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

CONSENSUS AGREEMENT

March 10-12, 2019
Washington, D.C., United States

THE NATIONAL COMMITTEE ON U.S.-CHINA RELATIONS AND THE GUANCHAO CYBER FORUM convened their first Track II Dialogue on the Digital Economy on March 11 and 12, 2019 in Washington, D.C. The dialogue brought together U.S. and Chinese experts from academia, think tanks, and industry for off-the-record discussions on digital economy issues of concern to both countries. *(See attached name list.)*

The United States and China are the world's two largest national economies and the primary drivers and beneficiaries of the digital economy. Given the broader role of existing technology in society today, and the novel challenges and opportunities that new technologies may present, both countries have a responsibility to lead in setting the rules and norms governing the digital economy.

Members of the two delegations discussed a variety of issues, including those around data governance, supply chain risk management, and the Internet of Things (IoT). In these and other areas, the U.S. and Chinese participants identified many similar risks. These include risks to public safety or to national or global security, as well as the possibility that policies designed to address these challenges may unnecessarily limit the benefits of the digital economy.

While identifying similar risks, the two delegations recognized that U.S., Chinese, and other global approaches to these issues differ, sometimes in fundamental ways. Nonetheless, they believe there is potential for positive joint and coordinated action by U.S. and Chinese actors. This document represents a joint accounting of the themes of the discussion, as well as a set of recommendations for government and private sector actors in each country.

DATA GOVERNANCE

The flow of data across borders is one of the greatest enablers of the digital economy that in turn drives economic growth in all countries. Yet, every business that operates internationally needs to deal with the issues of how data (both its own and that of third parties) can, and must, be collected, managed, stored, and protected. Data governance is thus fundamental to the growth of the digital as well as the global economy.

One of the major concerns international companies face today is the diversity of data governance frameworks. Conflicting emerging legal and regulatory frameworks are taxing the digital economy. To operate in multiple markets, businesses must incur substantial operational and legal costs to comply with differing, and often ambiguous or even conflicting, national laws, regulations and practices pertaining to data governance. Data localization requirements also make it difficult and expensive to manage global operations, especially for small and medium-sized companies.

Addressing these concerns would be of great benefit to both countries and to the global economy, potentially resulting in a 10 percent increase in global GDP.

Specific suggestions by the participants for cooperation and coordination between the two countries include the following:

- A consistent, clear set of definitions is key to developing further policies and methods that can be well-implemented in both nations. Appropriate U.S. and Chinese agencies should consider developing a joint white paper establishing common definitions. For instance, participants noted the dangers to both economies of an increasingly broad definition of national security.
- In discussing existing regimes for data governance, the participants identified several problems with the European Union's General Data Protection Regulation (GDPR), including concerns about adaptability to emerging technologies, high penalties, the need to establish safe harbors, obstacles to innovation, and high business costs that are inconsistent with U.S. and Chinese priorities. Participants concurred that reciprocity helps interoperability. In general, participants felt that the Cross-Border Privacy Rules (CBPR), promulgated by the Asia-Pacific Economic Cooperation (APEC) presents a promising starting point for identifying common areas of agreement for China and the United States. An upgraded version of the CBPR could contain beneficial parts of the privacy protection framework spearheaded by the European Union and its GDPR. On top of that, it is vital to consider the cost of certification and implementation, the feasibility of enforcement, and the scope and feasibility of the compliance certification process.
- The aim for both sides should be to seek a path towards ensuring interoperability between the two systems, two sets of legal frameworks, and differing approaches to data privacy. Both countries are in the midst of formulating and updating new frameworks for data governance, offering an opportunity to find common ground, based on existing international best practices.
- The United States and China should focus first on particular segments of the economy, as that may make consensus easier to achieve. Areas of focus identified include the following: financial services, a sector that is already accustomed to substantial government regulation and oversight; food safety and airplane maintenance, two areas where China and the United States are in regular communication; and the medical/pharmaceutical industries, where both share a strong concern in data security and product integrity.
- Both governments should encourage innovation and the free flow of data, understanding that the two countries have different approaches to national security and other objectives that may justify some restrictions on data flow.
- Both countries should adopt a risk-based approach in determining the scope of necessary regulations.
- U.S. participants encouraged China to continue exploring proposals to establish open data zones, for example in Pudong, Shanghai, Hainan Province, or Qianhai in Shenzhen.
- Protection of intellectual property rights (IPR) is essential to the encouragement of innovation and the growth of the digital economy. To aid industry in both countries, the United States and China should consider implementing an international IPR adjudication system. Regarding the regulatory enforcement of cross-border data flows, it is proposed to establish a specialized agency (which can be a multi-stakeholder entity) initiated by China and the United States with the participation of third-party neutral countries to supervise the compliance and certification of cross-border data flows.
- Rules should foster collaboration between government and business and encourage businesses to come forward when there is a breach, loss of data, or impact on the integrity of data.

SUPPLY CHAIN RISK MANAGEMENT

Corporations today rely on extensive global supply chains to deliver their products and services, and supply chains for IT products and services central to the digital economy present special challenges of reliability, trust, and security. These challenges lead to the potential for balkanization through specific regulatory requirements and mandating the use of certain technology that would duplicate efforts, increase costs, and inhibit innovation. With increasing supply chain security measures, companies of all sizes are challenged to meet such requirements, but small- and medium-sized enterprises, which the digital economy relies heavily on, in general have fewer resources for cybersecurity and other risk management measures.

As the bulk of supply chain activity involves business-to-business processes, industry is best situated to develop norms, standards, and procedures to manage the security and integrity of supply chains. Such rules should rely on industry standards developed through the international technology community. They should be grounded in a risk-

based approach and should be technology-neutral, ensuring greater adaptability as technology changes. There is also a role for verification by third-party experts that can certify the integrity of particular products or technologies.

Participants expressed their concern about the position of the U.S. government to increasingly "politicize" the interdependence of the digital supply chain. The delegates of both countries hope that the definition of national security can be made clear and measurable. The security-related restrictions on the import and export of digital products and services should be controlled within a narrow and precise range, without arbitrary expansion for political purpose, which is breaking down the well-integrated supply chain for digital goods and services for the two countries. The risk to the digital supply chain can be classified according to the level of product, process, enterprise, and industry chain, and adopt corresponding identification and management.

Insurance can also assist in managing supply chain risks. Cybersecurity underwriters increasingly work with businesses on preventative work and training before cybersecurity incidents, as well as with legal compliance, response, and recovery after such incidents. While threats are increasing, we should move toward a risk-based approach that does not stifle innovation.

INTERNET OF THINGS

The rapid adoption of smart, adaptive, and connected devices—the "Internet of Things" (IoT)—is occurring across virtually all critical infrastructure sectors. The IoT will bring significant societal benefits, many of which are already being realized through increased efficiencies, early detection of faults, improved reliability and resilience, and more. But the rapid and massive connection of these devices also brings with it risks, including new attack vectors, new vulnerabilities, and perhaps most concerning of all, a vastly increased ability to use remote access to cause physical destruction.

To deal with this complex interplay of networks and devices, governments and industries should set rules to govern the IoT, including standards of security, compatibility, and interconnectivity of devices sold in the global market. IoT products should be regulated and certified (in some cases, on an ongoing basis), similar to current practices such as the periodic inspection of elevators and the certification of electronic devices by UL. Different IoT systems (e.g., kitchen appliances vs. self-driving cars) will present varying levels and types of risk which will need to be addressed accordingly.

In the field of IoT, China and the United States should establish cooperation with the relevant international standards development organizations (ISO/IEC JCT 41) to formulate security compliance standards, test certification processes, improve the role of security governance at all levels, and enhance the social awareness of IoT security.

CONCLUSION

Today, the United States and China are the world's two largest economies and each other's largest trading partner. They are both well-positioned to reap the benefits of the digital age. At the same time, they both face similar threats and challenges. There is some urgency in the opportunity, driven not by any geopolitical or business agenda, but rather by the relentless march forward in technology development. Moore's Law today is enabling a new revolution in innovation born of the convergence in artificial intelligence, 5G, and our connected global digital infrastructure. Both countries stand to enjoy significant gains by laying new groundwork for collaboration, data sharing, threat and risk sharing, and continued security research. Whether it be combating cybercrime, protecting IoT systems, or providing consistent rules to allow their companies to operate globally, China and the United States will be much better off if they collaborate in dealing with these problems and provide a framework within which all businesses and individuals can unlock new opportunities to grow.

Despite the lack of strategic mutual trust given today's circumstances, the United States and China, as two major digital economies, can and will respect each other, find common interests and concerns, and conduct possible cooperation agreement on the basis of transparency and the rule of law.

CHINESE PARTICIPANTS

HAO Yeli	Vice President, China Institute for Innovation and Development Strategy
GUO Quanqi	President, CECC Holdings Corp. Ltd
LI Bo	Executive Director, Chunqiu Institute for Development Strategy
LV Benfu	Vice President, Guanchao Cyber Forum
LYU Jinghua	Visiting Scholar, Carnegie Endowment for International Peace
PENG Lihui	Secretary General, China Electronics Chamber of Commerce
Edward Tsai	Director of Investment, 360 Enterprise Security
WANG Bin	Vice President, Hikvision
WU Shenkuo	Professor of Law, Beijing Normal University
ZHANG Xundi	Senior Security Operations Specialist, Alibaba Group

AMERICAN PARTICIPANTS

Dennis Blair	Chairman and Distinguished Senior Fellow, Sasakawa Peace Foundation
Melissa Hathaway	President, Hathaway Global Strategies
Yancy Molnar	Senior Vice President, International Government Affairs & Public Policy, Chubb Group
Stephen Orlins	President, National Committee on U.S.-China Relations
Pamela Passman	President and CEO, CREATe.org
Thomas Quillin	Director, Cyber Security, Intel Corporation
Nigel Thompson	Vice President, Product Marketing, Blackberry
Paul Triolo	Practice Head, Geo-Technology, Eurasia Group
Graham Webster	China Digital Economy Fellow and Coordinating Editor, DigiChina, New America