U.S.-CHINA TRACK II DIALOGUE ON THE DIGITAL ECONOMY

CONSENSUS AGREEMENT

December 2-4, 2020
Zoom meeting

The National Committee on U.S.-China Relations, together with the China Institute for Innovation & Development Strategy, the Fuxi Institution and the Guanchao Cyber Forum, convened their third Track II Dialogue on the Digital Economy virtually through Zoom on December 2 and 3, 2020 (December 3 and 4, 2020 in China). The dialogue brought together U.S. and Chinese experts from academia, think tanks, and industry for non-governmental, off-the-record, in-depth discussions on digital economy issues of concern to both countries: 1. Key issues in the U.S.-China digital economy relationship; 2. Global supply chain and core technologies/semiconductors. (See attached name list.)

Over the two days of dialogue, the two sides actively explored how to define the common issues faced by both countries in the digital economy and how both governments could advance a common agenda for moving forward on a range of difficult issues. This document is a distillation of those discussions and recommendations.

PART I

Fundamental principles of U.S.-China interaction in the digital economy: what we strive to achieve in the long-run

As the two leading nations in the digital economy, the United States and China have overlapping long-term objectives. They both aim to pursue and commit to the goals of building and maintaining one global Internet; supporting open global technology supply chains; ensuring the free flow of data with trust; guaranteeing a level playing field for technology companies, capital, and entrepreneurs; and allowing technology firms to operate and innovate globally.

At the same time, while desiring openness and globalization, both countries need to address national security concerns posed by the digital revolution and the advent of advanced high capacity mobile telecommunications systems and artificial intelligence. Actions to protect such concerns will have an impact on the digital economy in specific ways: by limiting the ability of foreign firms to provide equipment or services for technological infrastructure; by limiting the transfer of data; by denying certain countries access to sensitive controlled technologies for national security reasons; and by restricting or disrupting supply chains.

We hope that this track II dialogue, and this document, can help our two countries develop the foundations for mutual trust to deal with the many concerns relating to the digital economy.

PART II

Current Trends and Challenges

We acknowledge the trends within the current situation are leading to a quite different outcome from the principals and aspirations stated above. We note the following ongoing actions by both the Chinese and U.S. governments in the digital economy sphere:

- Intensified restrictions on multinational corporations. Increasing imposition of restrictions on the ability of companies headquartered in the other nation to conduct normal business operations.
- The use of increasingly broad definitions of national security that result in restrictions around the supply of technology for companies operating in each country.
- Restrictions on data flows, including data localization rules, unclear data classification, and privacy rules.
- Restrictions on scientific research collaboration, including restrictions on the sharing of research data with scientists from other countries and limiting foreign students' and scientists' access to domestic universities and research centers.
- Preferential policies toward local technology companies. Preferencing domestic technology companies over foreign counterparts via standards, subsidies, investment reviews, national and local procurement procedures, security reviews, non-tariff measures, and other tools.
- Continuous disagreement on both the standards for determining critical issues, such as intellectual property infringement, forced technology transfer, cyber theft of IP, and appropriate remedies.
- Continued sophisticated cyber espionage activity that targets each nation's critical infrastructure and intellectual property.

While both countries have legitimate national security interests that often converge, differences also arise from diverging fundamental interests in both countries, including the definition and scope of national security. Different economic systems, political regimes, and stages of development drive different actions by each country and opposition to the actions of the other country. Examples of these are:

- China has the first or second largest market for most technology products, while U.S. companies control a plurality of advanced core technologies such as logic semiconductors and semiconductor manufacturing tools.
- The Chinese government objects to the restrictive actions that the United States government has taken in the digital economy sphere based on issues outside of the digital economy, including human rights concerns.
- The United States government objects to the actions that China takes to favor Chinese companies both in its own market and overseas, and the extraterritorial application of provisions in China's National Security Law, National Intelligence Law, and Data Security Law (Draft) that have implications for the digital economy.

Because of the asymmetry in each country's concerns, objectives and development levels, a simplistic approach of "reciprocal rules" will not lead to significant progress in resolving the above described issues. Only emphasizing on "reciprocity" likely would lead to collective and additional restrictive effects, forming a vicious circle that will inevitably lead to further separation/decoupling between the Chinese and U.S. digital economies, with the attendant negative impact of increased cost of doing business, less consumer choice, increased political friction, and weakened innovation and creativity. We will therefore need to develop agreements that are fair to each side but tailored to each country's distinct concerns.

PART III

The Foundation for Digital Economy Collaboration: Areas where our Dialogue identified potential alignment

Despite the recent negative momentum, Dialogue participants identified areas of converging goals and potential alignment that can be further developed. We believe that by pursuing a clear consensus and definitive agreement on such areas, we can achieve positive initial momentum that both sides can then leverage to solve more difficult issues. We list below areas of potential alignment, as well as how such alignment could be leveraged to develop a concrete consensus and agreement.

1. **Definition and Boundaries of National Security Interests in the Digital Economy.** The digital economy touches on many matters that can affect a nation's national security. However, it is important that those concerns be narrowly defined so as not to negatively affect the development and growth of the global digital economy. We can begin to define the demarcation between the technology infrastructure, data and supply chains that are relevant to national security, and those which are not. National security concerns cannot become a "catch-all" to advance other trade and industrial policy objectives. In the long run, we aim for the national security relevant restrictions to cover a minimal portion of the global digital economy. One manifestation of this alignment should be the establishment of a joint working group that debates, clarifies, and communicates the definition of national security in the digital economy, so that both countries are aware of each other's "red lines."

2. **Kickstarting and Resuming Scientific Collaboration, Supporting and Guaranteeing the Freedom of Scientific Research.** We can renew scientific collaboration in areas of joint interest, including the free flow of scientific data according to professional norms between U.S. and Chinese teams and reaffirming support for the global scientific community. A manifestation of this alignment could be the identification of several areas of high priority collaboration (such as a COVID-19 vaccination development and deployment process and launching a digital health science project to jointly combat the pandemic); and the sharing of such data with a jointly staffed scientific working group.

3. **Industrial Support Transparency in Key Technology Areas.** We can find a means for moving to mutual disclosure of all subsidies leveled by governments and government-linked commercial actors (e.g., government funded private equity funds) in the digital economy. A potential manifestation of this would be meeting our mutual commitments to multilateral and industrial mechanisms such as the World Trade Organization (WTO) and the Government and Authorities Meetings on Semiconductors (GAMS) to report on industrial subsidies in the semiconductor industry, and for China to join as soon as possible and support the WTO Government Procurement Agreement Framework. There are a number of well-developed and accepted frameworks for addressing the subsidies issue in particular technology sectors.

4. **Opening up Regulated Data Flows.** Companies and organizations on both sides cannot flourish sustainably within an environment whereby data generated in China never reaches the United States, nor whereby U.S.-generated data never reaches China. China and the United States have the largest data flows across borders. We can agree on data-sharing agreements, for both government and private enterprise purposes, facilitated with appropriate safeguards for privacy and national security, based on international best practices. A manifestation of this alignment could include joint work on the classification of data types, rules regarding the sharing of data according to its classification, clear definitions of what constitutes critical infrastructure, limits on government extra-territoriality access to data, and the removal of blanket data localization requirements. A specific agreement to consider would be allowing Chinese Internet companies continued access to the U.S. market in return for removing JV / local ownership requirements on U.S. controlled cloud providers operating in China.

5. **Initiating Cooperation on Cyberspace Governance.** The challenges and threats in cyberspace are global in nature, and the growing number of cyber-attacks, cyber-crimes, viruses and vulnerabilities can be harmful to all countries, including China and the United States. Currently, different countries and regions are divided on the rules of cyberspace governance, showing a tendency of disintegration and fragmentation, which is not conducive to addressing this common challenge. Restrictions can be eased in areas that do not involve national security, such as safety standards, technical standards, and vulnerability sharing platforms; support representatives from industry and academia on both sides, in a non-discriminatory manner, to participate in

relevant standard organizations, such as the Forum of Incident Response and Security Teams (FIRST), in order to enhance communication and information sharing and thus build international standards together through consultation.

6. **Demarcating Trade & National Security Issues Related to Semiconductors.** Both governments should recognize the importance of the global semiconductor value chain, and except for narrow and legitimate national security reasons, refrain from broad semiconductor decoupling policies (which include both supply chain localization and restrictive trade measures). We can pursue new approaches in the semiconductor industry that strike a balance between restricting the export of a specific set of well-defined, sensitive dual-use technology for national security versus limiting all exports of broad categories of technology due to economic policy concerns. A manifestation of this new arrangement could be a recommendation that both governments maintain the stability of the semiconductor supply chain and facilitate trade development in related fields by considering a more narrow and flexible export control regime tied to legitimate and specific national security concerns (such as military or sensitive dual-use technologies and end users) that eases restrictions on the flow of commercial semiconductors exclusively for civilian end-use (such as mobile 5G chipsets) and where possible would make greater use of a robust, validated end-user process that includes real-time, on-site monitoring that ensures shipments are not diverted for inappropriate end uses as opposed to broad and static restrictions. Both governments should take steps to make transparent information regarding industrial subsidies and procurement support in compliance with WTO and GAMS (or other relevant) agreements. Furthermore, both governments should agree to avoid market-distorting industrial subsidies.
7. **Intellectual Property.** We can develop new and improved intellectual property protections, greater penalties for IPR violations, and accelerated mechanisms to resolve joint disputes quickly. A manifestation of this new arrangement could be a joint U.S.-China IPR Tribunal to which companies from either side could bring disputes.
8. **Rules as the Core of Mutual Engagement.** Across areas of alignment, we can begin to define the joint rules by which the two countries and their respective companies interact in the digital economy. We can help corporate leaders understand what business opportunities are available to them in each country. A specific manifestation of this arrangement could be mutual publication of the standards by which CFIUS (in the United States) and the relevant foreign investment regulators, such as SAMR (in China), approve or deny cross-border investments and mergers and acquisitions.

PART IV

How to Get Started / Roadmap: Building the Framework for Mutual, Positive Engagement

It is time to move forward in the relationship, rather than simply reiterate our differences. It is time to take these topics of high-level alignment and work through the difficult discussions to identify areas of mutual agreement and concrete agreement. Within a short period of time, we need to build trust as well as momentum to address and solve more challenging issues.

We therefore recommend that the two governments resume direct dialogue and consultation mechanisms ("Track I" Dialogues) with the following process:

1. "Short-term" negotiations to find one or two reciprocal agreements on aligned issues such as regulated data flows, scientific collaboration, investment approval rules, and modifying export control requirements to reduce restrictions on the sale of commercial semiconductors exclusively for civilian end-uses (coupled with corresponding on-site monitoring and enforcement) which would build momentum and trust for larger negotiations.
2. "Long-term" negotiations on an integrated, single, global, semiconductor industry, with export control sanctions only where necessary for national security (based on narrowly defined national security interests in the digital economy) and industrial subsidies transparent and consistent with relevant WTO requirements.
3. "Long-term" negotiations on clear definitions of standards for national security sanctions and restrictions, including improved dispute resolution mechanisms, enforcement, and mitigation measures.
4. "Long-term" dialogue on data security and cybersecurity, to reverse the trend of generalizing security issues and to work closely on the definition and development of relevant global standards.

These working groups should leverage technical experts and industry experts and utilize simulations to understand how any agreement can have an impact on technology and market development. Both sides should clarify how these working groups have delegated sufficient authority within each country's complex internal governance procedures.

The Track II Dialogue structure can remain a helpful source of advice, insight, and analysis for the government-to-government discussions. Track II Dialogues should operate in parallel to the Track I Dialogues.

Therefore, we recommend the formation of permanent Track II Digital Economy sub-working groups (as well as academia, policy, industry and technology platforms) in various areas, including the following:

- Data governance in both commercial and scientific fields.
- Global technology infrastructure and supply chain security.
- National security interests and their relation to the digital economy, including reasonable limits.
- Industrial policy to support the digital economy, including subsidies, procurement rules, and licensing agreements.
- Intellectual property evaluation, enforcement, and monitoring mechanisms.

Removing Roadblocks: Areas Where We Have Not Reached Alignment and Recognition of the Need for Enforcement

- **Recognition of Topics "To Be Discussed Later."** Both sides understand there are certain disputes which have no path to immediate resolution because they touch on core interests. These include unfettered and open access of major U.S. Internet platform companies to the Chinese Internet market; transfer of sensitive national security-controlled technology to military end-users; and the unfettered access of major Chinese telecom companies to U.S.-sourced technologies. We suggest we put such issues to the side and find areas of short-term alignment.
- **Enforcement.** We realize both governments have many levers to shape the digital economy. Even if both sides agree to rules designed to avoid digital economy disruption, governments can use other means to subvert the original intent of such rules. It is of real concern to both parties that even if we define and legally adhere to agreed rules, we may not achieve the results to which both parties agreed. Therefore, we recognize the need to design enforcement mechanisms to track compliance and drive penalties and dialogue in case of such subverting actions.

Conclusion

As the world's two largest economies, the United States and China have the most at stake, both risks and opportunities, in the development of the digital economy. They will also have a tremendous impact on other nations that use Chinese and American-generated digital economy solutions. It is incumbent upon them both to reach mutually agreeable ways of working both collaboratively and competitively that can build the digital economy for the benefit of all people.

AMERICAN PARTICIPANTS

Dennis Blair	Knott Distinguished Visiting Professor, Department of Peace, War and Defense, University of North Carolina at Chapel Hill
Maura Caliendo	Global Chief Privacy Officer, Chubb
Michael Chertoff	Co-founder and Executive Chairman, The Chertoff Group
Jimmy Goodrich	Vice President for Global Policy, Semiconductor Industry Association
Robb Gordon	Senior Policy Director and Managing Counsel, Intel Corporation
Melissa Hathaway	President, Hathaway Global Strategies
Stephen Orlins	President, National Committee on U.S.-China Relations
Pamela Passman	Senior Associate (Non-resident), Center for Strategic and International Studies
Matthew Spence	Advisor to the President and Professor of the Practice, Thunderbird School of Global Management, Arizona State University
Christopher Thomas	Chairman, Integrated Insights Limited & Visiting Professor, Tsinghua University
Paul Triolo	Practice Head, Geo-Technology, Eurasia Group
Graham Webster	Editor in Chief, DigiChina, Stanford Cyber Policy Center and New America; China Digital Economy Fellow, New America

CHINESE PARTICIPANTS

CHEN Xiaogong	Former Deputy Director, Central Foreign Affairs Office
YU Hongjun	Former Deputy Minister, China International Liaison Office
HAO Yeli	Vice President, China Institute for Innovation and Development Strategy, General (retired); Chair, Guanchao Cyber Forum
GAO Xinmin	Vice Chairman of the Internet Society of China
LV Benfu	Professor and Director of the Research Center for Network Economy and Knowledge Management, Chinese Academy of Sciences
FENG Wei	Vice Chairman, China Institute for Innovation and Development (CIIDS)
LEE Xiaodong	Founder and CEO, Fuxi Institution; Professor and Director, Center for Internet Governance, Tsinghua University
LIU Yadong	Former Chief Editor of Science and Technology Daily, Ministry of Science and Technology, Dean of School of Journalism and Communication, Nankai University
XU Zhiwei	Researcher, Institute of Computing Technology, Chinese Academy of Sciences
WANG Zhile	Founder, New Century Multinational Corporation Research Center; and former researcher, Ministry of Commerce

WANG Peng	Vice President, China Electronic Information Industry Development Research Institute
ZHI Zhenfeng	Researcher, Institute of Law, Chinese Academy of Social Sciences
WANG Bin	Vice President, Hikvision
QIAO Siyuan	Senior Strategy Researcher, Qi-An-Xin Group
WEN Zhumu	Ph.D., Network and Information Security; Executive Director, 801 Cybersecurity Initiative
XIE Yongjiang	Executive Director of the Beijing University of Posts and Telecommunications Internet Governance and Law Institute
WANG Shijiang	Director of the Integrated Circuit Industry Research Institute at the China Electronic Information Industry Development Institute; Deputy Secretary General of the China Semiconductor Industry Association