NAVIGATING THE US-CHINA COMPETITION IN CYBERSPACE

It is indisputable that the United States and China have become two core pillars of the newly forming international cyber order; therefore, the dynamics of their relations in cyberspace have profound implications for the international system. Looking forward, aside from finding more rational ways to protect their own national interests, the two states need to think about how to shoulder responsibilities as global powers, address common concerns, and prevent disastrous crises in cyberspace. This article outlines their underlying tensions in cyberspace and offers insights on how to manage a healthy competition moving forward so that these two big powers can steer the world's digital future to a promising track.

Lyu Jinghua & Gaurav Kalwani*

TPQ
Summer 2020

* Lyu Jinghua is a Visiting Scholar at Carnegie Endowment for International Peace. Gaurav Kalwani is a Junior Fellow at Carnegie Endowment for International Peace.

Although cyberspace represents a relatively new facet of the US-China relationship, controversies within this domain have rapidly evolved into critical and contentious issues in the eyes of both parties, affecting a wide swath of policy areas such as trade, defense, transparency, and the rule of law. Understanding the development and underlying factors of tensions, the concerns of both sides, and the way in which these problems combine in the poorly managed competition over 5G will be crucial to moderating friction and building the future digital world.

The Evolution of US-China Tensions and Concerns in Cyberspace

Since China's entry into the Internet in 1994, US-China conflicts over information and communication technologies (ICTs) have gone through several stages with different points of disagreement. Up until Google's withdrawal from mainland China in January 2010, despite the clashes between the US and Chinese civilian hackers,[1] accusations of Chinese cyber espionage activities such as Titan Rain and Operation Aurora, and the fight over the WAPI (WLAN Authentication and Privacy Infrastructure) standard,[2] there was more cooperation than competition between the two countries. During this period, the US' primary focus was entering its Internet companies into the Chinese market, while China's main goal was to become integrated into the Internet by accepting the existing associated frameworks, protocols, and technologies.

The US and China's perception of the other in cyberspace began to shift in the early 2010s, when a political disagreement regarding online information emerged. The disagreement stemmed from the Obama administration's (particularly Secretary of State Hillary Clinton's) push for "Internet freedom" and harsh criticism of China's cyber censorship and its restrictions on the free flow of information. Around the same time, the Chinese government began to pay larger attention to the potential of social media in triggering and escalating social unrest after observing protest movements such as the Arab Spring and Occupy Wall Street. This observation led to China's strong advocacy for "cyber sovereignty", and a particular concern over the US' attempt to ideologically influence China via its call for Internet freedom.

The next major issue became cyber-enabled espionage activities, with the Mandiant report exposing China's multi-year economic espionage campaign[3] and with

[1] There were online conflicts between patriotic hackers during major crises in this period, such as the US bombing of the Chinese embassy in Belgrade, US arms sales to Taiwan, and the collision of a Chinese fighter jet and US spy airplane over the South China Sea.

[2] See, for example: Ping Gao, "WAPI: A Chinese Attempt to Establish Wireless Standards and the International Coalition that Resisted," *Communications of the Association for Information Systems*, Vol.23 (2008), https://aisel.aisnet.org/cais/vol23/iss1/8

[3] FireEye Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 18 February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Edward Snowden revealing the US PRISM Project[4] in 2013. Alongside concerns that these activities would cost the US hundreds of billions of dollars annually because of cyber theft,[5] the US also worried that willingness to invest in innovation would be eroded by such activities. On China's side, their most pressing concern was the number of surveillance targets they had not been fully aware of the US monitoring. Instead of simply putting forward ideas and concepts to address political concerns as before, this time both sides took concrete actions. While the US Department of Justice indicted five People's Liberation Army (PLA) officers for cyber espionage against US companies in 2014,[6] China initiated the De-IOE program the same year, which aimed to uninstall software made by American suppliers, including IBM, Oracle, and EMC, from its e-commerce companies and banks.[7]

"The US and China's perception of the other in cyberspace began to shift in the early 2010s, when a political disagreement regarding online information emerged."

Since 2017, the US has increasingly expressed concern over the vulnerability of its critical infrastructure systems to cyberattacks from China. In particular, the US has been stressing the potential threats China could pose by conducting cyberattacks with "localized, temporary disruptive effects on critical infrastructure."[8] A particularly pessimistic overview asserts that China can potentially thwart the US attempts to respond to such attacks, as "the offensive cyber capabilities of [its] most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures."[9]

Another major concern that has emerged in the same timeframe are the restrictions that China placed on companies' data routing and storage practices. Highly relevant

[4] Timothy B. Lee, "Here's everything we know about PRISM to date," *Washington Post*, 12 June 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

[5] See, for example: White House Office of Trade and Manufacturing Policy, "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," 18 June 2018, https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf

[6] Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," *US Department of Justice*, 19 May 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[7] "'De-IOE' in China," *Eyerys*, 26 June 2014, https://www.eyerys.com/articles/timeline/de-ioe-china#event-a-href-articles-timeline-russia-lifts-its-futile-two-year-ban-telegram-messaging-apprussia-lifts-its-futile-two-year-ban-on-the-telegram-messaging-app-a

[8] Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," *Office of the Director of National Intelligence,* 29 January 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[9] Defense Science Board, "Defense Science Board Task Force on Cyber Deterrence," *US Department of Defense*, 1 February 2017, https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf

to the concerns over China's policies on the flow of information mentioned above, the US' latest focus has been the "significant adverse effect" on trade and commerce that these restrictions could have with the implementation of China's new cybersecurity law.[10] The US asserts that China's commitments to market access and the equal treatment of foreign providers have been violated, as the new law requires notification and consent for cross-border transfer of potentially sensitive data, severely complicating the functioning of foreign firms while favoring domestic ones.

In contrast to America's case-by-case, sector-by-sector threat assessments and proclamations, China counters claims by noting the number of US originated cyber-attacks it received. More importantly, China emphasizes their asymmetric cyber capabilities, underlining the US dominance in Internet governance and supply chains, as well as its leadership in developing international cyber norms.

Huawei and 5G

All these issues that piled up over the years once again came to light with the 5G and Huawei controversy. This time, however, economic and geopolitical concerns were at the heart of the issue: 5G's faster connection and data transmission speeds, as well as lower latency, have the potential to enable not only significant economic growth, but also innovate critical technologies in a host of different fields. Despite being the global leader in the development and implementation of 4G technologies, the US worries that it might be left behind in the technology race over 5G or in related processes of global norm-setting, as reduced US leadership could produce unfavorable conditions for the future of its economic endeavors and global market presence.

Although the details are often classified, security concerns largely drive the current controversy over Huawei. Out of fear that China could leverage "backdoors" in the network to conduct surveillance and collect sensitive data, the US restricted government agencies from doing business with Huawei in August 2019,[11] and cut both Huawei and ZTE off from an 8.3 billion dollar government subsidy program a year later.[12] From a military angle, aside from 5G having profound implications on R&D, there is also the possibility of China monitoring—or disrupting—US military communications and network-dependent operations[13] within Chinese-built 5G ecosystems.

---

[10] World Trade Organization, "Communication from the United States: Measures Adopted and Under Development by China Relating to its Cybersecurity Law," 26 September 2017 https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf

[11] Steve Lohr, "U.S. Moves to Ban Huawei From Government Contracts," *New York Times*, 7 August 2019, https://www.nytimes.com/2019/08/07/business/huawei-us-ban.html

[12] Arjun Kharpal, "China's Huawei and ZTE Officially Designated 'National Security Threats' by the FCC," *CNBC*, 30 June 2020, https://www.cnbc.com/2020/07/01/fcc-huawei-zte-officially-designated-national-security-threats.html

[13] Erica D. Borghard and Shawn W. Lonergan, "The Overlooked Military Implications of the 5G Debate," *Council on Foreign Relations*, 25 April 2019, https://www.cfr.org/blog/overlooked-military-implications-5g-debate

Extending from their different political systems, the US also fears that Huawei would have to yield to the Chinese government's requests for sensitive data of US citizens or entities.[14]

"Extending from their different political systems, the US also fears that Huawei would have to yield to the Chinese government's requests for sensitive data of US citizens or entities."

However, the Huawei controversy is not only an accumulation of previously existing concerns. There are at least two new features that are worth noting. Most complaints made, and actions taken, by the US government in the past were directly against the Chinese government, by which companies in both countries were not deeply affected. More importantly, until now, the connections between companies withheld the two countries from being too extreme in their policies. However, this time, companies are involved as either targets, such as Huawei and ZTE, or as partners of their government in decoupling efforts. Some experts have cited the US' relative lack of tight control over corporations and local regulations as a reason China has sprinted ahead in 5G development.[15] To obstruct China's progress in 5G, the US has barred US-based companies from using equipment produced by Huawei.[16] By placing Huawei on the US Department of Commerce's Entity List, the US has prohibited US firms from conducting sales with the company, partially cutting off Huawei's access to crucial American products such as semiconductors that power Huawei products.[17]

In addition to these regulations on domestic companies, the US has also pressed its allies to prohibit Huawei from constructing their 5G networks[18] out of fear of Chinese espionage and potential vulnerability to cyberattacks or installed kill switches. The US has warned that alliances, and intelligence sharing arrangements in particular, would be in jeopardy if European countries were to use Huawei technology in their

[14] Julian E. Barnes, "White House Official Says Huawei Has Secret Back Door to Extract Data," *New York Times,* 11 February 2020, https://www.nytimes.com/2020/02/11/us/politics/white-house-huawei-back-door.html

[15] Nicol Turner Lee, "Navigating the US-China 5G Competition," *Brookings*, April 2020, https://www.brookings.edu/research/navigating-the-us-china-5g-competition/

[16] David Shepardson and Karen Freifeld, "Trump extends U.S. telecom supply chain order aimed at Huawei, ZTE," *Reuters,* 13 May 2020, https://www.reuters.com/article/us-usa-trade-china-trump/trump-extends-us-telecom-supply-chain-order-aimed-at-huawei-zte-idUSKBN22P2KG

[17] Karen Freifeld and Chris Prentice, "Exclusive: U.S. drafts rule to allow Huawei and U.S. firms to work together on 5G standards – sources," *Reuters,* 6 May 2020, https://www.reuters.com/article/us-usa-china-huawei-tech-exclusive/exclusive-u-s-drafts-rule-to-allow-huawei-and-u-s-firms-to-work-together-on-5g-standards-sources-idUSKBN22I1ZY

[18] David E. Sanger and David McCabe, "Huawei Is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives," *New York Times,* 15 May 2020, https://www.vnytimes.com/2020/02/17/us/politics/us-huawei-5g.html

5G networks.[19] It has also frequently used the term "like-minded governments" to draw a dividing line in efforts to "develop and deploy and manage secure and reliable 5G communications infrastructures."[20] Relations between the US and China have never been purely bilateral; their competition in cyberspace is now expanding and influencing other parts of the world at an unprecedented scale.

Underlying Factors That Drive Tensions

The current worsening of US-China relations is due to three main reasons. First, the lack of an acknowledgment of failed past policies toward each other; namely, the US expectation of "spur[ring] [the] fundamental economic and political opening"[21] of China as well as China's hope of accelerating its modernization with "Chinese characteristics"[22] and integration into the US-led international system. Second, the lack of a common threat, such as the Soviet Union during the 1970s, global terrorism in 2001, and the financial crisis in 2008. Third, the narrowed gap in national strengths, especially when measured in GDP. Altogether, the US has adopted an increasingly tougher approach toward China,[23] leading China to perceive that a rising power with a different political system is not welcomed, which resulted in "struggle" being the new bellwether of Beijing's relations with Washington.[24]

All three factors have been magnified in cyberspace in a more complex way. The increase in mutual suspicion of each other's intentions is deeply embedded in the cyber domain, where anonymous and invisible activities are prevalent. The US interprets every claim and action by the Chinese government in cyberspace as being part of efforts to increase its autocratic rule domestically, and to benefit from being the revisionist as well as the rule breaker on the international stage. China believes that the US' accusations and its call for international standards are meant to suppress China's rise and maintain the US' leadership in cyberspace.

The two countries also face the challenge of finding common ground in combating cyber threats. Although both assign much importance to cybersecurity, they have

---

[19] Patrick Wintour, "US defence secretary warns Huawei 5G will put alliances at risk," *The Guardian,* 15 February 2020, https://www.theguardian.com/us-news/2020/feb/15/us-defence-secretary-warns-us-alliances-at-risk-from-huawei-5g

[20] "US Calls for cautious EU policy on 5G networks," *Outlook India*, 2 May 2019, https://www.outlookindia.com/newsscroll/us-calls-for-cautious-eu-policy-on-5g-networks/1527100

[21] White House, "United States Strategic Approach to the People's Republic of China," 20 May 2020, https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.20.20.pdf

[22] Andrew Sheng and Xiao Gen, "Modernity with Chinese characteristics," *China Daily*, 30 October 2017, https://www.chinadaily.com.cn/opinion/2017-10/30/content_33878780.htm

[23] Richard C. Bush and Ryan Hass, "The China debate is here to stay," *Brookings,* 4 March 2019, https://www.brookings.edu/blog/order-from-chaos/2019/03/04/the-china-debate-is-here-to-stay/

[24] An Gang, "Coordination Exchanged for Struggle," *China-US Focus,* 9 October 2019, https://www.chinausfocus.com/foreign-policy/struggles-replace-coordination-in-china-us-relations

different priorities. While the US prioritizes the protection of critical infrastructure from cyberattacks, China senses more urgency in shielding itself from social instability caused by exchanges on social media that urge to challenge the government's ideology. Even though China also seeks to protect critical infrastructure, their major concern is their lack of self-reliance for key ICT elements.

> *"Cybercrimes might be the only area that both the US and China view as a threat."*

Cybercrimes might be the only area that both the US and China view as a threat. This common concern led to the establishment of the High-Level Joint Dialogue on Cybercrime and Related Issues in 2015, and building on the former, the Law Enforcement and Cybersecurity Dialogue in 2017. However, the issue is apparently not critical enough to core national interests that the two are willing to leave aside other differences, as they did before for other mutual interests.

The different assessments of comparative power which can increase tension and mutual suspicion also exist in ICT relevant areas. China's technology power has undoubtedly been rapidly growing. Its R&D spending grew by more than 17 percent each year from 2000 to 2017, while growth in the US averaged only 4.3 percent.[25] China's contribution to the Nature Index increased by 75 percent between 2012 and 2017, while its share of global scientific output increased from 9 to 16 percent during the same timeframe.[26] China also surpassed the US as the top source of international patent applications filed with the World Intellectual Property Organization (WIPO) in 2019.[27] However, China still finds itself largely lagging behind in some key areas—at least 29, in fact.[28] Spending on basic research, which is the backbone of innovation, only accounted for an average of 5 percent of China's overall R&D

[25] Niall McCarthy, "China Is Closing The Gap With The U.S. In R&D Expenditure –[Infographic]," *Forbes,* 20 January 2020, https://www.forbes.com/sites/niallmccarthy/2020/01/20/china-is-closing-the-gap-with-the-us-in-rd-expenditure-infographic/#66a2d6c15832

[26] "Nature Index 2018 reviews China's scientific performance over the past five years," *Springer Nature Group*, 13 December 2018, https://group.springernature.com/kr/group/media/press-releases/nature-index-2018-reviews-china-s-scientific-performance/16338530

[27] Stephanie Nebehay, "In a first, China Knocks U.S. from Top Spot in Global Patent Race," *Reuters,* 7 April 2020, https://www.reuters.com/article/us-usa-china-patents/in-a-first-china-knocks-us-from-top-spot-in-global-patent-race-idUSKBN21P1P9

[28] Sidney Leng, "China must stop fooling itself it is a world leader in science and technology, magazine editor says," *South China Morning Post*, 26 June 2018, https://www.scmp.com/news/china/society/article/2152617/china-must-stop-fooling-itself-it-world-leader-science-and

expenditure for many years;[29] this number in the US was around 17 percent in 2017.[30] Despite the striking number of patent filings, Chinese patent applications in ICT accounted for only 8.73 percent of the world total, while the US and Japan respectively accounted for 33.7 percent and 26.73 percent.[31] The different understandings engendered through readings of these figures help explain why the US views China as an equal rival in cyberspace, while the latter thinks of itself as much inferior, further increasing mutual misunderstanding and suspicion.

Aside from the three factors that have resulted in increased rivalry, the lack of internationally accepted cyber norms has made the controversy even more complex. The interpretation of cyber espionage is a good example. The US draws a distinction between cyber espionage for its national security and for economic benefits; while it accepts the former as a legitimate reason to carry out cyber espionage, it repeatedly describes the latter as an unacceptable reason.[32] Despite previously admitting that it conducted espionage on commercial entities, the US has cited national security purposes as the reason.[33] From the Chinese perspective, the line is too subtle since economic security itself is an integral part of national security. China also believes that the line was drawn as such mainly due to Snowden's disclosure of the US' surveillance activities in 2013.

Managing the Competition in Cyberspace

The intensified US-China tensions in cyberspace need to be effectively managed for three main reasons. First, they influence bilateral relations while being influenced by it at the same time. Since concerns in the cyber domain are critical to national interests, increased suspicion will further fasten the current "free fall" status of overall relations. Second, in recent years, both countries have increased their investments in military cyber capabilities and, by some interpretations, have also com-

---

[29] Wei Huang, "Advancing Basic Research towards Making China a World Leader in Science and Technology," *National Science Review*, Vol.5, No.2 (March 2018), https://academic.oup.com/nsr/article/5/2/126/4816745. The statistic is also reiterated by high-level Chinese officials. See, for example: Jill Shen, "China Aims to Be 'Country of Innovators': Science Minister," *TechNode*, 11 March 2019, https://technode.com/2019/03/11/china-strengthen-fundamental-research/

[30] Mark Boroush, "U.S. R&D Increased by $32 Billion in 2017, to $548 Billion; Estimate for 2018 Indicates a Further Rise to $580 Billion," *National Science Foundation,* January 2020, https://www.nsf.gov/statistics/2020/nsf20309/nsf20309.pdf

[31] China Power Project, "Are patents indicative of Chinese innovation?" *Center for Strategic and International Studies,* https://chinapower.csis.org/patents/

[32] Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace," *The Diplomat,* 19 January 2017, https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/

[33] David E. Sanger, "With Spy Charges, U.S. Draws a Line That Few Others Recognize," *New York Times,* 19 May 2014, https://www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html

mensurately adopted more aggressive cyber strategies.[34] As most cyberwarfare experts agree that cyberspace is an offense-dominant domain, it is appealing to initiate an attack first and, in so doing, gain an advantage. Therefore, the possibility of military conflict caused by miscalculations or misunderstandings in cyberspace has increased. Third, countries across the world will be forced to choose a side—as they did during the Cold War—if tensions continue to intensify. This will severely complicate efforts at global governance and norm-setting that will be critical in managing the diverse set of challenges brought on by the increased use of ICTs.

> *"The possibility of military conflict caused by miscalculations or misunderstandings in cyberspace has increased."*

It might be utopian to think it is possible to reset the US-China competition in cyberspace given the current situation. However, there are some actions that the governments can take together to prevent it from being detrimental not only to their bilateral relationship, but also to other actors across the world.

To start with, it is more necessary than ever to fold relevant discussions into existing dialogues at multiple levels. The lack of communication and negotiation channels for the US and China to discuss issues in this domain is a long-standing problem, caused in part by the topic's sensitivity, gaps in opinion, and the aggressive decisions made by both governments. The fact that these concerns are deeply interwoven with those in other areas complicates discussions as well. All of these factors only increase the need for dialogue. Aside from the current functioning but limited information sharing between Computer Emergency Response Teams (CERTs) from the two countries, the Law Enforcement and Cybersecurity Dialogue needs to be resumed as soon as possible to avoid misinterpretation of cybercrimes. The Diplomatic and Security Dialogue can be a channel for high-level officials to express concerns over the other's policy changes, and a platform to share major developments in their capabilities or policies. The Comprehensive Economic Dialogue can serve as the platform to exchange the detection results of cyber IP theft and concerns over

[34] For a useful debate on Chinese and American perspectives regarding cyber capabilities and strategy, see: Lyu Jinghua, "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward,'" *Lawfare,* 19 October 2018, https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward. And a response: Ben Buchanan and Robert D. Williams, "A Deepening US-China Cybersecurity Dilemma," *Lawfare,* 24 October 2018, https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma

cyber-relevant business practices. Moreover, the Memoranda of Understanding between the two Defense Departments can be used to share information on defense policy changes and major exercises, and to explore the possibility of setting ground rules for military conduct in cyberspace.

Because tensions in cyberspace are multifaceted, the two governments must also figure out how to set apart and address different concerns. The current trend of securitizing all concerns can achieve little other than to deprive stakeholders in cyberspace of the opportunity to discuss their interests and put forward solutions. More alarmingly, as it is the least negotiable topic among all debates, the tendency to use ideology as the core standard in determining the legitimacy of cyber-enabled tools will not leave any room to cooperate in potentially mutually beneficial areas. By finding ways to avoid this excessive securitization and use of ideology, the two countries could provide the necessary space for other countries and business actors to make decisions based on the best cost-benefit calculation in each case.

Aside from bilateral negotiations, the two countries need to collaborate on the international stage. For example, malicious cyber activities during the COVID-19 pandemic are an urgent issue that requires multilateral efforts. An efficient joint effort between the US and China will be essential in tackling this issue. On the whole, it is imperative to switch tracks now, before US-China relations in cyberspace irreparably deteriorate. Otherwise, tensions will threaten the digital future of not only the two states, but the entire world.