上海国際問題研究院
SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES

# COMPETITION WITHOUT CATASTROPHE

## *A New China-U.S. Cybersecurity Agenda*

Project Co-directors
Chen Dongxiao
Lu Chuanying

FEB 2021

# About SIIS

Founded in 1960, the Shanghai Institutes for International Studies (SIIS) is a government-affiliated high-caliber think tank dedicated to informing government decision-making by conducting policy-oriented studies in world politics, economics, foreign policy, and international security. SIIS maintains intensive and extensive exchanges and cooperation with research institutions at home and abroad, bolstering China's international influence and soft power.

SIIS boasts an authorized size of 106 full-time research fellows and staff, including 60% senior fellows. SIIS was ranked one of the top ten Chinese think tanks In 2006, and one of the top ten global think tanks (non-American) in 2008. SIIS comprises six institutes and six research centers, namely, the institute for global governance studies, the institute for foreign policy studies, the institute for world economic studies, the institute for international strategic studies, the institute for comparative politics and public policy, the institute for Taiwan, Hong Kong& Macao Studies, the center for American studies, the center for Asia-Pacific Studies, the center for Russian and Central Asian Studies, the center for West Asia and Africa studies, the center for European studies, and the center for maritime and polar studies. SIIS has also set up six in-house research platforms, i.e., the research base on people's diplomacy of Shanghai, center for the study of Chinese diplomatic theory and practice, center for world politics and political parties, center for China-South Asia cooperation, center for BRI and Shanghai studies, and center for international cyber governance. In addition, SIIS is an institutional member of the Shanghai International Strategic Studies Association and the Shanghai International Relations Association.

*Global Review* (bimonthly, Chinese) and the *China Quarterly of International Strategic Studies* are the two flagship journals of SIIS and have become a prestigious academic platform for domestic and international scholarship.

**Taskforce on Cybersecurity Studies**

195-15 Tianlin Road, Xuhui,
Shanghai, P.R. China
021-54614900|www.siis.org.cn

# Taskforce Introduction

## Project Director & Preface Author

**CHEN Dongxiao**, President, Shanghai Institutes for International Studies (SIIS)

## Project Co-director & Contributing Author

**LU Chuanying**, Senior Fellow, Center for International Cyberspace Governance, SIIS

## Contributing Authors

**XU Manshu**, Senior Fellow, Center for International Cyberspace Governance, SIIS

**SUN Haiyong**, Senior Fellow, Institute for Comparative Politics and Public Policy, SIIS

**JIANG Xudong**, Post-Doctoral Fellow, SIIS

**LI Yan**, Senior Fellow, Deputy Director, Institute of Sci-Tech and Cybersecurity Studies, China Institutes of Contemporary International Relations (CICIR)

**YANG Fan**, Deputy Director, Cyberspace International Law Center, Xiamen University

**ZHU Lixin**, Professor, Director, Institute of Rule of Law for Cybersecurity, Xi'an Jiao Tong University

**WANG Tianchan**, Ph.D. student, School of International Relations and Public Affairs, Fudan University

## Translators

**LI Xin**, Managing Editor, *China Quarterly of International Strategic Studies (CQISS)*, SIIS

**YANG Li**, Deputy Editor-in-Chief, *China Quarterly of International Strategic Studies (CQISS)*, SIIS

## Designers

**ZHANG Jun,** Department of International Exchanges, SIIS

**GE Jieyi,** Department of International Exchanges, SIIS

# Safeguarding Strategic Stability to Promote Common Well-being

*Chen Dongxiao*

The issue of cybersecurity has long occupied an important place on the China-U.S. agenda since 2012. Along with considerable attention from the top leaderships, the two governments have established various channels to settle cybersecurity disputes through dialogues and communications. Through a decade's evolution, the connotation of China-U.S. interactions around cybersecurity has been continuously expanding, while challenges constantly grow.

China and the U.S., as two major powers in cyberspace, are faced with common challenges in cybersecurity to a large extent, though inevitably troubled by accompanying divergent interests. With the superimposed effects of technological competition, geopolitical discord and sustained global spread of the coronavirus, the cyberspace governance has witnessed intensified fragmentation, factionalism, and ideological rivalry since 2020, presaging a bleak view for the future.

We, scholars at the Shanghai Institutes for International Studies (SIIS), believe that promoting dialogues, managing disputes and conflicts, strengthening cooperation, safeguarding cyberspace stability and common development serve the interests of both China and the U.S., and should thus be the primary base for bilateral interaction upon transition of the U.S. leadership. In this context, the SIIS Center for International Cyberspace Governance opted to lead a joint taskforce on cybersecurity studies with academic input of senior scholars in prestigious Chinese think tanks, in an attempt to make a preview of Biden's cyber policy and its impact on China-U.S. cyber dynamics, with policy recommendations toward promoting strategic stability and prosperity in cyberspace.

According to the report, the Biden administration would partially return to the Obama era cyber strategy, along the lines of reinstating the White House leadership and strengthening departmental coordination, stressing cybersecurity as a crucial national security issue, as well as fortifying governance capacity of the U.S. in the cyberspace and digital era through revitalized public-private partnership, alliance collaboration and multilateral diplomacy, etc.

Meanwhile, the report also argues that although Biden would calibrate the cyber policy of his predecessor, the new administration would largely inherit Trump's China policy, including that in the area of cyberspace and digital field, and particularly hang on to Trump's legacy of "containment and suppression" of China. This prospective policy direction will almost assuredly induce complexities to the overall China-U.S. relations, including the bilateral dynamics in cyberspace and the digital domain. Predictably, fierce competitions between China and the U.S. will continue in the cyber digital transformation, among which the contest for cyberspace rule-making will be further intensified. What's more, the U.S. behavior of high toning the so-called China-U.S. ideological conflict will for sure to severely impede bilateral efforts in promoting stable cyber relations.

For the purpose of safeguarding China-U.S. strategic stability and advancing shared interests in cyberspace and the digital domain, this report makes a list of policy recommendations as follows. First, to resume cyber-related dialogues and consultations. In particular, mechanisms for bilateral talks should be restored and strengthened over issues of shared interests and common concern, such as digital trade, cross-border data flows, combating cybercrime, and regulating state behavior in cyberspace. Second, to rebuild confidence building measures (CBMs). CBMs between the Chinese and American militaries may include restoring and reinforcing mechanisms for crisis prevention, risk control and reduction. Third, to reassure the value of international law as normative guidelines in the global governance of cyberspace and the digital domain. In coordinated practice and common application of "international law of co-existence" and "international law of co-operation", the two sides should work to define legal norms at times of crisis and step up consensus-building process of international law in areas of shared interests and common concern. Fourth, to revitalize agenda for China-U.S. cooperation on digital trade. The to-do list for collaboration may include designating anti-pandemic efforts to digital trade interactions, initiating "China-U.S. Digital Trade and Public Health Alliance", jointly setting new rules for e-commerce, and building a win-win scenario in digital infrastructure projects. Fifth, to reshape China-U.S. coopetition in cyberspace and science & technology. Both sides should work to revive high-level STC (science and technology cooperation) dialogues on emerging industries with focus on technological collaboration in areas concerning human well-being, and jointly decide on a rational borderline between STC and national security.

As year-round observers on China-U.S. cyber relations, the authors of this report have put forward questions which reflect the key cyberspace challenges that currently exist between the two countries. Similarly, it is in our belief that the policy recommendations initiated in the report would be of significant reference to the Biden administration's efforts in managing cyber and digital competition, expanding areas of cooperation, advancing cyber CBMs, and achieving China-U.S. strategic stability & common development in cyberspace.

# Competition without Catastrophe

## *A New China-U.S. Cybersecurity Agenda*

Since the Sunnylands summit between Chinese President Xi Jinping and then U.S. President Barack Obama in June 2013 when the two leaders discussed cybersecurity for the first time and reached a number of agreements, cyberspace has become a domain receiving constant strategic attention from both sides. From the Obama terms to the Trump administration, as bilateral interactions expanded to feature cyber-related issues, be it cybercrime or norms on cyber behavior, Beijing and Washington have come to realize that a stable China-U.S. relationship in cyberspace would have much broader implications for the political security, economic well-being, and social stability of both nations.

In the Obama era, multiple mechanisms were established for dialogues on cybersecurity, not least the high-level joint dialogue mechanism on fighting cybercrime and related issues, which helped stabilize the overall ties. With the launch of the first U.S.-China Law Enforcement and Cybersecurity Dialogue in October 2017, this positive momentum had continued in the Trump administration until Washington started a trade war by imposing punitive tariffs on a wide range of Chinese products in early 2018. In the ensuing years, as the rivalry intensified, almost all official dialogue mechanisms were suspended. Chinese individuals and tech companies, such as Huawei, ByteDance, and Tencent—facing indictments and restrictions for their alleged role in threatening U.S. national security—were among the hardest-hit victims of the escalating bilateral tensions.

The Trump administration had depleted the modicum of mutual trust accumulated through continued cybersecurity cooperation during Obama's second term, and turned nearly every cyber-related issue, such as the digital economy, into a potential source of strategic rivalry.

As cybersecurity remains high on President Biden's national security agenda, this report expects no radical departure from former President Trump's cyber policy in the next four years. Competition will continue to be the defining feature of China-U.S. cyber interaction in the Biden administration, as it had been during the Trump term. At the same time, initial signals from Beijing and Washington have indicated that there is still significant scope for cybersecurity cooperation in the years to come. While Beijing has made clear that it has never closed the door of cooperation, Washington has also emphasized that the U.S.-China rivalry will "not put global stability at risk," including the cyberspace. The Biden administration is expected to approach cyber issues in a more rational and comprehensive way, gradually resume cybersecurity dialogues between Beijing and Washington, and work toward a bilateral cyber relationship characterized by "competition without catastrophe."

The authors make a number of policy recommendations to both governments on some major cyber issues of strategic importance, including cyberspace governance, military confidence building, domestic legislation and international rule-making, digital trade, and digital technology competition,

in the hope of facilitating a more stable and positive cyber relationship between Beijing and Washington.

## Biden's Cyber Policy: A Preview

After four tumultuous years of the Trump presidency in which cybersecurity had been crowded out by other agendas deemed more existential, especially in the aftermath of the SolarWinds cyber breach in late 2020, the Biden administration is now under enormous pressure to make cybersecurity a front-and-center issue in its foreign policy agenda.[1] Biden's decades-long career in foreign affairs, as a seasoned Senator at the Foreign Relations Committee and then Obama's deputy, would also help the new administration restore a certain measure of discipline and coherence to a cyber strategy that is most likely to be organized along the following lines of effort.

First, reinstating the White House leadership in cybersecurity to coordinate the implementation of cyber strategy. The Trump administration faced a strong bipartisan backlash over its decision to terminate the White House cybersecurity coordinator position in 2018, a move considered to be a major backward for cybersecurity policy.[2] Since then Democratic and Republican members of Congress have been calling for restoration of the post and the National Defense Authorization Act 2021 includes a recommendation of the Cyberspace Solarium Commission on creating a larger, more empowered Office of the National Cyber Director in the White House. This Senate-confirmed National Cyber Director will be the president's principal adviser for cybersecurity-related issues and lead national-level coordination of cybersecurity strategy and policy. The Biden administration is expected to implement the recommendation in its early days to elevate cybersecurity as an imperative across the government.

Second, forging a stronger public-private partnership to better integrate domestic resources. The Democratic Party's 2020 Platform makes it clear that the new administration will work with the private sector to protect individuals' data and defend critical infrastructure.[3] Building on the party's longstanding close relationship with tech firms, which had been alienated during the Trump years, the Biden administration is expected to renew its partnerships with the private sector by sharing threat information and expanding investment in critical infrastructure and key technology to defend against

---

[1]Caitlin Chin, "After the SolarWinds hack, the Biden administration must address Russian cybersecurity threats," Brookings Institution, January 11, 2021, https://www.brookings.edu/blog/techtank/2021/01/11/after-the-solarwinds-hack-the-biden-administration-must-address-russian-cybersecurity-threats/.
[2]Tim Starks, "Dems Launch bid to undo White House Cybersecurity coordinator elimination," *Politico*, May 18, 2018, https://www.politico.com,https://www.politico.com/newsletters/morning-cybersecurity/2018/05/18/dems-launch-bid-to-undo-white-house-cybersecurity-coordinator-elimination-222934.
[3]2020 Platform Committee, "2020 Democratic Party Platform," July 27, 2020, p. 81, https://www.demconvention.com/wp-content/uploads/2020/08/2020-07-31-Democratic-Party-Platform-For-Distribution.pdf.

malicious cyberattacks.[4] To present a united front against rival cyber powers like Russia and China, as Biden repeatedly suggested on the campaign trail, the new administration will also have to find the largest possible common ground between tech companies' business interests and U.S. national security interests.[5]

Third, repairing alliance and partnership in Europe and Asia for coordinated cyber action. President Trump's "America First" doctrine has dealt a devastating blow to Washington's postwar alliance system across Europe and Asia. As an establishment politician and veteran foreign policy hand, President Biden will try to revitalize decades-old alliance and partnership with European and Asian nations by focusing on some common threats, including persistent cyberattacks.[6] The new administration will prioritize strategic coordination with the European Union and NATO on specific cyber issues to facilitate common actions based on mutual benefit and reciprocity.[7] As Secretary of State Antony Blinken put it during his confirmation hearing, cyber issues would be put at the heart of American diplomacy and Washington would strengthen coordination with allies and partners on digital trade, use of force in cyberspace, and international rule-making regarding cybercrime.[8]

Fourth, promoting multilateralism while taking back leadership in global cyberspace governance. During the campaign, Biden pledged that he would "resuscitate efforts to foster international agreements about the responsible uses of new digital tools, reenergize efforts to establish comprehensive cyber norms against attacks on civilian infrastructure, and make America a leader in encouraging others to adopt principles of responsible state behavior in the cyber domain."[9] The new administration is committed to putting America back in the leadership position in major global organizations, such as the WTO and OECD, to "shape the rules, agreements, and institutions that guide international relations." As the Democratic administration sees it, the world does not organize itself and if Washington does not engage and lead, other powers will fill the void and shape the rules, norms, and institutions in cyberspace to the detriment of U.S. interests. The new administration must work with allies to mobilize more than half the world's economy to stand up to China and negotiate

---

[4]Joe Biden, "Statement by President-elect Joe Biden on Cybersecurity," *Press Release*, December 17, 2020, https://buildbackbetter.gov/press-releases/statement-by-president-elect-joe-biden-on-cybersecurity/.
[5]Samuel J. Palmisano and Kiersten E. Todt, "A cybersecurity agenda for the Biden administration," *Fortune*, December 9, 2020, https://fortune.com/2020/12/09/cybersecurity-agenda-defense-biden-administration/.
[6]2020 Platform Committee, "2020 Democratic Party Platform," July 27, 2020, p. 57; and Evelyn Cheng, "Biden's pick for foreign policy head affirms a push to get allies on board with U.S. policy on China," CNBC, November 24, 2020, https://www.cnbc.com/2020/11/24/bidens-blinken-pick-implies-changes-for-us-foreign-policy-on-china.html.
[7]Lauren Zabierek and Julia Voo, "The Case for Increased Transatlantic Cooperation on Artificial Intelligence," Belfer Center for Science and International Affairs, August 2020, https://www.belfercenter.org/publication/case-increased-transatlantic-cooperation-artificial-intelligence.
[8]"Full Committee Hearing: Nomination," Senate Foreign Relations Committee, January 19, 2021, https://www.foreign.senate.gov/hearings/nominations-011921.
[9]Eric Geller, "Biden prepping to ramp up U.S. cyber defenses — while keeping some Trump policies," *Politico*, August 20, 2020, https://www.politico.com/news/2020/08/20/joe-biden-cyber-defenses-399530.

from the strongest possible position.[10]

## China-U.S. Cyber Dynamics in the Biden Era

China-U.S. cyber relations had turned confrontational under the impact of the trade war, technology blockade, and coronavirus pandemic during the Trump administration. Some of the cyber dialogue mechanisms could be restarted as the Biden administration is expected to tone down the harsh anti-China rhetoric of its predecessor. But on the other hand, given the strong bipartisan consensus on the growing "China threat," the Biden White House will carry on some elements of Trump's China policy.

First, intensifying ideological rivalry will be a severe handicap to the stability of bilateral cyber relations. A Democratic administration, sticking to the party's longstanding values-based approach to foreign policy, is expected to continue criticizing Beijing for its "repressive" cyber policy that allegedly undermines freedom, openness, democracy, and human rights. The Biden administration is also likely to retain and reinforce the restrictive measures against Chinese tech companies to push back against Beijing's so-called "digital authoritarianism."[11] Moreover, the world could be divided into two competing technology camps as Washington continues to push for a value-based techno-democratic alliance and accelerates China-U.S. technology decoupling. The Biden administration could also step up promoting Western values along the Belt and Road, increasing the costs for Beijing to promote a digital silk road.

Second, the contest for rule-making power will also intensify as Washington tries to take back its leadership position in cyberspace governance. The Biden administration will empower its cyber diplomatic agencies to allow the United States to lead international cooperation in cyberspace at the expense of Beijing's role and influence in cyberspace governance. The Global Partnership on Artificial Intelligence and AI Partnership for Defense that were launched during the Trump administration are expected to be strengthened as valuable instruments of American cyber power to preserve and consolidate Washington's superiority in emerging technologies. These exclusionary groupings will certainly stand in the way of China-U.S. technology cooperation in the Biden term.

Third, as the Biden administration sees it, cybersecurity must serve national security and economic well-being to preserve U.S. strategic advantage over China. The Biden team shares Trump's perceptions on cyber development and security and remains committed to implementing a cyber strategy in the service of economic and national security at home and maintaining America's superiority in the global

[10]2020 Platform Committee, "2020 Democratic Party Platform," July 27, 2020, p. 85.
[11]Erol Yayboke and Samuel Brannen, "Promote and Build: A Strategic Approach to Digital Authoritarianism," Center for Strategic and International Studies, October 15, 2020, https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism; and Aidan Powers-Riggs, "Covid-19 is Proving a Boon for Digital Authoritarianism," Center for Strategic and International Studies, August 17, 2020, https://www.csis.org/blogs/new-perspectives-asia/covid-19-proving-boon-digital-authoritarianism.

technology landscape vis-à-vis China and Russia. The Biden administration will try to curb Beijing's ICTs (information and communications technology) development through domestic legislation and international rule-making to consolidate U.S. firms' competitiveness over Chinese counterparts.

## A New Cybersecurity Agenda: Logic and Approach

Restoring and initiating cyber dialogue mechanisms at different levels. Intensified China-U.S. competition in cyberspace does not necessarily preclude cooperation on a wide range of cyber-related issues, which concern not only both nations' core interests but also the healthy development of cyberspace as a whole, for example, digital trade, cross-border flows of data, cybercrime, and norms for state behavior in cyberspace.[12] It serves the common interests of Beijing and Washington to work together on cyber risk control and address common cyber threats, as both want to ensure that growing competition does not put strategic stability in cyberspace at risk.[13] The global cyberspace governance process that had been hampered during the Trump presidency, is also likely to be revitalized under the administration of a Democratic president, whose party has long valued international institution building. Against this backdrop, China and the U.S. ought to step up dialogue and communication on the cyber issues of common interest with a particular focus on the following four areas.

First, restoring the bilateral cyber dialogue mechanisms, especially communications at high levels at an appropriate time. Beijing and Washington should strengthen agenda setting by fostering communication and cooperation on the latest cyber-related developments, such as the digital economy, data flows, and emerging technology applications.

Second, working together to improve relevant institutions under the UN framework. Despite its many shortcomings, the United Nations' legitimacy and authority should not be undercut. As permanent members of the UN Security Council, China and the United States must help improve the UN's cyber-related institutions to bolster its role in global cyberspace governance.

Third, building up platforms to jointly tackle global cyber threats and risks. As a new generation of technology emerges, in particular the increasing application of AI (artificial intelligence) and internet of Things, risks and threats with potential systematic implications have also been growing in cyberspace. China and the United States should set up relevant cooperative institutions for information sharing, prospective evaluation and coordinated response to fend off the rising problems.

---

[12]Cai Cuihong, "Geopolitics in Cyberspace: a new perspective on Sino-American relations [网络地缘政治:中美关系分析的新视角]," *Journal of International Studies*, No. 1, 2018, p. 40.
[13]Chen Dongxiao, "How to build a sustainable and resilient China-U.S. relationship in the Biden administration [拜登执政后如何重建可持续和富有韧性的中美关系]," U.S.-China Perception Monitor, December 23, 2020,
https://www.uscnpm.com/model_item.html?action=view&table=article&id=23807.

Fourth, encouraging communication and cooperation among multiple stakeholders in cyberspace. Cyberspace is so complicated and sophisticated a domain that even the world's two major powers are not able to solve all of its problems solely at the governmental level, either alone or jointly. The United States and China should create a hospitable policy environment to invite multiple actors' involvement in response to various cyber challenges, and ensure that politicization and securitization will not stand in the way.

Promoting military confidence building in cyberspace. Cyber strategic stability depends, to a large degree, upon the way in which strategic rivals engage with each other. Positive competition in cyberspace rests on strong mutual trust.[14] Many technical features of cyberspace, for example, anonymity, trans-boundary, and easy access, have made confidence building in cyberspace a daunting task for all actors.[15] When there is little strategic trust between two cyber forces, a tiny cyber accident may lead to strategic misjudgment and even military crisis. Therefore, confidence building between the Chinese and American militaries has become an imperative.

First, opening a diversified mechanism for communication to address cyber contingencies. As the western countries establish and employ mechanisms for peacetime crisis communication as important measures of cyber confidence building, Beijing and Washington could follow this model by setting up a liaison mechanism between the Cyberspace Administration of China and the U.S. Department of Homeland Security that involves designation of liaison officers, hotlines, and emails, as a direct communication link between high-level leaders in times of severe cyber crisis. This mechanism could serve as a supplement to existing crisis communication channels or as a new Track One mechanism focused on promoting strategic transparency.

Second, restarting military-to-military dialogues centered around crisis management. As crisis prevention serves the interests of both sides, Beijing and Washington must exercise strategic restraint and guard against any third-party actors, whether nation-states, organizations, or individuals, stirring up trouble in cyberspace. Both sides could supplement the Memorandum of Understanding on Notification of Major Military Activities Confidence-Building Measures Mechanism and the Memorandum of Understanding Regarding the Rules of Behavior for Safety of Air and Maritime Encounters with annexes on cybersecurity crisis notification and rules of behavior for safety in cyberspace. Following the model of the U.S.-U.S.S.R. agreement on the Prevention of Incidents On and Over the High Seas of 1972, China and the United States could also negotiate a bilateral agreement on the rules of engagement between the two militaries in cyberspace to help better perceive and interpret one another's cyber behavior, capabilities, and intentions, with a view to keep cyber incidents from

[14]Xu Manshu, "Reflections on promoting cyber strategic stability [促进网络空间战略稳定的思考]," *Information Security and Communications Privacy*, No. 7, 2019, p. 6.
[15]Lu Chuanying, "Security dilemma, misperceptions, and path choices in great power cyber relations [网络空间大国关系面临的安全困境、错误知觉和路径选择——以中欧网络合作为例]," *Chinese Journal of European Studies*, No. 2, 2019, pp. 120-121.

escalating into larger-scale crises or conflicts.

Third, focusing on the military application of emerging technologies to ease the security dilemma. The increasing application of ICT for military purposes is an unstoppable trend, exerting a far-reaching impact on traditional and emerging war-fighting domains like space and nuclear.[16] Chinese and U.S. military research institutions could conduct joint study and exchange programs focusing on the potential strategic risks and threats brought by emerging technologies, like drone, AI, and brain science, in order to prevent humanitarian crises and alleviate the security dilemma caused by the diffusion and abuse of new technology.

Applying international law to cyberspace. Though difficult to draw the line between international legal system and international political system, international law, as the primary legal form in the anarchical world society, can still influence states' calculation and decision-making with its innate normativity. Hence China and the U.S. should coordinate strategies on the application of international law with an effort to promote strategic stability in their bilateral cyber relations.

First, applying international law of co-existence to define legal norms at times of crisis. Concerning the issues at the core of national security interests, such as cybersecurity of nuclear command, control and communication (NC3) systems, China and the U.S. can work to draft binding international norms in form of prohibitory rules, clarifying the legal criteria and specifying state responsibility, so as to shape conceptual consensus and guiding principles for prevention of such crises. With regard to those key legal issues hard to reach consensus in the short term, yet influential to the state cyber behaviors, such as legal standards of cyberattack intensity and legal criteria for legitimate self-defense and countermeasures in response thereto, the two sides can, at the least, strengthen communications through dialogues of various channels, expounding their respective national stance in published forms. This may serve as evidence of meaningful international law practice, as well as a means to increase transparency and mutual trust.

Second, applying international law of co-operation to promote substantive legal collaboration. With regard to those cyber issues of shared interests, such as protecting critical infrastructure from cybersecurity threats, addressing cyberspace vulnerabilities and fighting transnational cybercrimes, China and the U.S. may strengthen the creations of norms that reflect common grounds to expand areas of cooperation in international law. As for those cyber issues with certain level of tangled interests but larger degree of divergence in the distribution thereof, such as ICT standards setting, cyber supply chain risk management (C-SCRM), balancing privacy protection & data security in cross-border data flow, etc., both sides are suggested to explore mutually accepted bottom-line rules, so as to reserve space for more extensive and open collaboration in the future. Such bottom-line initiatives may first focus on

[16]Zhou Hongren, "On strategic stability in cyberspace [网络空间的崛起与战略稳定]," *Global Review*, No. 3, 2019, pp. 21-34.

regulatory constraint on the extent and range of unilateral actions, especially those detrimental due to their arbitrariness but are justified, often too easily, by the expansive use and misuse of national security excuse.

Third, drafting mutually recognized technical safety regulations, trade rules and safety standards through domestic legislation. Mutual trust in cyberspace can be accumulated through respect to sovereignty, jurisdiction, data security management, enhancing supervisions on Internet companies, implementing commonly recognized security standards or credible standards, etc. International cooperation in specific areas, such as export control on sharing vulnerability information and cross-border access to e-evidence for combating cybercrime, can all be enhanced with certain degree of compromise from both sides.

Promoting digital trade as new increment of China-U.S. cooperation. Economic and trade cooperation has been the cornerstone of China-U.S. relations. With the Biden administration in place, the two sides should work to repair the trade relations and promote bilateral cooperation in trade and economy to the direction of expanding mutual benefits. Along this line, digital trade could potentially become a new increment of China-U.S. trade cooperation and a new impetus towards win-win collaboration between the two countries.

First, designating anti-epidemic efforts as an area of bilateral digital trade collaboration. The Biden administration has shared interests with China on fighting the pandemic and safeguarding global health governance. President Biden guaranteed the U.S. return to the World Health Organization (WHO) and placed pandemic-fighting as top priority on the to-do list of his administration. In line with the priority of the new U.S. administration, trade cooperation can help promote public health amid the pandemic. Among other potentials, initiation of a "China-U.S. Digital Trade and Public Health Alliance" could encourage bilateral collaboration on biology- and health-related enterprises by employing the convenience of digital business platforms, e.g. in clearance, record-keeping and logistics, etc. The application of digital technology could cut costs and increase efficiency, thus amplifying China-U.S. trade and public health cooperation positivity.

Second, referencing the existing U.S.-Europe mode of data transfer to facilitate the China-U.S. data arrangement. At present, the lingering disagreement in data security has posed serious threat to the stability of China-U.S. economic and trade cooperation. As the bilateral agreement on data transfer is still pending with unresolved disputes, China and the U.S. can make reference to the E.U.-U.S. Standard Contractual Clauses (SCC) to stabilize commercial exchanges between the enterprises. Should political discord further arise, the SCC model could still facilitate regular collaboration at the civilian level.

Third, setting new rules for e-commerce within the WTO framework. As the Biden administration expedited the WTO negotiations on e-commerce rules, a small coterie of U.S., Japan and Europe has

been formed aiming to set high-standard rules favorable to their interests, posing grave challenges to the "China solution."[17] In response, China should aim to safeguard the right of developing countries by promoting inclusiveness in the multilateral rules for digital trade, while proactively negotiating related issues with the U.S.

Fourth, working toward a win-win situation in the field of digital infrastructure. With the boom of digital economies, the Biden administration will likely resort to regional alliances to promote "digital partnerships" and increase foreign investment in digital infrastructure through intelligent city projects. Though challenges may arise from such U.S. endeavors to China's "digital silk road" initiative, China should take open-minded gestures along the line of China-U.S. "co-opetition" posture. Neither China nor America can single-handedly take on all digital infrastructure projects, and a large project is bound to open up opportunities for collaboration in sub-items. While seeking chances for big projects, China could also look for proper participation in U.S.-led subprojects as a potential form of cooperation.

Facilitating healthy competition in science and technology. Since 2018, China-U.S. competition in science & technology has exacerbated and spilt over into other areas. What's even worse, such competitions got mixed with the geopolitical divergences between the two countries, which have cast negative impacts on regional security and global economy & politics as a whole.[18] Given these contexts, a healthy competitive pattern needs to be worked out between China and America, which avails to dispute control, promotes mutual benefit and win-win scenario, and facilitates global economic recovery.

First, strengthening high-level dialogues in science and technology cooperation (STC). As the new round of scientific revolution brings out emerging industries of artificial intelligence and big data, there comes great potentials for bilateral cooperation with existing complementary strengths between the U.S. sophisticated technology and China's abundant data and application scenarios. To expand mutually beneficial cooperation and alleviate political restraints harmful to both sides, topics like export control, investment regulations on science & technology companies as well as enterprise compliance could all be put on agenda of the China-U.S. high-level consultations.

Second, promoting technological collaboration in areas concerning human well-being. Firstly, bilateral collaboration on climate change should be expanded. Be it technology of climate change monitoring and evaluation, negative emissions or carbon capture, China and the U.S. foresee extensive ground of shared interests, upon which, mechanisms of dialogues should be put into place. Secondly, as coronavirus remains a persistent global challenge, China and the U.S. should expand spaces for collaboration on vaccine development and modification to strengthen control on the pandemic and

[17]Xu Chengjin, "WTO e-commerce negotiations & China solution [WTO 电子商务规则谈判与中国的应对方案]," *World Economic Review*, No. 3, 2020, p. 57.
[18]Wei Zongyou, "China-U.S. strategic competition: American anxiety & Trump's China policy [中美战略竞争、美国'地位焦虑'与特朗普对华战略调整]," *American Studies*, No. 32, 2018, pp. 51-74.

pave the way for future prevention. Thirdly, the two states can explore collaborative agendas in space-related technology, and with this as the foundation, build toward international space collaboration community, which would involve more countries' contribution for the well-being of humankind.

Third, promoting cooperation on global governance of science and technology, where shared responsibilities and immense potentials stand. With regard to the digital infrastructure and ICT security, the two countries can set up agendas for governance.[19] In specifics, both sides can explore the possibility of creating an authoritative organization to supervise, evaluate and verify security risks confronting digital infrastructure. This process can involve participation of related countries, specialized international agencies and corporations concerned, in order to gather opinions of diversified actors in the establishment of international ICT security supervision institution. With such mechanism in place to scrutinize equipment security from suppliers, the concerns over digital infrastructure security can be expected to ease, which may help mitigate China-U.S. tensions in science and technology.

[19]Sun Haiyong, "U.S. sci-tech blockade & China in digital infrastructure collaboration [美国对华科技施压与中外数字基础设施合作]," *Contemporary International Relations*, No. 1, 2020, pp. 41-49.

## References


1. Karahan S, Wu H, Armistead L. "Evolution of US Cybersecurity Strategy" [C]//ICCWS *2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019.* Academic Conferences and publishing limited, 2019: 168.
2. Qian X. "Cyberspace security and US-China relations" [C]//*Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science.* 2019: 709-712.
3. Schneider J. "A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem" [J]. *The Washington Quarterly,* 2020, 43(2): 159-175.
4. Hoffman W. "Is Cyber Strategy Possible?" [J]. *The Washington Quarterly,* 2019, 42(1): 131-152.
5. Boylan B M, McBeath J, Wang B. "US–China Relations: Nationalism, the trade war, and COVID-19" [J]. *Fudan Journal of the Humanities and Social Sciences,* 2020: 1-18.
6. Zaidi S M S, Saud A. "Future of US-China Relations: Conflict, Competition or Cooperation?" [J]. *Asian Social Science,* 2020, 16(7): p1.
7. Beckley M. "The End of the Affair: US–China Relations Under Trump" [M]//The Trump Doctrine and the Emerging International System. *Palgrave Macmillan, Cham,* 2020: 227-245.
8. Klimburg A, Faesen L. "A Balance of Power in Cyberspace" [J]. *Governing Cyberspace,* 2020: 145.
9. Consolati J J. "Understanding Structures of Cyber Competition in an Era of Major Power Rivalry" [R]. *Lawrence Livermore National Lab.*(LLNL), Livermore, CA (United States), 2020.
10. Ma W. "The Digital War: How China's Tech Power Shapes the Future of AI, Blockchain and Cyberspace" [M]. *John Wiley & Sons,* 2020.
11. Jiang Tianjiao, "China-US Cyberspace Gaming and Strategic Stability" [J]. *Information Security and Communications Privacy,* 2020(09):11-17.
12. Lu Chuanying, "China-US Competition in Science and Technology: Historic Logic and Future Prospects" [J]. *China Information Security,* 2020(08):70-73.
13. Li Zheng, "China-US Decoupling in Science and Technology: Causes and Trends" [J]. *Contemporary International Relations,* 2020(01):33-40+32+60.
14. Wang Shoudu, "On China-US Strategic Stability in Cyberspace: Political Factors in US Cybersecurity Governance under Trump" [J]. *Information Security and Communications Privacy,* 2019(11):46-59.
15. Zhang Tengjun, "Trump's Cybersecurity Policy Adjustment" [J]. *International Review,* 2018(03):64-79.
16. Cai Cuihong, "Cyber Geopolitics: A New Perspective for Sino-US Relations" [J]. *The Journal of International Studies,* 2018,39(01):9-37+5.
17. Zhang Shu & Liu Hongmei, "Comparative Studies on China and US Cybersecurity Policies" [J]. *Information Security and Communications Privacy,* 2017(05):68-79.
18. Lu Chuanying, *Global Cyberspace Governance and Multi-stakeholders: Theories and Practices* [D]. East China Normal University, 2016.
19. Wang Xiaofeng, "Adjustment of US Cybersecurity Strategy vs. China-US New Model of Major-countries Relations" [J]. *Contemporary International Relations,* 2015(06):17-24+63.
20. Lang Ping, "Global Cyberspace Rule-making: Cooperation and Competition" [J].*World Outlook,* 2014(06):138-152+158.
21. Cai Cuihong, "China-US Relations in Cyberspace: Competition, Conflict and Cooperation" [J]. *The Chinese Journal of American Studies,* 2012,26(03):107-121+5.
22. Yi Wenli, "China and US in the Cyberspace: Divergences and Path to Cooperation" [J]. *Contemporary*

*International Relations,* 2012(07):28-33.

23. Stuart Patrick & Yang Wenjing, "Reform on Global Governance & US Leadership" [J]. *Contemporary International Relations,* 2010(03):54-62.
24. Shi Yinhong, "US Power, China Rise and World Order" [J]. *International Studies,* 2007(03):28-32+38.

Taskforce on Cybersecurity Studies



195-15 Tianlin Road, Xuhui,

Shanghai, P.R.China

021-54614900|www.siis.org.cn