141] This layer is the only concrete level that people can see and touch; it includes the copper wire, optical cable, satellite facilities, and other technical components that information flows rely upon. This section will emphasize China's efforts to protect the physical layer, maintaining technological independence and territorializing critical infrastructure. Further, it will introduce how China might spread censorship overseas through DNS cache pollution and building Internet infrastructure for developing countries–which raises doubts in the international community.

i. Strict Regulation of Cyber Infrastructure

Because the physical layer is the fundamental foundation of the logical and content layers, attacks on the physical layer are pervasive phenomena that could result in significant consequences for the nonphysical network. The 2010 Stuxnet computer virus, for example, exploited the vulnerability of Iran's nuclear enrichment facilities. The 2012 Flame malware collected private data, and the 2017 WannaCry ransomware worm invaded high-profile national systems. All of these examples underline the vulnerability of cyber infrastructure. Many countries prioritize technological independence at the physical layer as their foundational approach to prevent the paralysis of digital

---

[140] RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010); Stephen Dycus, *Congress's Role in Cyber Warfare,* 4 J. NAT'L SECURITY L. & POL'Y 155, 165 (2010).

[141] MICHAEL N. SCHMITT ET AL., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Cambridge Univ. Press, 2013).

infrastructure, especially for critical infrastructure.

At the initial stage in the 1990s, China's cyber infrastructure was not as well-developed as other countries. Chinese leaders were acutely aware that the unadorned national network infrastructure, especially in critical fields, overly relied on foreign imports.[142] As such, critical infrastructure has occupied a central spot in ensuring security within China's cybersecurity policy. Early on, legal documents generally held that computer security should emphasize "the maintenance of the safety of computer information systems in such important fields as State affairs, economic development, national defense and top science and technology." [143] Nowadays, President Xi pointed out that "[i]nfrastructural development in key fields such as finance, energy, electric power, communication, and transportation are the neural centers of cyber security."[144] The CSL identifies Critical Information Infrastructure ("CII") as vital to "state security, the national economy and the people's livelihood and public interest."[145] China has started making significant strides to design independent Internet architecture. Additionally, extensive national plans encompassing a variety of fields regarding core Internet infrastructure were intensively released.[146]

---

[142] SCOTT WARREN HAROLD, ASTRID STUTH CEVALLOS & MARTIN C. LIBICKI, GETTING TO YES WITH CHINA IN CYBERSPACE 69 (2019).

[143] *See, e.g.*, Zhōnghuá rénmín gònghéguó jìsuànjī xìnxī xìtǒng ānquán bǎohù tiáolì (中华人民共和国计算机信息系统安全保护条例) [Regulations of the People's Republic of China on Computer Information System Security Protection] (promulgated by State Council of the People's Republic of China, Feb. 18, 1994), Article IV.

[144] *Communist Chinese Fundamentals: Strategic Thinking of Network Power*, RED DRAGON 1949 (Jan. 2, 2019), https://reddragon1949.com/chinas-informatization-中國信息化/communist-chinese-cyber-fundamentals-strategic-thinking-of-network-power-共產主義中國網絡基礎：網絡/ [https://perma.cc/7BX9-FY3Q].

[145] Cybersecurity Law, *supra* note 22, at art. 31.

[146] For example, the Outline of National Informatization Development Strategy aims to build core technologies "to create a leading, 'secure and controllable' core technology system." USITO, STATE COUNCIL RELEASED AN OUTLINE OF THE NATIONAL INFORMATION DEVELOPMENT STRATEGY (2016), http://www.usito.org/news/state-council-released-outline-national-informatization-development-strategy. "China Manufacturing 2025 Plan" envisions domestically manufactured core components and key basic materials will reach 40 and 70 percent

The legislation protects critical information infrastructure, particularly cyber-attack inspection. In 2017, China launched a nationwide inspection of key network infrastructures such as finance, energy, electric power, communication, and transportation for the first time. Policy foundations for this inspection can be found in the CSL. The CSL establishes a systematic responsibility framework for the national cyberspace administration, for the departments in charge of critical information infrastructure security protection, and for CII operators. The CSL imposes mandatory testing and certification of computer equipment. Specifically, Article 21 and Article 34 prescribe ten security protection obligations for the critical information infrastructure operators "to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified."[147] Article 38 also compels CII operators to "conduct detection and assessment of their cybersecurity and potential risks [to] their own or entrust cybersecurity service institutions" and report the results of the assessment to relevant national departments at least once a year.[148] Additionally, other ancillary documents prescribe general network operators' responsibility to the CII operators, including carrying out internal training and drills, formulating cyber incident response plans, monitor the cybersecurity status during daily operation, reporting to associated governmental departments when cybersecurity risks are found, and evaluating and classifying potential risks.[149]

---

by 2020 and 2025, respectively. EUROPEAN UNION CHAMBER OF COMMERCE IN CHINA. CHINA MANUFACTURING 2025: PUTTING INDUSTRIAL POLICY AHEAD OF MARKET FORCES 11 (2017).

[147] Cybersecurity Law, *supra* note 22, at art. 21 & art. 34. The ten security protection obligations are: 1) developing Internet security procedures and determining the persons of responsibility. 2) taking technical measures to prevent network attack, 3) taking technical measures to monitor and record network operation, 4) taking measures of categorization and encryption to protect data,5) performing other obligations as prescribed by laws and administrative regulation, 6) designating persons in charge of security management, 7) conduct cybersecurity education and technical training, 8) making disaster recovery backups of important databases, 9) making emergency responses for cybersecurity incidents. *Id*.

[148] Cybersecurity Law, *supra* note 22, at art. 38.

[149] Paul Triolo, Rogier Creemers & Graham Webster, *China's Ambitious Rules to*

Due to the significant responsibility of CII operators, network operators, especially those of multinational companies, expressed concerns about the scope of what constitutes critical information infrastructure. Further, the vagueness of the law leaves foreign companies in a disadvantaged position. Although the Draft Security Protection Measures for CII listed four criteria to be considered as CII operators, it still leaves the interpretation of the specific scope and precise constitution of critical infrastructure to the government's discretion. [150] The broad definition of "critical information infrastructure operators" would seem to include major multinational corporations that have network infrastructure in China.[151]

China is not the only country to express concerns about American hegemony on Internet infrastructure. Both democratic and non-democratic countries, like Canada and Russia, have shown similar interests in pursuing self-designed core Internet infrastructure. For example, Canadian researchers suggested that "no regular internet user in Canada will be free from exposure to NSA surveillance" due to the lack of trans-Atlantic fiber optic cables.[152] While democratic countries believably propose developing Internet infrastructure "to advance the

---

Secure 'Critical Information Infrastructure', NEW AMERICA (July 14, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/ [https://perma.cc/NU9J-5PT4]; Law-Now, *China Publishes the Draft Security Protection Measures for Critical Information Infrastructure*, CMS (Nov. 7, 2017), https://www.cmslawnow.com/ealerts/2017/07/china-publishes-the-draft-security-protection-measures-for-critical-information-infrastructure?cc_lang=en [https://perma.cc/CSV3-CR6F].

[150] *Another Step Forward Filling in Blanks in the Cyber Security Law or More Questions Than Answers?*, HOGAN LOVELLS (2017), https://www.hoganlovells.com/~/media/hogan-lovells/files/updated-16-oct-a_brief_analysis_of_the_draft_key_information_infrastructure_protection_measures.pdf?la=en.

[151] KPMG CHINA, OVERVIEW OF CHINA'S CYBERSECURITY LAW 5-6 (2017), https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of -cybersecurity-law.pdf.

[152] Andrew Clement, *Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building*, CTR. FOR INT'L GOVERNANCE INNOVATION (Mar. 26, 2018), https://www.cigionline.org/articles/canadian-network-sovereignty [https://perma.cc/TDD7-54PK].

public interest,"[153] China has worked to improve Internet infrastructure with the same purported end, making critics skeptical. Many critics worry that concrete physical infrastructure will fortify state surveillance and censorship mechanisms.[154] As such, this article presents two case studies to argue that, at the physical level, DNS Poisoning and the potential threat to the freedom of the other nations' speech differentiates China from other nations.

ii. DNS Cache Pollution

DNS Poisoning occurs when a user attempts to retrieve the IP address from DNS servers, but encounters a blockage in forwarding the IP address to their computer. When their DNS is polluted, people cannot successfully open webpages. The Great Firewall (GFW) usually prevents domestic access to foreign websites, but has been found to cause collateral damage on an international scale. For example, in 2010, *all* traffic passing through the Beijing-based I-Root DNS were exposed to the risk of being unable to access websites censored by China.[155] For example, Facebook users in the U.S. might be censored if they used a Beijing node. Even though a Beijing node is not the closest node to U.S. Internet users, and thus unlikely, this scenario is not impossible due to the Internet's routing design.[156] Following this incident, research showed that approximately 26 percent of DNS resolvers across 109 countries were polluted.[157] As a result, the Beijing node was temporarily removed from the I-root DNS server in 2010.[158]

---

[153] *Id*. ("A national digital infrastructure strategy for Canada should be based on "network sovereignty" — the long-standing principle that to advance the public interest.").
[154] Jon Fringas, *China's New Internet Backbone Explained: Verified Sources, IPv6 at the Core,* ENGADGET (Nov. 3, 2013), https://www.engadget.com/2013/03/11/chinas-new-internet-backbone-detailed-for-the-public/ [https://perma.cc/NB8W-XCH7].
[155] Robert McMillan, *China's Great Firewall Spreads Overseas*, COMPUTERWORLD (Mar. 25, 2010, 4:19 PM), https://www.computerworld.com/article/2516831/china-s-great-firewall-spreads-overseas.html [https://perma.cc/84PB-NXWJ].
[156] Earl Zmijewski, *Accidentally Importing Censorship*, DYNAMIC DNS (Mar. 30, 2010), https://dyn.com/blog/fouling-the-global-nest/ [https://perma.cc/Y328-8NNV].
[157] Anonymous, *The Collateral Damage of Internet Censorship by DNS Injection,* 42 ACM SIGCOMM COMPUTER COMM. 22, 26-7 (2012).
[158] *Root Sever Plugs China Firewall Leak*, IT PROPORTAL (Mar. 31, 2010),

Similar incidents occurred in 2014 and 2015.[159]

Although the pollution has was seemingly unintentional,[160] China's unique firewall design still has the potential to generate impacts for other nations. Therefore, when China tries to improve Internet infrastructure for national security reasons like western countries, the legitimacy of "advancing the public interest" is compromised by the notorious censorship mechanism and its potential to spread censorship overseas.

At the physical level, publicizing the concept of cyber sovereignty allows China to introduce the importance of technological independence to network security regardless of the character of the state, further advancing its pursuit of technological development at the physical layer. This affords China some legitimacy to explore its Internet physical infrastructure. For example, in January 2018, China Unicom developed the world's first mimic DNS server. China initiated this project in hopes to, per the head of technicians, "effectively prevent various known and unknown attacks."[161] Although China hopes to advance its Internet infrastructure like other countries, the

---

https://www.itproportal.com/2010/03/31/root-server-plugs-china-firewall-leak/ [https://perma.cc/JD2U-TDLU].

[159] Paul Mozur, *China Websites Hit with Disruptions*, WALL STREET J. (Jan. 21, 2014, 9:40 AM), https://blogs.wsj.com/digits/2014/01/21/chinas-sina-baidu-and-other-big-websites-are-hit-with-disruptions/ [https://perma.cc/5ZC4-PFYK]; Zāo DNS tóu dú DDoS gōngjí de fúwùqì píngbì zhōngguó IP (遭 DNS 投毒 DDoS 攻击的服务器屏蔽中国 IP) [DDOS Attacked by DNS Server Blocks Chinese IP], CHINA DIGITAL TIMES (Jan. 23, 2015), https://chinadigitaltimes.net/chinese/2015 [https://perma.cc/W23P-E6SG].

[160] Jaikumar Vijayan, *China Internet Rerouting Likely Accidentals, Says Security Firm*, COMPUTERWORLD (Nov. 19, 2010, 3:15 PM), https://www.computerworld.com/article/2514686/china-internet-rerouting-likely-accidental--says-security-firm.html [https://perma.cc/S88A-HGTB].

[161] Yamei, *World's First mMimic DNS Server Operates in China*, XINHUA NET (Jan. 24, 2018, 1:18 PM), http://www.xinhuanet.com/english/2018-01/24/c_136920666.htm [https://perma.cc/76NR-P9TL]. Wu Jiangxing, a Chinese Academy of Engineering academician and head of the research team said, "[M]imic DNS server is just our first application. The mimic web server, mimic cloud, mimic data center and other network devices will be launched in the future." *Id*.

international community has legitimate concerns regarding the Great Firewall's design.

iii. Beyond Investing in Internet Infrastructure

In 2017, at the opening ceremony of the first Belt and Road International Forum, President Xi announced a digital Silk Road plan as a subset of the Belt and Road Initiative (BRI), which aims to intensify global cooperation in areas of digital economy and artificial intelligence.[162] Over the past two years, China has sent national technology champions to bring advanced IT infrastructure to BRI partner countries, embarking on an estimated $200 billion investment in projects around developing countries who are looking to modernize their Internet infrastructure.[163]

Alongside a wide range of gear and relatively cheap materials, observers pointed out that China also offers information systems, censorship training, and model laws for surveillance.[164] Freedom House describes how since January 2017, Chinese tech giants have built fiber-optic Internet infrastructure and networks in 38 countries and installed AI surveillance programs in 18 countries.[165] These programs will improve the infrastructure base and promote the economic growth of China's BRI partner nations; but, these programs also have the potential to insert backdoor mechanisms that could support propaganda and surveillance activities as well. These concerns are especially relevant when the BRI partners show an interest in

---

[162] Huang Yong, *Construction of Digital Silk Road Lights Up BRI Cooperation*, PEOPLE'S DAILY (April 24, 2019, 9:42 A.M.), http://en.people.cn/n3/2019/0424/c90000-9571418.html [https://perma.cc/A9YE-X98J].
[163] Russell Deeks, *The Digital Silk Road- China's $200 Billion Project*, SCI. FOCUS (Dec. 8, 2018, 6:00 P.M.), https://www.sciencefocus.com/future-technology/the-digital-silk-road-chinas-200-billion-project/ [https://perma.cc/A2EA-ZMYG].
[164] Sally Adee, *The Global Internet is Disintegrating. What Comes Next?*, BBC FUTURE (May 14, 2019, 6:00 PM), http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-next [https://perma.cc/YT2P-L639].
[165] Emily Dreyfuss, *The Internet Became Less Free in 2018. Can we Fight Back?*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/internet-freedom-china-2018/ [https://perma.cc/6LRN-2LNX].

pursuing surveillance. For example, as Tanzanian Deputy Minister for Communications Edwin Ngonyani states, "[i]n America, where most of these platforms originate, they often say freedom must be unlimited, but in our case we must find ways to make sure that while a person is free to say anything there are mechanisms to hold them accountable for what they say."[166] According to Samm Sacks in The Atlantic, Chinese influence helped Tanzania pass a cybercrime law which resembles the Chinese version.[167] In addition, even if some countries are reluctant to adopt censorship tactics, critics argue that Beijing would be able to leverage economic debts to force countries to censor their Internet.[168] Overall, despite the fact that the Chinese officials denied any intention to spread censorship,[169] critics warned that China's control of digital infrastructure projects might require, or at minimum, affect another country's intention to cordon off its social networks.

Other discussions also appear in the literature regarding China's strict regulation at the physical layer, but some are not worth serious attention. For example, in his book, Mueller spent many words discussing how a proposal entitled "DNS Extension for Autonomous Internet (AIP)," which was written by three Chinese engineers, will transform the global Internet into a series of national intranets by creating independent domain name hierarchies and root DNS servers.[170] While this proposal seems to conform to the state-centric multilateral agenda, this proposal is never mentioned by the official state media, and hardly reflects mainstream views of Chinese

---

[166] Asteruius Banzi, *Tanzania: Govt Seeks Chinese Help in Social Media*, ALLAFRICA (Aug. 1, 2017), https://allafrica.com/stories/201708020658.html [https://perma.cc/FE95-WVY2].
[167] Samm Sacks, *Beijing Wants to Rewrite the Rules of the Internet*, ATLANTIC (June 18, 2018), https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/ [https://perma.cc/CMN5-ER44].
[168] *Id*.
[169] James Griffiths, *China is Exporting the Great Firewall as Internet Freedom Declines Around the World*, CNN (Nov. 2, 2018, 2:34 A.M.), https://www.cnn.com/2018/11/01/asia/internet-freedom-china-censorship-intl/index.html [https://perma.cc/WR54-J9DB] (stating that China's Foreign Ministry Spokesman Lu Kang said the findings "are sheer fabrications").
[170] MILTON MUELLER, WILL THE INTERNET FRAGMENT? 36-41 (2017).

scholars.[171] Unrepresentative voices need to be distinguished in order to understand China's cyber strategy at the physical layer.

b. A Multilateral Approach to Cyber Sovereignty

To be on the Internet, the first requirement is to have an Internet Protocol (IP) number. Root servers, or name servers, are responsible for translating an IP address into a name. Root servers are easier to remember, such as Google.com. The root authority, also called Internet Naming and Numbering Authority, is a central authority for assigning IP numbers and administering root domains. The Domain Name System (DNS) and the allocation of IP numbers, then, are of crucial importance for operations at the logical layer. Goldsmith and Wu suggested that the Internet's future rests on the DNS, a "global law without which there would be no Internet."[172] The hierarchical structure of the DNS made it a centralized one as there must only be a single root for the hierarchical name space.[173] The ownership of this single root is of critical importance as it has the power to decide whether to allocate a name within a given domain namespace,[174] affects valuable Internet-related property rights,[175] and has particular political and national security importance.[176] The root authority is currently controlled by a private corporation: the Internet Corporation for Assigned Names and Numbers (ICANN), which also happens to have a contractual obligation to the U.S. Department of Commerce.

In contrast to ICANN's proposition for restricting participation by national governments, and instead of engaging the participation of social sectors, China has been actively advocating for a multilateral model which calls for the principle of equal level of governmental

---

[171] As of June 2019, only three citations of the Chinese version of this proposal could be found.
[172] GOLDSMITH & WU, *supra* note 3, at 168.
[173] *Id*. at 194.
[174] MARTIN CLARK, DATA NETWORKS, IP AND THE INTERNET: PROTOCOLS, DESIGN AND OPERATION 456 (2003).
[175] GOLDSMITH & WU, *supra* note 3, at 31.
[176] LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE 194 (2009).

participation i. In short, China is pushing for a government-driven model of Internet governance. This article, then, argues that China has a strong motivation to challenge the ICANN model by pushing for a government-driven multilateral model in the global Internet governance landscape. To do so, this article outlines the evolution of the multilateral model, and articulates how cyber sovereignty contributes to the promotion of multilateralism.

i. The Rise of a Multilateral Internet Governance Model

As Internet development progressed, disputes arose on how to regulate the logical layer, resulting in two rival cyber-diplomacy regulatory schemes. The U.S. and its Western allies embrace the multi-stakeholder model, which emphasizes engaging a wide range of participation from multiple sectors, especially from the private sector.[177] Participation by national governments in ICANN is restricted and government officials are prohibited from serving on the corporate board of directors.[178] Other countries and world powers, such as Brazil, Russia, India, China and South Africa (BRICS), increasingly express a restive attitude towards America's dominance of such a vital and centralized organization for regulating the Internet.[179] They subscribe to the multilateralism model, which asserts that countries should establish a non-intervention policy regarding cyber regulation.

The late emergence of the multilateral camp was an anti-monopolistic reaction to the existing multi-stakeholder model. Multi-stakeholderism follows the principles of "seeking the private sector's participation in Internet governance," and committing to "advocate for inclusiveness in fora that take up such issues."[180] As Lawrence E. Strickling, U.S. Assistant Secretary of Commerce for Communications and

---

[177] Eichensehr, *supra* note 18, at 330.
[178] ICANN, Board Governance Guidelines, https://www.icann.org/resources/pages/overnance/guidelines-en.
[179] Eichensehr, *supra* note 18, at 321.
[180] EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE, PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011).

Information, said, "the steadfast policy of the U.S. government has been to promote these values of inclusion and participation through our support for the multistakeholder process."[181] However, developing countries complained that the inclusiveness Strickling proudly underlines seems to only include dominant ICT carriers and other non-state sectors. These actors are usually composed of U.S. actors and cater to U.S. interests.[182] Important non-governmental participants and decision-makers within ICANN were predominantly American during the cyber-utopian age. Further, globally competitive private sector actors certainly do not favor most of the developing countries, which comprise the majority of the multilateral camp. In this case, the multilateralists worry that the Internet would be controlled by strong business operators like Alibaba and Apple, leaving the development of Internet standards in transport, routing and security, and managing the TCP/IP protocol in the hands of American-dominated non-governmental sectors like the Internet Engineering Task Force (IETF).

The multilateralists also criticize interferences from the U.S. Government, because America openly and repeatedly discourages governmental participation even while representing multi-stakeholderism. This criticism dates back to the birth of ICANN, which has legally remained under contract with the U.S. Commerce Department. Milton Mueller pointed out that, as much as ICANN's managers and its supporters in business and the U.S. government would like to refer to it as a "bottom-up" organization, it is in fact

---

[181] Lawrence E. Strickling, *Keynote Address by Assistant Secretary Strickling at Columbia Institute for Tele-Information*, NAT'L TELECOMM. & INFO. ADMIN. (June 24, 2013), https://www.ntia.doc.gov/speechtestimony/2013/keynote-address-assistant-secretary-strickling-columbia-institute-tele-informat [https://perma.cc/J8X3-FVT7].

[182] Eichensehr, *supra* note 18, at 347 ("Although the United States supports the multistakeholder model at least in part for freedom of expression reasons, the bottom-up governance model also serves U.S. interests because many of the nongovernmental voices that the model amplifies, including technology companies and nongovernmental actors, have ties to the United States or share its values."); Sandeep Joshi, *India to Push for Freeing Internet from U.S. Control*, HINDU (Dec. 7, 2013, 11:55 PM), http://www.thehindu.com/sci-tech/technology/internet/india-to-push-for-freeing-internet-from-%20us-control/article5434095.ece [https://perma.cc/DQ42-FSAF].

exclusively beholden to a single sovereign, the U.S. government.[183] He questions the decentralization feature of ICANN, which symbolizes the current multi-stakeholderism system, and describes the government intervention from the U.S. as "a new form of centralized control over the Internet and a sharp departure from the earlier Internet's freer, self-governing, and technically neutral administration."[184] Wu and Goldsmith also questioned the sincerity of the U.S. government's discussion about "bottom up governance" and "the Internet community."[185] They suggested that the U.S., "never actually ceded control or either ICANN or the root" and "the physical root, the computer containing the root zone file, remained under the ownership of the United States."[186] Ben Wagner emphasized this towards ICANN, arguing that the primary functions of institutions such as ICANN and the vaunted concept of multi-stakeholderism, are meant to provide "symbolic legitimacy theatre" to the overall Internet governance regime and prevent new Internet regulatory institutions from being created.[187]

Entering 2010, the multilateral model became increasingly popular in the Global South, and a strong competitor to replace the multi-stakeholder model. Multilateralism has, however, been criticized for restraining freedom of expression and top-down control over the regulation of the DNS.[188] These two criticisms were rooted in its state-driven regulatory mechanism: the multilateral model is a traditional governance mechanism whereby governments come together to discuss the coordination of international telecommunications issues. The next section will explore how China exemplified this model and analyze some of its shortcomings.

---

[183] MILTON MUELLER, NETWORKS AND STATES, THE GLOBAL POLITICS OF INTERNET GOVERNANCE 62 (2010).
[184] *Id*. at 64.
[185] *See* GOLDSMITH & WU, *supra* note 3, at 169.
[186] *Id*.
[187] BEN WAGNER, SYMBOLIC POWER AND LEGITIMACY THEATRE: CONSTRUCTING LEGITIMACY IN GLOBAL INTERNET GOVERNANCE 157-74 (2016).
[188] Eichensehr, *supra* note 18.

ii. Aligning Cyber Sovereignty With Multilateralism

The multilateral countries made continuing efforts to propel the transfer of the root authority from ICANN to traditional UN-driven bodies, such as the ITU or the UN Committee on Internet-Related Policy (CIRP), under the belief that the Internet should be governed the same way as other media, like broadcasting and telecommunication tools. Under the multilateral model, the regulatory organization "functions firmly in the hands of the governments in the committee" with advisory groups from technical, business, civil society, and international organization sectors that would "advise and assist" them.[189] This compares to the ICANN model, which gives more weight to civil society and business groups for policy design and has governments perform the advisory role.[190]

As a country which views itself as one of the most important forces on the global stage, China not only strictly controls cyberspace domestically, but also strives to incorporate its understanding of cyber sovereignty into the international system. Binxing Fang, the main architect of the Great Fire Wall project, pointed out that the first of the major objectives for which to advocate cyber sovereignty internationally is to contribute to or enhance China's leading position in international law. [191]

China is a firm advocate for the multilateral model on the international stage. It utilizes cyber sovereignty as a kind of diplomatic language to promote the multilateralist cyber strategy of having state sovereigns control cyberspace, rather than a mixture of non-state actors. There are two explanations for this strategy. First, although Chinese academic technicians played a key role in launching the Internet in the early

---

[189] Milton Mueller, *A United Nations Committee for Internet- Related Policies? A Fair Assessment,* INTERNET GOVERNANCE PROJECT (Oct. 29, 2011), https://www.internetgovernance.org/2011/10/29/a-united-nations-committee-for-internet-related-policies-a-fair-assessment/ [https://perma.cc/YDC3-5ZWR].
[190] JEREMY MALCOLM, MULTI-STAKEHOLDER GOVERNANCE AND THE INTERNET GOVERNANCE FORUM 40-43 (2008).
[191] FANG, *supra* note 74, at 120-24.

days, they did not partake in cyber-utopianism, nor did they have self-governed technical communities to independently run the Internet. The open character of the Internet may liberate information exchange and mobilize social resistance in many cases,[192] but it is still far from the anarchist spirit of cyber-utopianism. As China never implemented the anarchical social value sometimes seen in the Internet, non-governmental forces that enable the operation of multi-stakeholderism are weak. Second, unlike John Parlow, the Chinese government fundamentally does not see excluding government regulation as relevant to building a humane and fair world.[193] Cyber sovereigntists do not recognize universal values; they believe that the "humane and fair world,"[194] includes respecting other states' will to freely choose whether to censor online harmful speech, to control Internet insecurity, and to regulate. It is not a declaration of the independence of the Internet, but a declaration of how the elite tried to impose a liberal imagination on other states.

Unsurprisingly, China is not the only country that espouses the multilateral model. Since the founding of the Shanghai Cooperation Organization in 2009, China has forged a close partnership with Russia in promoting the state-driven internet governance model. They have successfully lobbied for the inclusion of the term "multilateral" into documents at WSIS,[195] regularly held international fora,[196] and released a joint statement on the subject of cyber security issues.[197] The

---

[192] YANG, *supra* note 93.
[193] *See*, *e.g.*, Wu & Ni, *supra* note 11.
[194] John Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/8S52-8XRT].
[195] David Bandurski, *China's Cyber-Diplomacy*, CHINA MEDIA PROJECT (Dec. 21, 2015), http://chinamediaproject.org/2015/12/21/chinas-cyber-diplomacy/ [https://perma.cc/TZF7-XLMJ].
[196] Jack Margolin, *Russia, China, and the Push for "Digital Sovereignty,"* GLOBAL OBSERVATORY (Dec. 2, 2016), https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/ [https://perma.cc/DZT3-GAW3].
[197] Xi Jingping & Vladimir Vladimirovich Putin, *The Joint Statement Between The Presidents of the People's Republic of China and The Russian Federation on Cooperation in Information Space Development,* CHINA DAILY (June 26, 2016, 9:54

central themes of "non-intervention" and "equal government participation" were repeatedly emphasized in their cooperation. For instance, in the "International Code of Conduct for Information Security" that China, Russia, Tajikistan, and Uzbekistan submitted to the UN General Assembly in September 2011, states are required "to reaffirm all States' rights and responsibilities to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage."[198] In another joint statement published in 2016, they reached consensus in "jointly advocating respect to and opposing infringements on every country's sovereignty in information space" and "resist[ing] the interference via information space in other countries' internal affairs, disruption of social order, incitement of inter-ethnic, inter-racial and inter-religious antagonism, and undermining national governance."[199] Their stances and cooperation are bound to face backlash from multi-stakeholders.

A major criticism leveled by Western countries, and by the United States in particular, is that the multilateral entities fail to include non-state perspectives, especially those from the private sector. Assistant Secretary Strickling expressed this reservation in relation to the Washington Council on International Trade (WCIT) process in 2012, noting that, "[o]nly member states will have a vote at the ITU. A treaty conference, such as the WCIT, can never be a true multistakeholder process where all interests are fairly represented."[200] Phil Verveer, the deputy assistant secretary for the Obama State Department, echoed this concern by explaining that "[g]overnmental proposals to expand the ITR's to include centralized control over the Internet through a top-down government approach would put political dealmakers, rather

---

A.M.), http://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm [https://perma.cc/4686-QMJ3].

[198] Timothy Farnsworth, *China and Russia Submit Cyber Proposal*, ARMS CONTROL ASS'N (NOV. 2011), https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal [https://perma.cc/GP7M-UAN2].

[199] Jingping & Putin, *supra* note 197.

[200] Strickling, *supra* note 181.

than innovators and experts, in charge of the future of the Internet."[201] The common wisdom that the Internet is an open place with minimum governmental participation that cyber-utopianists left for the world also underlines this criticism. The early cyber-utopianists have left a legacy of social consciousness that embedded a free and open character within discussion of the Internet, despite the fact that the self-governance plan did not survive its encounter with the U.S. government. This social consciousness later became an intangible yet important asset to the persistent belief in multi-stakeholderism, which openly encourages the participation of non-governmental sectors.

Additionally, the United States and its Western allies worried that China would utilize the language of Internet freedom and sovereignty to justify their own surveillance activities and suppression of free speech. They see installing the concept "equal role," in terms of governmental responsibility, as a precursor to regulating content and weakening the dominating position of civil society and Western-influenced groups in executing Internet policy.[202] In an interview with the *New Yorker*, Prof. Tim Wu characterized China's Internet sovereignty as "a statement of private international law as typically practiced," suggesting that "the big difference is that other countries . . . have a certain respect for the network as a platform for free speech . . . [B]ut China is unique in its lack of respect for the idea of an open Internet."[203]

c. China's Domestic Practices

As China pushes for a greater role for governments in regulating the Internet internationally, it has also been preparing itself to take on such responsibility by experimenting with self-designed architectures domestically. These homegrown architectures are national efforts

---

[201] *International Proposals to Regulate the Internet: Hearing Before the Subcomm. on Commc'n and Tech. of the Comm. on Energy and Commerce*, 112th Cong. 42 (2012).
[202] Eichensehr, *supra* note 18, at 332.
[203] Evan Osnos, *Can China Maintain Sovereignty over the Internet*, NEW YORKER (June 10, 2010), https://www.newyorker.com/news/evan-osnos/can-china-maintain-sovereignty-over-the-internet [https://perma.cc/WA5B-MT3G].

made to prevent future cyber-attacks.

The deployment of the Internet Protocol version 6-based network (IPv6, CNGI-CERNET2) reflected China's ambition to become the leading player in the creation of the next generation of the Internet. China was in a poor position relative to the U.S. at the IP level, due to an address shortage under the current IPv4 system. As such, China published a national plan to boost the Internet development industry, aiming to collect 200 million active users of IPv6 by the end of 2018, with the number set to exceed 500 million by 2020.[204] Compared to the original design of IPv4, which left security out of its design, IPv6 supports end-to-end encryption and is more secure. It is more difficult to attack domain name parsing—which will advance the security of communications between the DNS and IP addresses.

Cyber sovereignty corresponds to the aforementioned cybersecurity concern through the development of sovereign Internet architecture. China has monitored massive cyber-attack incidents in the logical layer, such as malwares, hardware vulnerabilities and content linked to "malicious" IP addresses.[205] The number of attacks has increased, ranging from National Top-Level Domain Name (gTLD) to operations of content delivery network (CDN). However, this legal protection generated international controversies. The draft of "New Domain Name Rules," included Article 37, stipulates that any foreign domain name whose website is hosted in China must be registered with a Chinese domain name registrar.[206] Failure to meet this requirement

---

[204] Tuījìn hùliánwǎng xiéyì dì liù bǎn (IPv6) guīmó bùshǔ xíngdòng jìhuà (推进互联网协议第六版(IPv6)规模部署行动计划) [Action plan for putting the Internet Protocol Version 6 (IPv6)-based Network into Large-scale Use] (promulgated by Central Committee of the Communist Party of China, Nov. 2017).

[205] CNCERT HÙLIÁNWǍNG ĀNQUÁN WĒIXIÉ BÀO (CNCERT 互联网安全威胁报告) [CNCERT INTERNET SECURITY THREAT REPORT] (2016), http://www.cac.gov.cn/wxb_pdf/CNCERTmonthlyreport/2016monthly12.pdf.

[206] Deanna Wong et al., *Towards a Greater Chinese Firewall?: China Issues New Draft Domain Name Rules*, HOGAN LOVELLS (Apr. 14, 2016), http://ehoganlovells.com/rv/ff0026c6507ea55724410f416647a579da6faa4f [https://perma.cc/6JTH-2SKJ].

could result in inaccessibility for mainland users. In response, American Ambassador Daniel Sepulveda and his colleagues published a joint statement, describing this proposal as "forced localization" which would "potentially create new barriers to the free flow of information and commerce across borders and consequently infringe upon internationally recognized commitments on free expression and trade."[207] In the end, Article 37 was deleted when the law was formally enforced.

d. Content Regulation with Chinese Characteristics

Content-layer regulation occupies a central place in China's multi-layered regulatory system. Before the establishment of the CAC, Adam Segal observed that Chinese policymakers, like their Russian counterparts, are more prone to emphasizing "information security" as opposed to America, which understands cyber sovereignty as being more about infrastructure-based security.[208] Information security, or Information sovereignty, implements regulatory scrutiny of the spread of information.[209] Gong Wenxiang described how the concept of information sovereignty began to percolate around 2005, and a majority of Chinese literature proposed information sovereignty as allowing China to resist cultural hegemony and information colonialism. After the CAC launched, content regulation is still the forefront area of these three layers: as of June 2017, the majority of laws and documents it published focus on the content layer.[210]

---

[207] David Taylor & Daniel Madden, *US Government Slams Chinese Domain Name Rules,* LIME GREEN IP NEWS (MAY 30, 2016), https://www.limegreenipnews.com/2016/05/us-government-slams-chinese-domain-name-rules/ [https://perma.cc/MNR8-J782].

[208] Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty* 3 (Hoover Institution, Aegis Paper Series No. 1703, 2017).

[209] Adam Segal, *Chinese Computer Games: Keeping Safe in Cyberspace*, 91 FOREIGN AFF., 4 (2012).

[210] Xuanfeng Ning & Han Wu, *Observations and Perspectives on the 1st Year Implementation of the Cybersecurity Law,* LEXISNEXIS: CHINA LEGAL REV. (2017), https://hk.lexiscn.com/mnl/detail.php?meta_content_id=2206&eng=&crid=a54d7dfb-9105-0e26-fbd4-e1a686337039&prid= [https://perma.cc/2LSA-Q3FE].

i. Censorship and Content Regulation

"Online positive publicity must become bigger and stronger, so that the Party's ideas always become the strongest voice in cyberspace."
-Synthesizing Xi's Cyber Strategic Thinking on Cyberspace, Qiushi[211]

This Section will analyze China's regulation at the content layer by probing into censorship and introducing the interview mechanism for content management since the age of Internet of Things. Although Internet governance has become a pervasive phenomenon, what makes China distinctive is that corresponding laws do not only apply to physical infrastructure located within Chinese territory. Additionally, they include censorship at the content layer that does not share physical exclusivity and fails to meet the criterion of "territorial localization" utilized in common wisdom.

Before the birth of the CAC, a large variety of Ministries incorporated supervising online publications into their general responsibilities, in addition to overseeing traditional fields of publication.[212] However, despite the fact that these Ministries published the early legal documents for online content regulation, the State Council Information Office and the Central Propaganda Department remain the top decision-making authority for establishing laws and policies . Stepping into the age of Internet of Things, public opinion through online content has been seen as of "the utmost importance to propaganda and

---

[211] Elsa Kania, Samm Sacks, Paul Triolo & Graham Webster, *China's Strategic Thinking on Building Power in Cyberspace*, NEW AMERICA (Sep. 25, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/ [https://perma.cc/DS5E-XW2E].

[212] The Ministry of Radio, Film, and Television (MRFT) is responsible for online media release and film production; the Ministry of Culture (MOC) bears the primary responsibility for overseeing cultural-related Internet literacy publication; Other related Ministries, such as the Ministry of Posts and Telecommunications (MPT) and the Ministry of Industry and Information Technology (MIIT) whose primary jobs are not regulating online publication, also assigns the Internet Service Providers (ISPs) the responsibilities to regulate online materials.

ideological work" in the eye of General Secretary Xi.[213] In 2014, the Cyberspace Administration of China (CAC) was officially authorized to be responsible for monitoring and regulating online content publication.[214]

The legal basis for censorship can be found in many laws with similar wording, but Article 15 of the "Regulation on Internet Information Service" Law shows a suitable origin of the definition, with nine scenarios for categorizing which contents "conforms to the law" and which should be censored.[215] As these nine rules established the bottom line for censorship in the content layer, other recent departmental rules adopted them in essentially the same way with different wordings.[216] While these rules may seem too broad to be useful, the judicial interpretation co-released between the Supreme

---

[213] Kania, Sacks, Triolo & Webster, *supra* note 211.

[214] (国务院关于授权国家互联网信息办公室负互联网信息内容管理工作的通知) [Notice of the State Council on charging the Cyberspace Administration of China with the Content Management of Information on the Internet] (promulgated by State Council, Aug. 26, 2014).

[215] (互联网信息服务管理办法) [Regulation on Internet Information Service of the People's Republic of China] (promulgated by the State Council, Sep. 25, 2000). These nine scenarios are: 1) against the Cardinal Principles set forth in the Constitution; 2) detrimental to State security, State secrecy, State power and national unification; 3) detrimental to State honor and interests; 4) instigating ethnic hatred or discrimination and detrimental to national unity; 5) detrimental to State religious policy, propagating heretical or superstitious ideas; 6) disseminating rumors, disrupting social order and stability; 7) disseminating obscenity, pornography, force, brutality and terror or crime-abetting; 8)humiliating slandering others, trespassing the lawful rights and interests of others; 9) other contents forbidden by laws and regulations. *Id*.

[216] See, *e.g*., (信息网络传播权保护条例) [Regulation on the Protection of the Right to Communicate Works to the Public over Information Networks] (promulgated by the State Council, Jan. 30, 2013, effective Mar. 1, 2013), at art. 56; (互联网域名管理办法) [Measures for the Administration of Internet Domain Name] (promulgated by the Ministry of Industry and Information Technology, Aug. 24, 2017, effective Nov. 1, 2017), at art. 28 [hereinafter Measures]; (互联网视听节目服务管理规定) [Provisions on the Administration of Internet Audio-Visual Program Service] (promulgated by the State Council, Aug. 28, 2015), at art. 16.

People's Court and the Supreme People's Procuratorate in 2013 provides some reference.[217]

These nine criteria for content censorship reflect China's pursuit of national and ideological security. At the national level, most censored content addresses the maintenance of public order. China views maintaining social order as the necessary foundation for economic growth, which provides the government with its legitimacy. While democratic countries usually view terrorism as a threat to national security, the Chinese government goes beyond terrorists and includes content that could elicit collective actions as national threats.[218] Guided by a goal of maintaining social order, it represses online information that has the potential to trigger offline collective actions, including even ones that praise the government.[219] At the ideological security level, China censors content detrimental to its international image and deems maintaining "a clear cyberspace" as a valuable source of national political security. Ideological thinking that conflicts with socialist values, which sometimes included Western democratic values, are deemed errant and are not welcomed. With regard to "online rumors, violent video, and other harmful information" that damage the clear cyberspace, the Theoretical Studies Center Group of CAC published accordingly in Qiushi;

> We must . . . steadily control all kinds of major public opinion; dare to grasp, dare to control, and dare to wield the bright sword; refute erroneous ideas in a timely manner" to "prevent mass

---

[217] (最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的规定) [Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Specific Application of Law in the Handling of Defamation Through Information Networks and Other Criminal Cases] (promulgated by the State Council, Sep. 6, 2013).

[218] *Decision of the National People's Congress Standing Committee Regarding Safeguarding Internet Safety*, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA (Dec. 28, 2000), https://www.cecc.gov/resources/legal-provisions/decision-of-the-standing-committee-of-the-national-peoples-congress [https://perma.cc/G9PF-BQCV].

[219] King, Pan, & Roberts, *supra* note 95.

> incidents and public opinion from becoming online ideological patterns and issues.[220]

To clean up these "erroneous ideas," China designed an extensive and technologically sophisticated mechanism of Internet censorship. It demonstrates its ambition and capability for governmental control over Internet communications by featuring explicit techniques such as a keyword filtering mechanism, the enforcement of the Real-Name Registration policy, blocking individuals' access to virtual private networks (VPNs), and implicit techniques such as using algorithms to divert search results.

It is important to point out the three layers do not operate independently of each other. In the age of the Internet of Things, China has started to incorporate standards designed for regulating the physical layer and logical layer to influence the content layer. Scholars have identified the content layer as the layer most susceptible to the strict control of higher layers, but not vice-versa.[221] In other words, squeezing the physical layer or the logical layer will stymie innovation on the content layer, but strict control of the content layer alone hardly has any influence on the basic physical or logical layers. China's legislation reflects this point.

The Cybersecurity Law (CSL) demonstrates China's pursuit of data localization at the content layer through regulating critical infrastructure at the physical layer. Article 37 of the CSL sets the legal basis for the data localization rule and is perhaps the most controversial rule of the CSL. The rule requires full access to stored data within the critical information infrastructure and a security assessment of the data or approval from relevant regulators is necessary before exporting these data aboard.[222] In response to this,

---

[220] Kania, Sacks, Triolo & Webster, *supra* note 211. Qiushi is generally viewed as the governmental mouthpiece who trumpets the government's official policies and ideologies.

[221] ANDREW D. WURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 46 (Routledge-Cavendish, 1st ed. 2007).

[222] Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, DIPLOMAT (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-

which is arguably the broadest scope of data localization in the world, some observers evaluate Article 37 as stressing the importance of protecting the critical infrastructure of major communication industries and setting the foundation for enforcing penalties on organizations and individuals who break into the nation's critical infrastructure.[223] On the other hand, critics have argued that the CSL will "have significant operational and business implications for domestic and international network operators, as well as for suppliers of network products and services."[224] International observers also worry that the CSL allows the theft of foreign clients' data and hampers the development of innovative capabilities. [225] Lance Noble, the Policy and Communications Manager of the European Union Chamber of Commerce in China, warned that uncertainty surrounding the law could make foreign technology firms reluctant to bring their best innovations to China.[226] Researchers have shown that data localization has an economic disadvantage with a negative correlation between data localization and national GDP and investment.[227]

China refined and republished the "Measures for the Administration of Internet Domain Names" in 2017.[228] Article 28 lays out the criterion of

---

need-to-know/ [https://perma.cc/VVV2-82PK].

[223] *The China Cybersecurity Law has been Finalized—Is Your Organization Ready to Comply with the New Law?*, PWC (2017), https://www.pwccn.com/en/issues/cybersecurity-and-privacy/china-cybersecurity-law-2017.html [https://perma.cc/N4XW-SJCC].

[224] Barbara Li, *China' Cyber Security Law: Enforcement Actions are on the Way*, NORTON ROSE FULBRIGHT (Nov. 2017), https://www.nortonrosefulbright.com/en/knowledge/publications/7e835eec/chinas-cyber-security-law-enforcement-actions-are-on-the-way [https://perma.cc/J2L8-42CX].

[225] Andrew Blake, *Chinese Cyber Law Challenged by Tech Titans over Intellectual Property, Security Concerns: Report*, WASH. TIMES (Dec. 2, 2016), https://www.washingtontimes.com/news/2016/dec/2/chinese-cyber-law-challenged-tech-titans-over-inte/ [https://perma.cc/2V2P-VCRA].

[226] Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Firms Guessing*, N.Y. TIMES (May 31, 2017), https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html [https://perma.cc/U8BM-5393].

[227] Matthias Bauer et al., *The Costs of Data Localization: Friendly Fire on Economic Recovery* (Eur. Ctr. Int'l Political. Econ., Occasional Paper 3/2014, 2014), http://hdl.handle.net/10419/174726.

[228] (互联网域名管理办法) ["Measures for the Administration of Internet Domain

Internet content restriction as other previous versions. However, compared to the previous versions published in 2002[229] and 2004,[230] which it replaced, this version added a new rule in addition to the nine scenarios, stating "[n]o domain name registry or domain name registrar may provide services for domain names that contain contents as listed in the preceding paragraph."[231] Article 38 reinforces content control by stipulating that "no domain name skip may be provided for a domain name that contains the contents as listed in paragraph 1 of Article 28 of these Measures."[232] Violators can be charged with a fine of not less than 10,000 yuan nor more than 30,000 yuan.[233] This legal modification illustrates the constraints imposed on domain name service providers: they are no longer only responsible for the content they manufacture, but are now also required to oversee the content manufactured by others who use their services. This extension of responsibility on the logical layer therefore allows China to deepen its control over online content.

Although China placed heavy responsibilities on providers of all sorts, the intervention is a rather complicated task for the platform providers. Intervening in the spread of content which will break the law is a basic requirement. However, they do not only need to intervene; they must also ensure their intervention is on the right track. Published in 2017, a notice regarding Internet comments postings includes the Article 7, which explains that the provider "shall not interfere with public opinions by selectively deleting or recommending comments, among others, for seeking illicit interests based on erroneous value

---

Names" in 2017], https://cnnic.com.cn/PublicS/fwzxxgzcfg/201710/t20171026_69608.htm [https://perma.cc/T9KX-W3YR].

[229] Measures, *supra* note 216.

[230] (中国互联网域名管理办法) [Measures for the Administration of Internet Domain Names of China] (promulgated by Ministry of Industry & Information Technology, Dec. 20, 2004).

[231] Measures, *supra* note 216.

[232] Measures, *supra* note 216, art. 38.

[233] Measures, *supra* note 216, art. 51.

orientation."[234] To be accurate, selective deletion or recommending comments is encouraged, especially for contents which "violate the law," is contrary to the "correct orientation," or sabotages "active and healthy network cultures."[235] Whether such selective deletion or recommendation is lawful is contingent upon whether the value orientation is "erroneous." Similar emphasis on the "correct orientation" is repeatedly included in other "normative documents" published by the CAC, ranging from regulations in response to self-publishing microbloggers[236] and video-makers[237] to professional WeChat subscribed articles.[238] Because of the blurry definition of the "erroneous" idea and difficulties of compliance, the CAC sometimes steps in to supervise service providers when they do not fulfill their censorship mandates. In the next section, this article will discuss the CAC supervision system with an administrative design called "the interview."

ii. The Interview Mechanism

In 2015, the CAC released a normative document which describes the interview mechanism.[239] It requires the CAC or the local Internet

---

[234] (国家互联网信息办公室关于印发《互联网跟帖评论服务管理规定》的通知) [Notice of the Cyberspace Administration of China on Issuing the Provisions on the Administration of Internet Comments Posting Services], at art. 7.

[235] *Id*. (promulgated by the Cyberspace Administration of China, Aug. 23, 2017, effective Oct. 1, 2017), at art. 4.

[236] (微博客信息服务管理规定) [Provisions on the Administration of Microblog Information Services] (promulgated by the Cyberspace Administration of China, Feb. 2, 2018), at art. 5.

[237] (互联网直播服务管理规定) [Provisions on the Administration of Internet Live-Streaming Services] (promulgated by the State Internet Information Office, Nov. 4, 2016), at art. 3.

[238] (互联网用户公众账号信息服务管理规定) [Provisions on the Administration of Internet User Public Account Information Services] (promulgated by the Cyberspace Administration of China on Sep. 7, 2017), at art. 4.

[239] (互联网新闻信息服务单位约谈工作规定) [Provisions on the Interview of Entities Providing Internet News Information Services] (promulgated by the State Internet Information Office on Apr. 28, 2015), at art. 4 (hereinafter Provisions).

Information Office to set up interviews with "entities providing internet news information services" who commit "a serious violation of the law or regulation."[240] This is done in order to "promote internet operation in accordance with the law and internet operation in a civilized manner" and to "create a clean online environment."[241] By giving warnings during the dialectic interview, the CAC encourages compliance and cooperation by business entities, and voluntary modification or deletion of illegal contents. The CSL establishes the legal basis for participants in the interview, stating that "the network operator shall take measures to make rectification and eliminate hidden risks as required."[242] After its implementation, giving alerts and ordering rectifications has become the most commonly practiced technique the CAC employs.

The CAC and its local office "interviewed" over 2000 websites in 2017, a few hundred more than the totals in 2015 and 2016 combined. Popular websites include the news aggregation websites, like UC Toutiao, Jinri Toutiao, news publishing websites, such as Fenghuang Website, Xinlang, Souhu, Wangyi, and self-publishing websites Kwai, Zhihu, and TikTok. Common reasons that trigger interviews include hosting content involving fake news, insulting communist martyrs, excessive self-promotion by commercial stars from the entertainment industry, and content against the rules.[243] Three of nine scenarios that will elicit the interview mechanism directly address the content layer,[244] including 1) the entity seeks unlawful interests by gathering, editing, publishing, reprinting or deleting news information; 2) the entity fails to deal with illegal information in a timely manner and the circumstances are serious; or 3) the entity fails to establish a sound system for content management and network security or fails to

---

[240] Provisions, *supra* note 228, at art. 2.
[241] Provisions, *supra* note 228, at art. 1.
[242] Cybersecurity Law, *supra* note 74, at art. 56.
[243] 北京网信办整治自媒体平台,约谈腾讯凤凰今日头条等 (CAC Beijing office rectified self-publishing platforms and interviewed Tencent, ifeng, and jinritoutiao), CZTV (July 19, 2017, 8:27 P.M.) http://n.cztv.com/news/12606676.html [https://perma.cc/F8CQ-26NG].
[244] Provisions, *supra* note 228 at art. 4.

implement such a system. Furthermore, deciding what to censor on a local level to a certain degree also reflects the will of the Propaganda Department, because in practice, most of the local offices do not operate as an independent CAC office; they are integrated into the provincial Propaganda Department.

The interview technique can be understood pursuant to the regulatory pyramid of Ayres and Braithwaite's responsive regulation theory.[245] This theory envisages a hierarchy of sanctions. When the state authority notices enterprises which conduct their business activities in a way which will cause infringement of the law, they first use persuasive measures like negotiation and conciliation to encourage cooperation and compliance. If negotiation does not work, then the authority will escalate their response to administrative sanctions and financial penalties. Criminal prosecution is the last resort which is only applied when every other choice of remedy is exhausted. Professor Lu reasoned that CAC's interview mechanism resembles the hierarchical regulation model in terms of this escalating approach.[246] Article 7 of "the Provision" mandates several punishment measurements: "a warning, a fine, an order to suspend business for rectification, revocation of a permit" and "a severer [sic] punishment" if an illegal act continues after multiple interviews. However, the interview mechanism slightly digresses from this pyramid: the degree of punishment usually, but not always escalates from warning to "the severer [sic] punishment." The severity of the violation and the economic impact of the company also have to be factored in when deciding which level of punishment to start. For example, leading live social media streaming platform TikTok was ordered to delete content poking fun at communist martyrs[247] and was fined 1000,000 RMB

---

[245] Lu Chao (卢超), Hulianwang Xinxi Neirong Jianguan Yuetan Gongju Yanjiu (互联网信息内容监管约谈工具研究) [A study on the interview mechanism regarding content regulation] 2 CHINESE PUBLIC ADMINISTRATION (中国行政管理) (2019).

[246] *Id*.

[247] Jiawei Xu & Ji Bian, *Douyin Advertisement Suspended for Releasing Defamatory Information of Chinese War Hero*, PEOPLE'S DAILY (July 2, 2018, 1:41 PM), http://en.people.cn/n3/2018/0702/c90000-9476754.html [https://perma.cc/7K56-

(approximately 140,000 USD).[248] However, Rage Comics was summarily shut down for the same reason.[249]

The purpose of setting up interviews is not simply warning and punishing those platforms that serve illegal content in a case-by-case manner. To do this would elicit an endless Tom and Jerry game. Instead, Tom tries to catch Jerry by developing a self-regulating system in the interview mechanism: the CAC tries to dominate the platforms by instructing them on which content should be deleted, which ideally eventually launches a self-censoring mechanism within the company. For example, Kwai and Toutiao hired thousands of new employees to scrutinize illegal content after the interview.[250] However, self-censorship may trigger an enhanced version of censorship. Because the interview is recorded and included in the routine assessment and annual inspection files,[251] the news agencies and platforms are incentivized to avoid being summoned by the CAC, which provide motivation for the platforms to apply a stricter scope of self-censorship. Additionally, it is worth noting that the "modification" does not only mean deleting content deemed as violating the law - the Internet service providers are also required to add content with the "correct orientation" after the interview. For instance, on one of the many occasions Weibo was interviewed in 2018, its "trending topics" feature ("re'sou") was temporarily halted for a week as the CAC found it overly publicized some of the television stars who would pay to increase their exposure on its trending column.[252] A week later, the

---

HE72].

[248] She Ying(佘颖), 抖音的教训不应只是百万元罚款 (The lesson Tiktok should be learning should include things more than millions in fines), PEOPLE'S DAILY (Nov. 19, 2018, 8:25 AM), http://it.people.com.cn/n1/2018/1119/c1009-30407699.html [https://perma.cc/UMT5-BWM4].

[249] Manya Koetse, *China's Online 'Baoman' Community Shut Down: Behind Rage Comics*, WHAT'S ON WEIBO (May 20, 2018), https://www.whatsonweibo.com/chinas-online-baoman-community-shut-down-behind-the-rage-comics-baozou-manhua-craze/ [https://perma.cc/AU4G-XZ83].

[250] Emma Lee, *Kuaishou is Hiring More People to Filter Content after Crackdown on "Vulgar" Content*, TECHNODE (April 8, 2018), https://technode.com/2018/04/08/kuaishou-content-patrols/ [https://perma.cc/5V6P-HJZQ].

[251] Provisions, supra note 228 at art. 8.

[252] Ranking Digital Rights, *China Temporarily Shuts Down Weibo Services,*

users rejoiced upon the reintegration of the trending function, but surprisingly found the launch of a brand-new column called "New Era" ("xin'shidai").[253] "New Era" mainly promotes content praising socialist values and exhibits national achievements.[254]

Issuing remedies that start with warnings rather than punitive measurements avoids inefficiencies of administrative cooperation within the bureaucracy. Although other departments also conduct interviews, the CAC plays a major role in the first step of the hierarchical regulation model. Their influence was weakened with increasingly severe punishments at the upper level, as the escalating measures involve a more complicated collection of governmental participators. For example, Article 42 of the "Provisions on the Administrative Law Enforcement Procedures for Internet Information Content Management" assigned telecommunications departments to "close the website, revoke the license for the value-added telecommunications business of Internet information services, or cancel its recordation."[255] Therefore, the CAC could avoid the interview and warning steps, and instead directly follow the relevant provisions for punitive measures against errant operators who had committed "serious violation of the law." Allowing a certain degree of flexibility actually empowers the CAC and avoids regulatory conflicts with other departments.

This interview mechanism at the content layer epitomizes China's

---

Facebook Accused of Censoring Egyptian Activists, Lyft Employees Could be Spying on Riders (Feb. 2, 2018) https://rankingdigitalrights.org/2018/02/02/china-temporarily-shuts-down-weibo-services/ [https://perma.cc/2RUQ-SWHM].

[253] Guanchazhe Website (观察者网), 微博热门区新增新时代频道，弘扬社会主义核心价值观 [*New Era Segment was launched in Weibo Trending Section to Promote Socialist Value*] Sina Tech. (Feb. 1, 2018, 7:49 PM) http://tech.sina.com.cn/i/2018-02-01/doc-ifyrcsrw6512478.shtml [https://perma.cc/5BV8-PVH5].

[254] *Id*.

[255] (互联网信息内容管理行政执法程序规定) [Provisions on the Administrative Law Enforcement Procedures for Internet Information Content Management] (promulgated by the Cyberspace Administration of China on May. 2, 2017), at art. 42.

cyber governance strategy: although China expresses an assertive attitude in censoring content it deems inappropriate, the primary goal is not to shut down every domestic Internet company found to violate the censorship rules, especially the most influential Internet content providers. As the Internet service providers strengthen their content censorship or change features of services after the interview, they are mostly exonerated from punitive measures that they should be imposed because of their previous "serious violation of the law or regulation"[256]. In other words, the interview mechanism allows Chinese Internet companies to violate regulations without penalties, which will bring further economic benefits. But nudging companies to self-modify does not compromise the domination of the strong central government; the Chinese central government still has an absolute say on what constitutes a "serious violation to the law," whereas domestic Internet companies can only choose between either modifying their content, which will not trigger any punishment even after committing a "serious violation to the law," or not modifying as required and risking not being able to operate their business in the Mainland anymore. The interview is not to investigate, nor is it meant to allow the service providers to negotiate for some room in the published content. It is essentially non-negotiable in nature, including "a warning, point out the problems, or issue an order of rectification or correction." This presents a new challenge for weak and disadvantaged service providers in deciding where the red line is drawn, and thus potentially enhances the likelihood of self-censorship.

V. Conclusion

The centralization of the CAC and the strict control imposed by the Cybersecurity Law—the hefty responsibilities imposed on the network providers to regulate the content at the content layer and to safeguard the network security at the physical layer - illustrates China's ambition to take the Internet as the fifth sovereign. But as Hong Shen argued, it would not contribute to our understanding of China's approach on Internet governance if we limit our understanding to a level that reduces China to "a heavy-handed authoritarian state motivated by the

[256] Provisions, *supra* note 228, at art. 2.

drive to elevate governments and intergovernmental organizations as the sole governors of the global Internet."[257] To develop a cohesive understanding of China's Internet sovereignty, we need to investigate the whole picture: while the Chinese government is a firm supporter of a strong nation-state approach, Internet governance dynamics are also shaped by multiple participants including local state agencies, business units, industry cultural norms and institutional forces.[258] Their participation might not be as salient as the ICANN model in which each member is entitled to a vote, but it is inadequate to see their role as a static and purely subordinate state. In short, we should see not only the centralizing feature of the CAC, but also, and more importantly, the inside mechanism of the governmental agencies. This allows us to see how inefficient cooperation among state agencies impacted centralization, and recognize how the CAC makes compromises during the interviews with Chinese business units.

Invisible participation that comes from multiple cooperating players benefits from China's move to capitalize the Internet. By reviewing the historical emergence of the Internet in China, it becomes clear that one distinguishing factor of the Chinese interpretation of cyber sovereignty was its original intention for the Internet development: building an advanced economy. Unlike the United States, which championed the Internet's ability to spread knowledge without borders, the main role China assigned to the Internet was to impel economic development. China never had Internet founding fathers who fought for the independent Internet spirit, nor believed in its decentralizing ability to reject dominant theories of system design, like the western pioneers once did. The Chinese soil for the Internet to grow was the economic development and ICT infrastructure building plans. It served as a governmental tool to boost the economy since day one and is still expected to advance the national economy in the present, despite a more complicated Internet environment. Because of this compelling economic incentive, business units are allowed to

---

[257] Hong Shen, *supra* note 19, at 305.
[258] *Id*. at 305-06; Xia Jun, *China's Telecommunications Industry in the Era of 3G and Beyond: Market, Technology, and Institutions,* 36 TELECOMM. POLICY 793, 798 (2012).

modify their illegal activities without punitive measures during the interviews.

Content regulation at the content layer embodies an assertive nation-state stance as the other factor which contributes to China's unique interpretation of cyber sovereignty. There is not substantial difference from other nations in terms of building the infrastructural network at the physical layer, and all states, including Western democracies, place restrictions on the cyber realm. However, the way governments limit information at the content layer is the key battleground that differentiates China from other democratic states. While democratic countries usually see national security as being compromised by terrorism threats, the Chinese government casts a much wider net: including inappropriate and illegal content that threatens core socialist values as both cyber and national threats.

As Lu Wei, the previous head of the Cyberspace Administration of China (CAC) and the former director of the Central Leading Group for Internet Security and Informatization stated, cyberspace is a double-edged sword for China.[259] Chinese policymakers consider cyberspace not only as an essential tool for economic growth, but also as a potential threat to domestic stability and national security. Achieving cyber sovereignty essentially requires striking the right balance between maintaining social stability and promoting economic development.

---

[259] Lincoln Davidson, *Lu Wei: Four Rules for Being a "Good Chinese Netizen,"* COUNCIL ON FOREIGN REL. (June 10, 2015), https://www.cfr.org/blog/lu-wei-four-rules-being-good-chinese-netizen [https://perma.cc/2MF6-7X3W].