NBR

POLITICAL AND SECURITY AFFAIRS

STABILIZING CYBERSECURITY IN THE U.S.-CHINA RELATIONSHIP

A brief for the U.S.-China Relations in Strategic Domains Project
by Adam Segal

As the 2011 International Strategy for Cyberspace declares, the United States has a national interest in an "open, interoperable, secure, and reliable" Internet that fosters international trade, economic development, and innovation; strengthens international security; and promotes free expression. China, however, has a contrasting vision, and cyberattacks and the rules of cyberspace are likely to be a high priority issue during the September 2015 summit between Presidents Barack Obama and Xi Jinping.

U.S.-CHINA RELATIONS IN THE CYBER DOMAIN

Cyberspace is an especially contentious issue in the Sino-U.S. relationship. According to Assistant Secretary of State for East Asian and Pacific Affairs Daniel Russel, cyberspace has the "potential to drive strategic mistrust in the relationship" between the two nations.[1] Beijing and Washington have been unable to find common ground on cyberattacks, the security of information and communications infrastructure, and Internet governance. Cyberattacks constitute a threat to the national security, foreign policy, and economy of the United States, and many of these attacks emanate from China. Some of these attacks are conducted by state actors or by hacker groups sponsored by Chinese government actors. Other attacks are conducted by criminals working on their own.

These attacks fall into three categories. The majority are the cyber-enabled theft of intellectual property,

[1] Daniel Russel, "Preview of the Seventh U.S.-China Strategic and Economic Dialogue," U.S. Department of State, June 18, 2015, http://fpc.state.gov/243965.htm.

business strategies, and trade secrets. There is also a widespread campaign of political and military espionage such as the hack of the U.S. Office of Personnel Management, which may have exposed the records of over twenty million current and former federal employees. In addition, the members of the People's Liberation Army Unit 61398 have reportedly penetrated the networks of natural gas pipelines and electric utilities, possibly to map the potential future battlefield or prepare for a destructive attack.

The cybersecurity issue has also spilled over into trade relations. In part motivated by disclosures of U.S. cyberespionage against Chinese targets made by the former National Security Agency contractor Edward Snowden and in part a reflection of a long-held techno-nationalism, Chinese policymakers have introduced a number of regulations designed to reduce dependence on foreign suppliers for critical technologies. New banking regulations, for example, and the draft antiterrorism and national security regulations in China require companies to share source code and build backdoors into encrypted products in an effort to make technology "secure and controllable." Although the bank regulations were suspended in April, protectionism remains tightly linked to cybersecurity concerns.

Beijing has also stepped up efforts to shape the governance of cyberspace. In November 2014, China hosted the World Internet Conference in Wuzhen, a clear signal that it intends to take a more active role in defining the international agenda. In particular, Beijing has stressed the norm of Internet sovereignty—the idea that every state has the right to make rules and regulations covering cyberspace—and has argued that this right should be recognized internationally. In other words, the global Internet should be subject to local controls.

Beijing recently extended its vision of the Chinese Internet to the United States. In April 2015, researchers at the Citizen Lab at the University of Toronto and the International Computer Science Institute at the University of California, Berkeley, discovered what they called the "great cannon," a program that hijacked traffic and directed it at GreatFire.org, a site that runs mirrors of other sites blocked in China, and GitHub, a software coding site that was also hosting content Beijing found objectionable, in order to overload and crash both sites' servers. The Great Cannon attack knocked GitHub offline for five days and was an unacceptable interference to Internet access and free speech within the United States.

During the June 2015 Strategic and Economic Dialogue (S&ED), senior U.S. officials warned their Chinese counterparts that the theft of intellectual property undermines trust and threatens the economic foundations of the bilateral relationship. Recent press reports suggest that Washington is considering sanctioning individuals or entities that benefit from cybertheft.[2] If such a move comes after the conclusion of the summit, President Obama should clearly explain to President Xi when the two meet how the sanctions will be implemented and what evidence the United States has of the hacking. President Obama will want to stress that the United States is getting better at attribution and that it is willing to make some types of evidence public to support its claims.

[2] Ellen Nakashima, "U.S. Developing Sanctions against China over Cyberthefts," *Washington Post*, August 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

RECCOMENDATIONS

While the two sides are unlikely to close the gap on cyberespionage, they should broaden and deepen the discussions on cybersecurity and cyberconflict. Beijing suspended the U.S.-China cyber working group after the indictment of five alleged PLA hackers in May 2014, but the discussions to manage disagreements do not have to be housed within one formal structure and should continue in the S&ED and military-to-military contacts. The announcement of a new dialogue between the U.S. Department of Homeland Security and Chinese Ministry of Public Security is a useful step, though it will focus on cybercrime.

Attribution remains a point of contention, with Beijing calling the United States' claim that China was behind the attacks on the U.S. Office of Personal Management "irresponsible and unscientific." Yet a shared understanding of what types of evidence can be used to attribute an attack and how that information is presented would be an important first step to defining norms of behavior. At the June 2015 S&ED, State Councilor Yang Jiechi called for China to work with the United States to develop an "international code of conduct for cyber information sharing." While the Chinese side has not offered any specifics, Washington and Beijing could establish a joint forensics team, made up of experts from the government, private sector, and academia, to investigate an attack on a third party and identify types of information to be shared.

Beijing and Washington have a common interest in preventing escalatory cyberoperations—attacks that one side sees as legitimate surveillance but the other views as prepping the battlefield. The two sides could consider conducting formal discussions on acceptable norms of behavior and possible thresholds for use of force as well as greater transparency on doctrine. These cooperative measures can reduce the chance of misperception and miscalculation and thus diminish the likelihood that a conflict in cyberspace will become kinetic.

Additionally, Beijing and Washington have a common interest in preventing extremists and other third parties from attacking critical infrastructure. Terrorist groups have so far shown greater dexterity in the use of the web for recruitment, fundraising, and propaganda than in launching destructive attacks, but that will change over time. The Islamic State of Iraq and Syria (ISIS), for example, has a stated desire to develop cyberweapons and has reportedly recruited hackers from Western Europe. To respond to emerging challenges, the United States and China should discuss joint measures to prevent the proliferation of capabilities.

It is unlikely that the summit will produce new cooperative measures on cybersecurity, given the high degree of mistrust between the two sides and the growing political pressure in the United States to sanction China for the recent hacks. Perhaps the most that can be expected is that Washington and Beijing will signal a willingness to continue substantive discussions to manage disagreements and prevent escalation of events in the cyber domain to actual conflict. ~

Adam Segal is the Maurice R. Greenberg Senior Fellow for China Studies and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations.

U.S.-China Relations in Strategic Domains

U.S.-China Relations in Strategic Domains is a 24-month joint project between NBR, the Institute for China-US People-to-People Exchange, and the Institute of International and Strategic Studies, both at Peking University. This project is made possible by the generous support of the Carnegie Corporation of New York, and seeks to produce a forthright examination of the challenges in establishing greater trust and cooperation in U.S.-China relations in strategic domains and bilateral exchanges. The goal of the research and discussions is to produce pragmatic recommendations for U.S. and Chinese policymakers in order to strengthen the most important bilateral relationship in the Asia-Pacific. In 2016, the project will culminate in a series of analysis papers co-authored by American and Chinese experts, under the guidance of eminent scholars from both the United States and China.

For more information, please visit the NBR website.

NBR

THE NATIONAL BUREAU *of* ASIAN RESEARCH

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

1301 PENNSYLVANIA AVENUE NW, SUITE 305
WASHINGTON, D.C. 20004 • 202-347-9767

WWW.NBR.ORG @NBRNEWS