THE NATIONAL BUREAU *of* ASIAN RESEARCH

COMMENTARY

China's Evolving Cybersecurity and Cyber Development Strategy

BY JING DE JONG-CHEN

Published: March 29, 2017

In the often fractious U.S.-China relationship, cybersecurity has emerged—in some unusual ways—as one of the few areas of successful bilateral cooperation. In 2016, both countries made progress in narrowing the gap on core issues, including cybercrime, theft of intellectual property (IP), and cyber norms. Yet admittedly, both countries still have a long way to go. China's Cybersecurity Law, which becomes effective in June 2017, raises significant concerns among U.S. government officials and business leaders, who worry that China's policies will restrict market access for foreign companies. A guiding concept of the new law is Internet sovereignty, which is defined as "China's right to police the Internet within its borders and to participate in managing international cyberspace." Under the new law, equipment suppliers from a range of industries will be required to undergo security reviews to ensure adequate protection from hackers. The United States and many other Western governments have expressed concerns that this policy will discriminate against foreign competitors or lead to requirements for transfers of proprietary technologies. With these developments in mind, this commentary seeks to provide context for the progress that the United States and China have made on cybersecurity issues to date and to highlight the serious challenges that lie ahead.

China's Cybersecurity Strategy

China's Cybersecurity Strategy, released in December 2016 by the Cyberspace Administration of China, provides a good framework for understanding advances in the country's position on global collaboration. The Cybersecurity Strategy prioritizes the Internet as an economic engine, calls for a new people-centered approach to Internet development, and indicates the government's willingness to allow foreign technology companies to participate in developing national security standards.

Most importantly, the strategy acknowledges the roles of government, industry, social organizations, and the public in maintaining effective cybersecurity. At the same time, however, China's cybersecurity policies continue to reaffirm its cyber sovereignty, promoting the right of individual nations to control Internet use within their borders and to set their own rules

---

JING DE JONG-CHEN *is a Partner and General Manager, Global Security Strategy and Diplomacy, at Microsoft Corporation. She has 20 years of industry experience and domain expertise in cybersecurity policy, technology, and strategic partnership development. The views expressed in this essay are the author's own.*

and priorities for Internet development. In short, if China's approach to cyber issues remains complex, it is also clearly evolving, becoming more nuanced and rule-driven.

Making Progress on Cybersecurity and Cyber Norms

Cybersecurity and cyber norms are sensitive and important issues for China. As members of the UN Group of Governmental Experts (GGE), China and the United States worked with many countries, including Russia, to reach consensus on key issues.[1] Although there is still no commonly adopted legal framework of international norms, laws, and arms control treaties in cyberspace, the UN GGE reports represent a significant step forward in promoting global collaboration and building consensus for efforts to prevent and minimize cyberwarfare damages, while simultaneously allowing participants to defend their national networks and other cyber assets.

Another important milestone is the Third Joint Dialogue on Cybercrime and Related Issues. Then U.S. attorney general Loretta Lynch and secretary of homeland security Jeh Johnson, together with Chinese state councilor and minister of public security Guo Shengkun, recommitted their respective nations to cooperating on investigating cybercrimes emanating from either country and to refraining from cyber-enabled IP theft with the intent of providing competitive advantages to companies or commercial sectors. Both sides agreed to collaborate on network protections by enhancing network hygiene and promoting best practices. Further, the United States and China agreed to engage in regular reciprocal sharing of malicious IP addresses, malware samples, analytic products, and relevant network protection information. The two countries acknowledged the misuse of technology and communications for facilitating violent terrorist activities and opted to continue sharing information to tackle this issue. They also acknowledged the value of the U.S.-China cybercrime hotline and agreed to continue to use this mechanism.

Balancing Cybersecurity and Internet Development: A Programmatic Approach

In March 2016, China unveiled the national innovation portion of its 13th Five-Year Plan, including its commitment to "Internet plus." This initiative is designed to drive economic growth and foster new industries by integrating mobile technology, cloud computing, big data, and the "Internet of things" with Chinese business and manufacturing. One month later, President Xi Jinping chaired a cybersecurity and information forum and clearly set out China's changing view of key cyber issues. In a speech to domestic stakeholders, Xi described cyber strategy as a central part of his diplomatic vision of "a community of common destiny." He said that Internet development should be based on a "people-centric approach," which includes providing 700 million people with accessible, affordable, and easy-to-use Internet services. He also emphasized the value of the Internet as a tool to improve the flow of information, technology, capital, and talent, as well as goods and services, and to improve productivity within a flexible economic model.

According to Xi, the government should encourage Chinese enterprises to compete globally, expand international markets, and develop defensive and offensive cyber capabilities. In addition, Xi called on the government to support domestic research into core technologies, which he described as the "key to China's Internet development." Xi also commented on the importance of industry collaboration. He noted that unlike Microsoft, Intel, Google, and Apple, Chinese Internet enterprises are not experienced in collaborating with each other. This has created a technology innovation gap between China and other countries.

During his speech, Xi explained that cybersecurity requires collaboration among government, industry, and social organizations; noted that public involvement is an important part of cybersecurity; and explained the need to balance national security and Internet

1 UN Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security," https://www.un.org/disarmament/topics/informationsecurity.

development. He also called for enhanced Internet defense capabilities and a system to protect information infrastructure in critical industries, including finance, energy, telecommunications, and transportation. Finally, he urged government authorities to establish mechanisms to report risks and share information.

This pragmatic view could lead to opportunities for Chinese industry to play a larger role in cyber policy issues. In addition, it may signal new opportunities for China, other governments, and the global information and communications technology (ICT) industry to work toward mutually beneficial international policies on core issues of common concern, such as supply-chain trust.

Linking National Economic Strategy with Cyber Development

Making cybersecurity a top policy priority for presidential meetings led to an important bilateral agreement at the U.S.-China Strategic and Economic Dialogue in Beijing in June 2016. Both governments agreed on the need for cybersecurity in commercial sectors and agreed to adhere to the following principles: ensure consistency with World Trade Organization agreements, be narrowly tailored, take into account international norms, and do not discriminate based on a supplier's country of origin. Most importantly, the agreement stated that the countries should not unnecessarily impose nationality-based conditions or restrictions on the purchase, sale, or use of ICT products by commercial enterprises.

The two governments also affirmed the principle that access to a full range of global technology solutions strengthens the cybersecurity of commercial enterprises. This is a significant development for the ICT industry because both Chinese and global companies have struggled for years to gain proper acceptance and to overcome market-access barriers.

President Xi's remarks for domestic audiences about China's active participation in select bilateral agreements suggest an evolution toward a more comprehensive approach to Internet usage by aligning national economic strategy with Internet development and cybersecurity. After Xi established this new direction, China's Ministry of Industry and Information Technology announced that it will adopt three initiatives to advance China's strategy to become a global cyber power:[2]

- implement a "broadband China" investment project
- increase network speed and reduce access costs to encourage startups and innovation
- carry out the Internet Plus initiative

These initiatives demonstrate a long-term national cyber infrastructure development strategy for building a vibrant cyber-based economy within the next decade.

Creating a Legal Framework and Enforcing Cyber Policies

Like most nations, China believes that defending against cyberattacks on citizens, critical infrastructure, and the economy is a matter of national security. As a result, the government is working to develop new laws and policies that attempt to balance issues of national sovereignty with economic growth in the cyber domain.

One example of the new approach is the China Counter-Terrorism Law approved by the National People's Congress in December 2015 and implemented in 2016. It provides a comprehensive framework—legal, administrative, and technical—to address both domestic and international terrorism.[3] As China develops policies and regulations to support the law, it will also establish a new government authority to manage compliance. A counterterrorism group and national intelligence center will use the framework the law provides to streamline antiterrorism work across government agencies and departments. In addition to coordinating the activities of government entities in China, it will coordinate "trans-regional

---

2 Zhang Feng, "MIIT Takes Three Measures to Boost Cyber Power National Strategy and 'Internet Plus' Initiative," Cctime.com, May 15, 2016.

3 Eric Carlson, Ashwin Kaja, and Yan Luo, "China Enacts New Counter-Terrorism Law," *National Law Review*, January 5, 2016. The new law also provides, for the first time, a legal definition of terrorism and outlines how the government will approach this challenge. China now defines terrorism as "any proposition or activity that, by means of violence, sabotage or threat, generates social panic, undermines public security, infringes on personal and property rights, and menaces government organs and international organizations—with the aim to realize certain political and ideological purposes."

efforts on counter-terrorism intelligence and information gathering." This includes working with law enforcement in the host country to conduct cross-border data searches instead of imposing data residency requirements and restricting cross-border transactions. These policies help advance global trade while at the same time respecting national sovereignty.

The implementation of China's Cybersecurity Law, effective June 2017, will have a significant impact on both Chinese and international businesses and may impose further restrictions on Chinese citizens. While some details are yet to be determined, the law outlines responsibilities for Internet technology and service providers to address content censorship, enforce real-name registration for Internet services, give mandatory assistance to law enforcement, and require data residence of personal and important data associated with critical infrastructure, including in the banking and transportation sectors. China also added language that corresponds to the U.S. position on sanctions against foreign hackers, such as freezing assets. Technology providers will be required to comply with national standards and will be subject to government-run cybersecurity reviews before receiving procurement approvals by the public sector and state-owned enterprises.

China has long maintained the position that a nation should have the right to control how the Internet is governed inside its borders. As the country with the world's largest population of Internet users, China believes this issue is nonnegotiable. For U.S. companies doing business in China, however, the use of cybersecurity threats can appear as a pretext for establishing trade barriers. This policy is especially problematic in view of growing popular support for retaliatory protectionist policies in the United States and Europe.

Moving forward, Internet governance will continue to be a contentious issue between China, aligned with Russia, and the United States, in agreement with Europe. The Sino-Russian position maintains that governments must take the lead in managing domestic and international use of the Internet to avoid political and social disruption as well as other types of misuse, from cybercrime and terrorist activities to intelligence gathering and the spread of antigovernment sentiment. For example, China's Cybersecurity Law includes a provision that requires "any person and organization using networks [to] abide by the Constitution and laws, observe public order and respect social morality," and forbids a long list of activities that may be "endangering national security and stability." In contrast, U.S. and European governments advocate for a multi-stakeholder model where the government, private sector, and civil society have equal obligations in governing the Internet.

An ICT Industry Perspective

As societies worldwide continue their increasing dependence on ICT resources—and as citizens, organizations, and governments rely more heavily on secure data and devices to conduct their business and pursue their goals—the importance of cybersecurity will continue to grow. China has accelerated the growth of its Internet-based economy with the support of Chinese global Internet service providers such as Baidu, Alibaba, and Tencent. The government is forging new opportunities for commerce by cooperating with other non-U.S. economies through investments such as the creation of the Asian Infrastructure Investment Bank and the One Belt, One Road initiative, linking Asia with Europe directly over land and sea. Chinese state-owned enterprises are also increasing their acquisitions of foreign high-tech companies, a trend that raises concerns for the governments where these companies are located.

State-sponsored investment and policies that leverage access to foreign markets will enable Chinese industries to acquire core technologies and thrive in domestic and international markets. This strategy also increases Chinese competitiveness in countries like the United States where trade rules have been more liberal. As two of the world's most influential nations, China and the United States share responsibility for leading international efforts to establish cybersecurity policies and promote consensus around Internet governance.

Despite improved cooperation and greater collaboration on addressing cybercrime and cybersecurity, the two governments continue to hold very different positions on other cyber governance issues.

From a U.S. industry perspective, businesses will need to invest in the legal compliance required by China's new Cybersecurity Law and associated regulations, as mandatory national security standards. Companies and their customers will also face risks for any noncompliance due to technical difficulties. If penalized by the Chinese government, U.S. companies may face the dilemma of having to remove products and services from the marketplace. At the same time, information technology users in China may be forced to adopt less secure solutions due to lack of competition.

It remains to be seen how and if the administrations of Presidents Trump and Xi commit to building joint partnerships to promote cybersecurity, cyber norms, and security innovation. If they do, the ICT sector can provide both governments with the tools to address cyber threats as new forms of computing continue their rapid evolution and adoption. China's recognition of the value of Internet-based economies provides an opportunity for the ICT industries in China, Europe, Asia, and the United States to work collectively to address their common interests, including issues such as supply-chain trust. And ultimately, the best approach to protecting the Internet worldwide is to allow the ICT industry to drive innovation and to permit users to adopt the most advanced and reliable solutions without discriminating based on the national source of a product.

NBR

THE NATIONAL BUREAU *of* ASIAN RESEARCH

1414 NE 42ND STREET, SUITE 300
SEATTLE, WA 98105 • 206-632-7370

1819 L STREET NW, NINTH FLOOR
WASHINGTON, D.C. 20036 • 202-347-9767

WWW.NBR.ORG @NBRNEWS