Cyberstability Paper Series

New Conditions and Constellations in Cyber

A Chinese Perspective on the Future of Cyberspace

Xu Peixi
Professor & Director of Global Internet Governance Studies Center,
The Communication University of China

July 2021

Cyberstability Paper Series
New Conditions and Constellations in Cyber

A Chinese Perspective on the Future of Cyberspace

Xu Peixi | Professor & Director of Global Internet Governance Studies Center, The Communication University of China

July 2021

Internet governance has moved beyond a narrow technical dimension of the early days and come to include all the key social topics, ranging from the digital economy, technological innovation, and military modernization, to political stability. It compasses all the stakeholders of the state, private sector, and civil society, and involves all the government institutions from commerce to defense. While the Internet empowers the grassroots and creates new opportunities for social justice, it is increasingly being haunted by military adventures, power competitions, disinformation campaigns, and financial fraud. Luckily, the plurality of relevant actors in cyberspace means that many of the proposed norms on regulating cyber behavior have wider appeal than it may seem.

This article firstly discusses how China perceives external threats, and observes that history or sovereignty is China's dominant perspective about cybersecurity. Then, it points out the fact that China is the most dependent country on the digital economy, and development is the dominant perspective in that field. It argues that China's worldview about cyberspace is reflected in its Confucian and Daoist traditions, and recommends a transnational and pluralistic approach to looking at cyberspace. It concludes with an analysis of several developing cyber norms.

In terms of security, a dominant Chinese perspective about cyberspace has been shaped and predetermined by past historical experiences and memories inherited and projected from the agrarian and industrial ages. This can be said to be a Chinese perspective about cybersecurity, under which cyberspace is a new domain where external threats originate.

Xu Peixi is Professor and Director of the Global Internet Governance Studies Center at the Communication University of China (CUC). He is an active participant of IGF and China-EU, China-U.S. cyber dialogues.

In agrarian centuries, external threats mainly came from the land, and nomads in the territories north and west of the Great Wall had a natural tendency to execute large-scale invasions in times of bad weather and in periods of China's disunity.[1] The need to exercise national defense against nomads is one of the three factors ruling out the possibility of a decentralized China, in addition to the necessity to tame the Yellow River and the obligation to commit vast resources to save people and regions struck by drought and flood caused regularly by fluctuations in the monsoon rainfall. Against such a backdrop, a unified China was born as early as 221 BC, and this feature of early unification and centralized governance serves as the sole and most evident difference between Chinese and European cultures.[2] From then on, unity, oneness, and harmony as important Chinese cultural values have been emphasized.

Over the industrial centuries, major threats were from the sea, and China was repeatedly defeated by European and Japanese powers. The one hundred years, from the 1840s to the 1940s, of foreign subjugation and occupation is referred to as the "era of national humiliation" in history discourse and political rhetoric.[3] The desire to account for this is reflected in the first words of the Chinese national anthem, which call on China to "stand up."

In terms of security, a dominant Chinese perspective about cyberspace has been shaped and predetermined by past historical experiences and memories inherited and projected from the agrarian and industrial ages.

In the digital age, cyberspace has been added as a new frontier where external threats against China's integrity and unity originate. At the beginning, cybersecurity was understood from an information security perspective. The online content filtering system known as the Great Firewall started to operate in 2003. The 2013 Snowden leaks made China aware of the fact that Chinese targets—ranging from private companies such as Huawei, to universities such as Tsinghua University, to the very top of China's leadership, China's President—are vulnerable to foreign intelligence agencies.

It was within this context that institutional reforms were made and the Leading Small Group for Cybersecurity and Informatization was established in 2014, representing a distinctive shift of approaching Internet issues from a perspective of economic growth and content challenges, in addition to that of infrastructure security. In December 2015, the Chinese President, Xi Jinping, proposed the notion of cyber sovereignty as a response to external cyber threats.

Development is the dominant perspective when looking at the Chinese economy in general and the digital economy in particular. On 20 September 1987, China successfully sent the first email to Germany, entitled "across the Great Wall we can reach every corner in the world." On 20 April 1994, China achieved full-functional connection to the Internet by opening a line through Sprint Co. Ltd. The Internet was introduced into China in the late 1980s and early 1990s, in a social background with two distinct features.

Firstly, the first unique feature was the rise of the grassroots user base. Decades of radical revolutions and social movements had flattened the traditionally hierarchical Chinese society and removed the ropes and chains binding the people, such as imperial authority, clan authority, religious authority, and patriarchal authority. Radical revolutions went to such extremes that traditional hierarchical codes were abolished, Buddhist temples were torn down, family-tree books were burned, and worship of ancestors was abandoned. Most effective of all, gender equality has been legally guaranteed.[4] Without these steps, it is difficult to imagine that a grassroots user base—with the Internet being available to the common people—would have been possible at all.

A second feature was the rise of the market. The Third Plenary Session of the 11th Central Committee held in 1978 paved the way for the installation and prosperity of market mechanisms, in pursuit of modernization. Private ownership was acknowledged and legally regulated. Economic development was the new logic of social evolution. As a result, China entered a massive economic growth phase unlike anything in human history. Chinese society is therefore undergoing a rapid transition on three levels: the agrarian level, the industrial level, and the informational level. Unlike with advanced Western economies in which the industrial phase alone took three centuries, the two transitions on the three levels have been happening simultaneously in China over the last four decades.

It was against this social background, featured by the co-rise of the grassroots user base and the market, that the Internet was introduced into China in the late 1980s, where it unleashed waves of innovations and changes that are arguably deeper than that which has been witnessed elsewhere. Led by the Internet and new ICTs, and globally integrated into the world economy through trade regimes such as the WTO, these innovations have nurtured the emergence of scores of leading companies. This includes the manufacturer Huawei, technology conglomerate Tencent, electronics company Xiaomi Inc., and also Internet giants such as the Internet search engine Baidu, e-commerce giants Alibaba and JD.com, the online content platform ByteDance, life service platform Meituan, ride-sharing giant Didi, microblog social network Sina Weibo, and video-hosting service Youku Tudou, among others.

These domestically or locally dominating technology companies, together with a plethora of other digital businesses, are defining the digital lifestyles of nearly one billion Chinese Internet users. China's digital economy was valued at 39.2 trillion Yuan (approximately 6 trillion USD) in 2020, accounting for 38.6 percent of the GDP of the same year, and from that perspective making China the most dependent country on the digital economy.[5] This pursuit for digital prosperity serves as the economic reason for China's vision about building "a community of shared future for mankind in cyberspace."[6] This makes China the least willing and the most anxious to see signs of fragmentation of the Internet, and a potentially strong supporter of many developing cyber norms proposed by state or non-state actors as diverse as Microsoft Corporation, the Global Commission on the Stability of Cyberspace, the Carnegie Endowment for International Peace, the Internet & Jurisdiction Policy Network, French President Emmanuel Macron, and Internet pioneer Tim Berners-Lee.

In contrast to the Chinese perspectives of approaching cybersecurity from history or from a sovereignty perspective, and approaching the digital economy from a development or globalization perspective, a typical Western way of addressing cyberspace, however, often seems viewed through a lens of good guys versus bad guys, or even good versus evil. While the Chinese viewpoint sees itself as essentially pragmatic, it often considers the Western viewpoints to be essentially moralistic, at best. From the 2017 Trump Administration onwards, this worldview of good guys versus bad guys has become increasingly salient and has been translated into concrete digital policies, driving global Internet governance into a downward spiral of fragmentation and foreseeing a scenario of a digital Cold War.

Represented by the *Clean Network Initiative*, a systematic and historically unprecedented intervention in the global supply chain is taking place. This not only interrupts the roll-out of 5G, seen as being an important technological development, but also other cutting-edge technologies. These anti-trade measures are gaining momentum and casting divisions in the global Internet ecosystems at the cost of global businesses.

Numerous proposals and initiatives demonstrating the good-guys-versus-bad-guys perspective are being made. Nations as diverse as Russia, China, Iran, and North Korea are conveniently categorized together by a plethora of politicians, think tankers, and sometimes even by academia, and packaged into enemies, bad guys, adversaries, or, at best, as competitors. These voices claim to warn about "the rise of digital authoritarianism."[7] China was labeled as representing a "digital authoritarian model"[8] and was constantly accused of spreading "authoritarian tech."[9] At the same time, the EU and the United States are called upon to work on "countering digital authoritarianism" and "addressing China together."[10]

The increasing popularity of the rhetoric happens before a backdrop of rising geopolitical tensions in the digital and non-digital realms. But the terminology is not new. Broadly, it resembles a digital rearticulation of a mixture of Orientalist imaginations, a Cold War ideological framework, and a Huntington lens of civilizational clashes.

Specifically, it is a digital rebirth of *Four Theories of the Press*: authoritarian theory, libertarian theory, social responsibility theory, and Soviet Communist theory,[11] which were written in the years of the Cold War. All the good virtues, such as libertarianism and social responsibility, are owned by the West. All the bad characteristics, such as authoritarianism and Soviet Communism, are attached to the others. The Four Theories framework of thinking had influenced media and communication learners for decades before it was systematically reflected and fundamentally challenged, in *Media, Messages, and Men,*[12] *Agents of Power,*[13] *Last Rights: Revisiting Four Theories of the Press,*[14] and *Normative Theories of the Media.*[15]

Rather than applying the good-guys-versus-bad-guys perspective, it would be more appropriate to argue that all societies and cultures have both authoritarian and libertarian orientations in handling the mixed security and development challenges posed by cyberspace, and each orientation occupies a position in the libertarian-authoritarian continuum.

Under such a thought experiment, the United States as a nation in itself owns the most authoritarian and the most libertarian elements of Internet governance, occupying the two ends of the continuum. The U.S. military and NATO, located in the far left of the continuum, are, knowingly or not, shaping the most authoritarian elements of Internet governance, by imagining enemies or adversaries that need combatting. On the other side, the U.S. IT sector, Silicon Valley, and Internet technical communities, located in the far right of the continuum, are promoting the most libertarian version of Internet governance. They represent two contradictory values and practices, and their ways of cooperation and competition in the digital age would, to a large extent, decide the fate of the Internet. There has never been a singular value about cyberspace, even in the United States itself—the birthplace of the Internet.

While the Chinese viewpoint sees itself as essentially pragmatic, it often considers the Western viewpoints to be essentially moralistic, at best.

The same may also be true about China, which has its authoritarian and libertarian traditions that are represented by Confucianism and Taoism. They are the hidden codes that guide thinking about old fields and new domains. Taoism and Confucianism are both opposites and complementary. Xiao summarizes: "Whereas Confucius and Mencius, one of the foremost Confucian thinkers, promoted moral cultivation and a hierarchical system of human relations as solutions to the social chaos of their times, the founders of Taoism, the mythical Laozi and Zhuangzi, viewed such moral and social efforts as artificial constraints on the very nature of human beings and the *Tao* (Way) of the universe.

Laozi and Zhuangzi advocated the idea of *wuwei* (effortless action), which has led to Taoism being associated with the themes of naturalness, spontaneity, relatedness, pluralism, anarchism, and laissez-faire government."[16]

Chen observes that the fundamental difference between Confucianism and Taoism is that they evolve respectively into the ideological agents of state actors and non-state actors, and the former often serves a restricting role, the latter an intriguing and liberating role.[17] The early days of Internet growth were an annotation of a Taoist approach. "Its development was driven by non-governmental developers, providers, and users of the new services." "Internet standards, codes, and guidelines...came not top down by majority voting of elected parliamentarian representatives, but were drafted bottom up by the respected and competent key players of the global Internet community."[18]

As cyberspace evolves to include more stakeholders, tensions between different pillars of society exist. State, commercial, and grassroots logics meet, expand, interact, and compete in the new domain. Domestic disagreements between different actors about how the Internet should be governed are no less evident than in the global arena.

As one example, the private online video platforms did not rise and succeed in China overnight. They survived a most tightly regulated broadcasting sector, and it took many struggles to push back China's state efforts to have them nationalized. As another example, the cities of Beijing and Shenzhen have drastically different ride-sharing policies, reflecting different local priorities. In terms of the grassroots Internet financing industry serving a completely new consumer credit market, there have been rising tensions between the new companies and vested interests in the state-controlled banking sector.

Together with all the domestic and geopolitical realities, cyberspace differs from many other domains in that it covers a whole spectrum of dimensions, and these dimensions are interconnected and intertwined due to the oneness nature of the global Internet. Under the circumstance, globally speaking, it is difficult to repeat the successes in nuclear weapons (*Treaty on the Non-Proliferation of Nuclear Weapons*), sea (*United Nations Convention on the Law of the Sea*), and climate change (*Paris Climate Agreement*). The current fragmented landscape of cyber and digital dialogues will continue for longer than perhaps was originally hoped by early observers.

However, in spite of the challenges and frustrations, global efforts to reach agreement on certain cyber norms are delivering positive results. States, businesses, and civil society actors are seeking global solutions. In December 2014, Microsoft proposed six cybersecurity norms. In November 2018, the Global Commission on the Stability of Cyberspace issued its final version of an eight-norms package.[19] Many of these norms were already referenced in the nine principles of the Paris Call.[20]

In July 2019, Tim Berners-Lee published the first draft text of the Contract for the Web, proposing eight principles by which to save the Internet.[21] In September 2020, Chinese Foreign Minister Wang Yi launched *Global Data Security Initiative*, outlining eight principles calling for a facts-based approach instead of an ideological one, by which to solve global data disputes.[22] In March 2021, the OEWG 2019-2020 published its final report. In May 2021, the UN GGE 2019-2020 adopted a consensus report.

While the above-mentioned initiatives reveal quite different understandings about cyberspace, they contain many vivid details and, most important of all, they aim at seeking global solutions rath-

er than at just making accusations. State and non-state stakeholders' positions regarding cyber espionage, the public core of the Internet, cross-border content, and cybersecurity vulnerability, are gaining visibility. Most tellingly, a number of seemingly very different norms have turned out to be closer to each other then they had originally seemed.

These norms-building processes, with varying degree of success, underline a consistent and constructive thread in the global cyber dialogue. They persist in seeking global solutions and refuse to be carried away by increasing geopolitical tensions. Within the processes, actors from technical and political backgrounds meet, stakeholders from security and business circles communicate, and people with idealistic and realistic viewpoints cooperate.

The first example is the so-called Cyber Espionage Norm.[23] On 25 September 2015, China and the United States came to an understanding about cyber espionage activities. The norm limits the activity of espionage in that it disavows intellectual property thefts by military and intelligence agencies "for intent of commercial advantage," while not addressing other forms of espionage. The norm was reconfirmed also between China and Britain (2015), the United States and India (2016), and China and Canada (2017), and was found in Group of 20 (2015) and Group of 7 (2017) outcome documents. It is also one of the nine principles of the *Paris Call* (2018). The most salient feature of the original Xi-Obama agreement is that it protects the vulnerabilities of the industry but does not weaken the strengths of the intelligence actors on either side. By that token, the norm symbolizes a win-win result, perhaps not just between China and the United States, but also between the industry and intelligence agencies.

The second example is the Non-Interference with the Public Core of the Internet Norm.[24] On 21 November 2017, the Global Commission on the Stability of Cyberspace (GCSC) issued a call to protect the public core of the Internet. The norm started as a report submitted in March 2015 to the Dutch Ministry of Foreign Affairs. "Its main argument is that the Internet's infrastructure and core protocols should be regarded as a global public good that is in need of protection against unwarranted interventions by states and other parties."[25]

The norm is similar to the cyber espionage norm in wording, and it nevertheless implies a message that penetration into undersea cables is permitted as long as it does not cause tangible damages. On the other hand, the most valuable part of the norm is that it may help to reduce the anxieties of many non-Western nations about the theoretical possibility that their country code top-level domains, such as .uk, .de, or .cn, might be removed from cyberspace.

The norm's association with global public good does not appear in the final report of the GCSC, but does appear in the 2019 *EU Cybersecurity Act*, which states: "The public core of the open internet, namely, its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. ENISA should support the security of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular, DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone."[26]

China's diplomatic position about the public core norm remains hesitant and unclear. In a statement about the initial pre-draft of the OEWG report, China comments that the concept "has not gained global consensus yet."[27] However, the norm, particularly the *EU Cybersecurity Act* version that brings back the phrase "global public good," gives a firm commitment about cyber stability and should be welcome in China.

The third example is the Vulnerability Norm.[28] In December 2014, Microsoft published *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*, and proposed six bold norms to limit conflict. The first norm proposed that states should be prohibited from inserting vulnerabilities or backdoors. The Microsoft proposal turns out to be the most prohibitive norm among similar proposals.

In contrast, the GCSC's proposal about the vulnerability norm is not as restrictive. It says that "state and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace."[29] The GCSC norm singles out the development and production phases and, meanwhile, the norm implies that even the development and production phases can be tampered with, if the action does not impair cyberstability.

The public core norm, particularly the *EU Cybersecurity Act* version that brings back the phrase "global public good", gives a firm commitments about cyber stability and should be welcome in China.

Chinese legal language often indirectly indicates a prohibitive signal about inserting backdoors by state actors. However, China's *Global Initiative on Data Security* does not mention how state actors should behave, but makes it clear that "ICT products and services providers should not install backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices."[30]

The fourth example is the norm to not use ICTs to interfere with the internal affairs.[31] On 9 January 2015, the Shanghai Cooperation Organization (SCO) proposed the *International Code of Conduct for Information Security* to the United Nations, pinpointing such a wording about ICTs and internal affairs.

The SCO proposal is broad and contains both technical and content elements, but tilts more toward content. It has something in common with the suggestion in the *Tallinn Manual 2.0* that cross-border propaganda may constitute a violation of sovereignty if it incites turmoil. Seeing itself as a victim of decades of one-way flow of information, China is more than willing to further define norms in this aspect.

The proposed norms in this area are either technically focused or content focused. A pure content perspective is reflected in Article 20 of the *International Covenant on Civil and Political Rights*, prohibiting "any propaganda for war" and "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,"[32] and the digital application of this international legal instrument is inspiring the cross-border content moderation working group at the Internet & Jurisdiction Policy Network, based in Paris.

GCSC represents a technical perspective when proposing a norm to protect electoral infrastructure, saying, "state and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites."[33]

The above norm-building processes show that, even though there may be very different motivations for actors to propose or agree upon a specific norm, in technical detail and outcome they may be more alike. This realistic, pragmatic, yet global way of approaching cyber challenges increases the odds of finding commonalities between different states, stakeholders, and cultures, reduces the scenario of a digital Cold War, and pushes global Internet governance toward a digital commons, similar to the current direction in which global co-operation on climate change is heading.

Endnotes

1 Ray Huang. Broadening the Horizons of Chinese History. New York: M. E. Sharpe, Inc. 1999. 29.

2 Ibid. 23.

3 Larry A. Samovar, Richard E. Porter, Edwin R. McDaniel, and Carolyn S. Roy. Communication between Cultures (9th Edition). Boston: Cengage Learning, 2017.174.

4 For instance, the 1950 People's Republic of China Marriage Law was the first law introduced by the newly founded Republic. See Chen Xinxin. "Marriage Law Revisions Reflect Social Progress in China." China Today, April 2001. https://web.archive.org/web/20100629155714/http://www.chinatoday.com.cn/English/e2001/e200103/hunyin.htm.

5 China Digital Economy Development White Paper. China Academy of Information and Communications Technology, April 2021. 5.

6 United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security. UN GA, October 2020. https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com20/resolutions/L8Rev1.pdf.

7 See "The Rise Of Digital Authoritarianism: China, AI, & Human Rights," a seminar series ran from September to October 2020 by the Hoover Institution. Accessible at https://www.hoover.org/events/rise-digital-authoritarianism-china-ai-human-rights.

8 See "A Transatlantic Effort to Take on China Starts with Technology," a virtual event ran by CEPA. Accessible at https://cepa.org/event/a-transatlantic-effort-to-take-on-china-starts-with-technology/.

9 See the "#DefendDemocracy" virtual series, ran by the Alliance of Democracies. Accessible at https://www.allianceofdemocracies.org/initiatives/the-campaign/defenddemocracy-virtual-series/.

10 See the "EU-US Future Forum," a virtual forum ran by the Atlantic Council from May 5-7, 2021. Accessible at https://www.atlanticcouncil.org/programs/europe-center/eu-us-future-forum/.

11 Fred S. Siebert, Theodore Peterson, and Wilbur Schramm. Four Theories of the Press. Urbana: University of Illinois Press, 1956.

12 Merrill and Lowenstein. Media, Messages, and Men: New Perspectives in Communication. New York: David McKay Company Inc,1979.

13 Herbert Altschull. Agents of Power. New York: Longman, 1984.

14 John C. Nerone. Last Rights: Revisiting Four Theories of the Press. Urbana: University of Illinois Press, 1995.

15 Clifford G. Christians, Theodore L. Glasser, et al. Normative Theories of the Media. Urbana: University of Illinois Press, 2009.

16 Xiao Xiaosui. "Taoist Communication Theory" in Encyclopedia of Communication Theory edited by Stephen W. Littlejohn and Karen A. Foss. Thousand Oaks: Sage Publications, 2008. 955.

17 Chen Guying. New Comments on Laozi & Zhuangzi. Bejing: ZHONGHUA Book Company, 1991. 4.

18 Wolfgang Kleinwächter. "200 Years of Negotiation on Cross-Border Communications: From Intergovernmental Treaties to the Multistakeholder Model for the Governance of the internet" in Towards Equity in Global Communication? edited by Richard C. Vincent and Kaarle Nordenstreng. Cresskill: Hampton Press, 2016. 129.

19 GCSC. Norm Package Singapore. GSCS: The Hague, November 2018. https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

20 Paris Call. "The 9 Principles," accessed June 22, 2021. https://pariscall.international/en/principles.

21 Berners-Lee, Tim. "Contract for the Web,"Contract for the Web, accessed June 22, 2021. https://contractfortheweb.org/#main.

22 Ministry of Foreign Affairs for the People's Republic of China. "Global Initiative on Data Security,"last modified September 8, 2020. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml.

23 "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." See The White House Office of the Press Secretary. "Fact Sheet: President Xi Jinping's State Visit to the United States."Last Modified September 25, 2015.https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

24 "State and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace." See The Global Commission on the Stability of Cyberspace. "Global Commission proposes definition of the public core of the Internet."Last Modified July 5, 2018. https://cyberstability.org/news/global-commission-proposes-definition-of-the-public-core-of-the-internet/.

25 Dennis Broeders. The Public Core of the Internet: An International Agenda for Internet Governance. Amsterdam: Amsterdam University Press, 2015. 7.

26 See European Parliament. "REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)." Official Journal of the European Union¸ last modified April 17, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32019R0881&qid=1623624957963.

27 See United Nations Office for Disarmament Affairs. "Open-ended Working Group."Accessed June 17, 2021. https://www.un.org/disarmament/open-ended-working-group/.

28 "States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services." See Microsoft. International Cybersecurity Norms: Reducing conflict in an Internet-dependent world. Microsoft Corporation, 2015.https://www.microsoft.com/en-us/download/confirmation.aspx?id=45031.

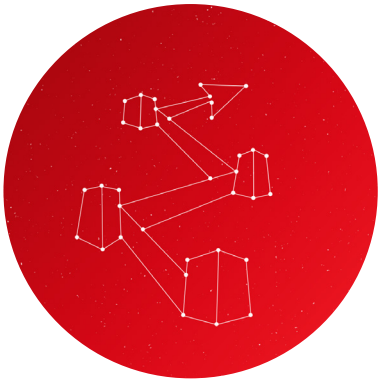
29 See Global Commission on the Stability of Cyberspace. "Norm to Avoid Tampering."Accessed June 17, 2021. https://cyberstability.org/norms/#toggle-id-3.

30 See China.org.cn. "Global Initiative on Data Security."Accessed June 17, 2021. http://www.china.org.cn/chinese/2020-09/15/content_76704524.htm.

31 "Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability." See Ministry of Foreign Affairs of the People's Republic of China. "International Code of Conduct for Information Security."Accessed June 17, 2021. http://infogate.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t858317.shtml.

32 See United Nations Human Rights Office of the High Commissioner. "International Covenant on Civil and Political Rights." Accessed June 17, 2021. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

33 See Global Commission on the Stability of Cyberspace. "Norm to Protect Electoral Infrastructure."Accessed June 17, 2021. https://cyberstability.org/norms/#toggle-id-2.



About the Author

Xu Peixi is Professor and Director of the Global Internet Governance Studies Center at the Communication University of China (CUC). He obtained his Doctoral Degree from CUC and a Licentiate Degree from the University of Tampere, Finland. His research interests include Global Communication, Internet Governance, and Cybersecurity. He has authored over 50 articles published in academic journals, including *China Information Security* and *Modern Communications*, as well as three books: Global Governance from Traditional Media to the Internet (Tsinghua University Press), The Shaping of Cyber Norms: Origins, Disputes, and Trends (China Social Sciences Academic Press), and Digital Cold War Studies (Guangming Daily Press). Xu Peixi is a member of the MAG of China IGF. He is an active participant of IGF and China-EU, China-U.S. cyber dialogues. He can be reached at xupeixi@gmail.com.

About the Cyberstability Paper Series

Since the release of the final report of the Global Commission on the Stability of Cyberspace in November 2019, the concept of cyberstability has continued to evolve. A number of new 'conditions' are emerging: new agreements on norms, capacity building and other stability measures have been proposed and solidified within the United Nations and elsewhere, and stakeholders are exploring ways to increase stability and minimize the risk of conflict in cyberspace through technical fixes or governance structures. The constellations of initiatives involved in working towards cyberstability is expanding, underlining the need to connect the traditional state-led dialogues with those of the Internet communities from civil society and industry. Gaps continue to close, between the global north and south, between technology and policy, but also the stability in and the stability of cyberspace.

The first Cyberstability Paper Series explores these "New Conditions and Constellations in Cyber" by collecting twelve papers from leading experts, each providing a glance into past or future challenges and contributions to cyberstability. The papers are released on a rolling basis from July until December 2021, culminating in an edited volume. All papers will be available for open access, and a limited number of printed hardback copies are available.

Published by

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre
for Strategic Studies