Confidence Building for Cybersecurity

between China and the United States

Dong Qingling

In recent years, cybersecurity has become a contentious issue in the Sino-American relationship. Edward Snowden’s revelations in 2013 of the United States government’s surveillance around the world gave China an argument to counter American complaints that China was stealing intellectual property (IP) from American companies and research institutes. The United States government has repeatedly accused Chinese hackers of invading American corporate, proprietary economic data and stealing sensitive national security information. Meanwhile, the Chinese government is dissatisfied with the way that United States leaders and politicians instigate protests and social upheaval using the Internet.

In addition, the Chinese government notes that a large number of malicious global cyber attacks actually originate from computers hosted in the United States.\(^1\) Both the United States Department of Defense and the

\(^1\)Dong Qingling is Associate Professor, School of International Relations, University of International Business and Economics(SIR-UIBE); Post-doctoral Researcher, Cyber Security Program, China’s State Information Center(SIC).

The China Daily reported that in the first five months of 2013 about one-third of hacking attacks on Chinese computers appeared to originate from the United States. In addition, a total of 249 Chinese government and academic websites were hacked from January to May 2013, 54 of which were apparently targeted by U.S.-based
Chinese People’s Liberation Army view cyberspace as a new conflict domain, and they are watching each other warily. Nationalist “hacktivism,” in the form of website defacement, service denials and network exploitation, is flowing both ways across the Pacific.²

Some strategist and information technology observers believe that the unfortunate feeling of Sino-American distrust in the cyberspace realm is dangerous, as it can exacerbate broader strategic distrust and contribute to hostility, which threatens the health of the most important bilateral relationship in the world.³ Even more, the potentially poisoning effect of cyber distrust is taking place at a time when there is genuine uncertainty about the degree, nature and speed of changes in the global balance of power.⁴ As such, it is becoming increasingly urgent for China and the United States to regulate conflicts and build confidence in cyberspace. The following measures are worth consideration.

Dialogue and Key Terminology

Internet Protocol (IP) addresses, see Xinhua, China, U.S. Talks on Cyber Security Go Well, July 10, 2013.
² IGCC, China and Cybersecurity: Political, Economic, and Strategic Dimensions, Report from Workshops held at the University of California, San Diego April 2012.
⁴ Kenneth Lieberthal and Peter W. Singer, Cybersecurity and U.S.-China Relations, February 2012.
As many analysts have noted, distrust is growing between the United States and China in cyberspace. The reasons may be plentiful, but one of the most important factors is that cybersecurity lacks a common, shared vocabulary. Even such terms as “information” and “cyber attack” are used differently by the American and Chinese governments. In addition, there are many different types of “attacks,” but there is little agreement on how to characterize and categorize these differences.\(^5\)

For instance, even on the question of how to define cybersecurity. For the Chinese authorities and media, cybersecurity means technological safety and political stability. In other words, the Chinese side emphasizes information content and safety, and they state that cyberspace should not develop into a realm for political struggle. For the United States, however, cybersecurity refers to technological resilience, intellectual property protection and privacy. In short, the United States side stresses the freedom of cyberspace and data protection.

Over the past two years, officials from Washington and Beijing have accused each other of supporting hacking activities, and the issue of cybersecurity is spilling into other areas of bilateral relations. This suggests that China and the United States need to hold some form of dialogue on cybersecurity at various levels of government. Focused on the economic implications of cyber espionage, initial Sino-American dialogue could begin

by defining the terms of the global debate on cyber norms.⁶

Until now, the global debate on cybersecurity has been centered around controlling Internet crime, coping with hostile attacks on critical infrastructure and developing legal norms to limit cyber conflicts between countries.⁷ In the next step, China and the United States must pay greater attention to the economic implications of cyber warfare on the global economy and the future of Sino-American commercial ties. Both sides should recognize how cyber conflict threatens to disturb the stability of the global economy and international relations. The two countries must start serious negotiations at different levels to draft a code of conduct for cyberspace.

In 2011, United States President Barack Obama and Chinese President Hu Jintao made commitments to improve the Sino-American bilateral relationship. In a joint statement, the two leaders specifically agreed to “advance cooperation to […] address cybersecurity.”⁸ In anticipation of this commitment, in May 2011 the EastWest Institute (EWI) and the Internet Society of China (ISC) convened a team of Chinese and American experts for a bilateral dialogue on cybersecurity. “China-US Bilateral on Cybersecurity: Fighting Spam to Build Trust,” the team’s first report, represents initial

---


⁷ Ibid.

efforts by Chinese and American experts to work together on cyberspace challenges.\(^9\)

In June 2013, Xi Jinping and his counterpart Barack Obama held an informal summit during which the two leaders discussed cyber issues for the first time, emphasizing the urgency of enhancing dialogue and cooperation in cyberspace and pledging to promote the establishment of a fair, democratic and transparent global internet management mechanism. Such a mechanism will be managed by the United Nations and will seek to build a peaceful, secure, open and cooperative cyberspace. In spite of the above consensus, however, China and the United States have different stances on how to protect their infrastructure and cyber information. The policy differences on both sides remain significant.

President Obama, for example, tried to draw a line between government-to-government hacking (spying) and government-to-corporate sector hacking. Perhaps in the United States, military spying is considered part of national interest and corporate spying is considered a crime. In China, however, a country with a very powerful state-owned enterprise (SOE) sector, this difference is not as clear.\(^{10}\) It is thus necessary for both sides to reach a consensus on key terminology, such as information infrastructure,

---


\(^{10}\) Alistair D. B. Cook, *The Cybersecurity Challenge and China and USA Relations*, EAI Background Brief No. 828, June 20, 2013.
cybersecurity, cyber espionage, cyber attack and cyber war. It is worth noting that similar dialogue has already been initiated between the United States and Russia, but it is not on the agenda for Sino-American relations.

Reducing Misperceptions and Increasing Transparency

Up until now, most government cybersecurity efforts have been shrouded in secrecy. Fair information practices, due process principles and the need to foster government-to-government or government-to-private cooperation all require transparency. Every country needs to elucidate a policy and strategy in order to limit misperceptions by other countries. On December 22, 2011, James Lewis from the Center for Strategic and International Studies wrote, “This year’s theme was “Norms”; next year’s theme will be “Confidence Building Measures.””  

In 2009, the China Institutes of Contemporary International Relations (CICIR) and Washington-based Center for Strategic and International Studies (CSIS) started a “Track 2 Sino-U.S. Cybersecurity Dialogue.” Thus far, they have held eight formal meetings on cybersecurity, accompanied by several informal discussions. A broad range of American and Chinese

---


12 China Institutes of Contemporary International Relations (CICIR) & Center for Strategic and International Studies (CSIS) Joint Statement, Bilateral Discussions on Cooperation in Cybersecurity, June 2012.
officials and scholars responsible for cybersecurity issues have participated in these meetings. The goals of the discussions have been to reduce misperceptions, increase transparency and identify areas of potential cooperation, including confidence building measures (CBMs) and agreements on norms and rules for cybersecurity. CSIS and CICIR have already put a number of ideas for cybersecurity cooperation on the table.

The “Track 2 Sino-U.S. Cybersecurity Dialogue” emphasizes a shared interest in avoiding misperceptions and miscalculations that could lead to conflict, while also focusing on proposals that could help reduce tensions in the cyber arena. Both CICIR and CSIS believe that confidence building measures (CBMs) – including increased transparency on cyber doctrine, reciprocal visits among civilian and military officials, formal exchanges of information on threats, descriptions of decision-making processes and joint exercises – are the antidote to strategic distrust.

In recent meetings, government representatives participated in three simulations in which each side described how it would react to a cyber crisis. This exercise showed that both countries have formal processes for dealing with cyber crises, but it also revealed that there is currently no identified channel of communication. Both sides agree that a formal rather than ad hoc approach to communicating during a crisis would be ideal – even if this simply means knowing exactly who to reach out to.\textsuperscript{13} China, Japan and the Republic of Korea already have a formal coordination process that allows their three national CERTS to exchange technical information. A similar formal process between the United States and China CERT is necessary.

**Regulating “Non-state Actors” Based on Law and Norms**

In contrast to the traditional security realm, the lines between state and non-state actions in cyberspace are often shifting and blurred. In cyber attacks or cyber espionage, the existing technological measures usually are unable to distinguish who is the real attacker and who should be held responsible for losses and damage.

In this context of non-discrimination, the so-called “patriotic hacker” communities and other non-state groups, including student and even cyber criminal groups, are often mobilized by their respective governments for

\textsuperscript{13} Ibid.
cyber operations. This aggravates problems of attribution and provides states with plausible deniability when they are accused of malicious activities in cyberspace.\textsuperscript{14}

In past engagements and communications, China and the United States shared views on the risks posed by “third party” actors, especially non-state actors such as terrorist groups, as well as the need to limit their development of cyber capabilities. On a similar note, both sides share the opinion that increased cooperation on cybercrime (including financial crime, fraud and child pornography) help produce useful exchanges between law enforcement officials in both countries.\textsuperscript{15} Though there is agreement on the benefits of cyber cooperation, implementation has proven difficult. Existing law enforcement cooperation mechanisms only meet infrequently and requests for investigative support are not always fruitful,\textsuperscript{16} mostly because there are still a lot of procedural difficulties and political obstacles.

The expert workshop between CICIR and CSIS has explored ideas for cybersecurity that are based on both international law and the creation of norms for responsible behavior in cyberspace. A number of specific measures for responsible international conduct have already been proposed, but they

\textsuperscript{14} Kenneth Lieberthal and Peter W. Singer, Cybersecurity and U.S.-China Relations, February 2012.

\textsuperscript{15} China Institutes of Contemporary International Relations (CICIR) & Center for Strategic and International Studies(CSIS) Joint Statement, Bilateral Discussions on Cooperation in Cybersecurity, June 2012.

\textsuperscript{16} Similar ideas can see Kimberly Hsu, China and International Law in Cyberspace, May 6, 2014.
will require further discussion and refinement.

Fortunately, both sides recognize that the existing laws of armed conflict, as well as the rules of proportionality, discrimination and the distinction of legitimate military targets, already provide a framework for protecting civilian targets. All nations should observe these regulations and norms in cyberspace.

**Focus of Future Dialogue**

In July 2013, United States Secretary of State John Kerry established a cybersecurity working group during a visit to Beijing, and the two sides worked to patch up ties that have been poisoned by the information revealed by National Security Agency whistleblower Edward Snowden regarding United States hacking into Chinese computers. The two sides held candid and in-depth discussions on the bilateral cyber working group, international cyberspace rules and measures to boost dialogue and cooperation on cybersecurity. Both sides agreed to hold an informal meeting at an appropriate time before the following strategic security dialogue.

However, in May 2014, the Chinese government decided to suspend its involvement in the cybersecurity working group after the United States indicted five Chinese military officials for allegedly stealing trade secrets. China’s Foreign Ministry called the United States’ move a “serious violation
of the basic norms of international relations.”¹⁷

What are the key roadblocks to developing effective cyber cooperation between China and the United States and how can they be overcome? What should be on the agenda for future Sino-American cyber talks? Perhaps there is a surplus of issues and problems to address, but one thing is clear: most analysts assume that the continuing discussion on bilateral cybersecurity should work to develop norms and build confidence in order to increase stability. The focus of dialogue at the next stage should emphasize the following questions and factors.

**How to increase the transparency of cyber measures?**

China and the United States often blame each other for a lack of transparency in computer network operations. Rather than being well coordinated, each nation’s cybersecurity efforts could be better described as nascent and ad hoc. This is not a recipe for easy cooperation.¹⁸ Some measures can be taken, such as establishing direct dialogue between the two governments, stability and risk reduction measures, accepting the applicability of existing laws of armed conflict, observing existing commitments on the protection of intellectual property, adherence to the

---


Budapest Convention on cybercrime and states taking responsibility for actions in cyberspace by individuals within their territory.

**How to restrict the weaponization of cyberspace?**

In senior policy circles, malware has been described as “a weapon of mass destruction” able to “destroy society” – a modern version of the so-called “existential threat.” Following the cyber attacks in Estonia and Georgia in 2007 and 2008 respectively, as well as the attack on Iran’s nuclear facilities in 2010, it is becoming increasingly clear that cyber warfare has become an “unavoidable element in any discussion of international security.” To date, cyber warfare has already become an integral part of military planning and organization in at least 33 countries.

There have already been extensive discussions over the question of what sort of behavior should be regarded as an act of war in cyberspace. Both the United States and China agree that there should be a high threshold for calling an event in cyberspace an act of war – not everything bad that happens in cyberspace is necessarily an attack. Most malicious activities in cyberspace do not involve attacks or warfare. At the same time, there are areas of ambiguity regarding the scope, duration and effect of cyber actions, and

---


these questions must be clarified. This includes pledges not to use cyber warfare and to refrain from developing cyber weapons.

**How to manage relevant network activities?**

Though network interconnection now transcends national boundaries, the management and operation of a network is still under the jurisdiction of a single country, and thus the principle of sovereignty must be appropriated applied. The real world is connected to the networked world, so the rules of the real world must also apply to cyberspace. The Budapest Convention, which was created in 2001, fails to adequately reflect the concerns of developing countries in fighting cybercrime. Additionally, there are inevitable concerns over violation of sovereignty and incompatibility with domestic legislations caused by transnational actions. A new international convention on cybercrime should be authorized within the United Nations framework at both the bilateral and multinational levels. Furthermore, an international management body should be created to ensure the equitable distribution of Internet resources.

In conclusion, both China and the United States should work together to enhance dialogue on cybersecurity so that they can play a positive role in strengthening mutual trust, reducing mutual suspicion, managing disputes and expanding cooperation. It is now apparent that cybersecurity is on the agenda of the world’s governments. Reducing some of the uncertainty
around cybersecurity is a good place to start, not only to guide states but also so that citizens know how they should behave.