China's Alternative Roles in Countering International Economic Cyber Espionage

Wang Xiaofeng

Abstract: This article examines China's respective roles as a suspect, victim, and stakeholder in countering international economic cyber espionage (ECE) activities. Refuting the widespread evidence and cases that have misguided those with interests or concerns in cyber security issues, the author underscores the cognitive defects and logical fallacies in the prevailing suspicion and accusations against China. Not only is China among the victims of ECE activities, it will face even more ECE threats in the future. With growing cyber capacity, however, China has been determined to develop into a strong cyber power while playing a more active role as a key stakeholder in containing ECE activities. To maintain a secure and favorable cyberspace, the international community must join hands in working out a common code of conduct in cyberspace, acknowledging China's strenuous efforts and indispensable role in international

Wang Xiaofeng is Associate Professor at the Center for American Studies, Fudan University. His mailing address is 680 Guoquan Road, Shanghai 200433, China. He can also be reached at xiaofeng@fudan.edu.cn. *This article was first presented at the Conference on Controlling Economic Cyber Espionage held on June 16–18, 2015, jointly sponsored by the Syracuse University Law School and NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). The author would like to thank the China National Social Sciences Fund for its financial support during the writing of this article.*

China Quarterly of International Strategic Studies, Vol. 2, No. 4, 549–568
DOI: 10.1142/S2377740016500251

cyberspace governance. The United States, in particular, needs to adopt a legal approach in seeking to settle ECE disputes with China while making more commitments to their bilateral cooperation against economic cybercrime.

Keywords: Economic cyber espionage (ECE); China's cyber strategy; global public space; China-U.S. relations.

Economic cyber espionage (ECE) activities have attracted increasing attention from the international community and become a hot topic especially between China and the United States, the two major cyber powers. The Chinese government is often accused of stealing technological talents and business secrets from or through the Internet, yet it has invariably denied such accusations. After the U.S. Department of Justice (DOJ) brought prosecution against five Chinese military officers in May 2014, the dispute intensified to such extent that it led the China-U.S. cyber dialogue to a long deadlock.[1] Fortunately, on Chinese President Xi Jinping's visit to the United States in September 2015, leaders from both countries reached a consensus that neither government would conduct and/or condone economic espionage in cyberspace,[2] which has greatly helped ease the frictions between both countries over the issue.

Although international ECE is acknowledged as a major challenge to the economic security of many countries, there has been limited cooperation among them on the issue, and there is no immediate prospect for a widely acceptable resolution. The linkage among the preferred rules of major cyber powers is weak if not absent. The U.S. government insists in differentiating ECE activities from cyber intelligence gathering for the purpose of national security, while China advocates that all cyber espionage is unacceptable.

---

[1]China decided to suspend talks within the China-U.S. Cyber Working Group when U.S. Department of Justice sued Chinese military officers and urged the U.S. government to stop making mistakes and recall the indictment. See "China Reacts Strongly to U.S. Announcement of Indictment against Chinese Personnel," May 20, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157520.shtml.

[2]Ellen Nakashima and Steven Mufson, "U.S., China Vow Not to Engage in Economic Cyber Espionage," *The Washington Post*, September 25, 2015, https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

Does China really employ a policy to encourage ECE activities over other countries as often suspected? How should China promote its image and role in countering international ECE? By examining the widespread suspicion and accusations against China, this article explores China's alternative roles in countering international ECE activities, and argues that China is not only a victim of such activities, but it also plays an ever more active role in cyberspace as a key stakeholder.

Suspicion of China's Involvement in International ECE Activities

Over the past decades, the Chinese government has been frequently suspected of sponsoring ECE activities over other countries. Such suspicion is mainly based on the following assumptions.

The first assumption is that China has adopted a state policy of participating in — or at least sponsoring — ECE activities, with the aim to acquire advanced technologies from Western countries. This is because Western countries have been exercising restrictions on technology transfer or export to China, due to ideological differences and geopolitical concerns.[3] Foreign companies are also reluctant to transfer core technologies and patents to China so as to maintain their competitive advantages. These facts, as some tend to believe, prevent China from obtaining advanced technologies through legal channels and in conventional ways. Therefore, when China continues its pursuit of an ambitious strategy for science and technology development with a rather limited R&D budget, it naturally invites wide suspicion. Some even believe that the whole "863 Project"[4] is actually an espionage program.[5]

The second assumption is that China owes much of its rapid development, especially its eye-catching innovations in high-tech fields, to economic espionage. China has experienced remarkable economic growth

---

[3]The export control policies include the Paris Coordinating Committee during the Cold War and the Wassenaar Arrangement since 1996.

[4]The "863 Project" refers to a state-sponsored project initiated by the Chinese government in March 1986 to promote development of advanced technologies in various fields. It was replaced by a new national R&D plan issued on February 16, 2016.

[5]Ulsch N. MacDonnell, ed., *Cyber Threat: How to Manage the Growing Risk of Cyber Attacks*, (New York, NY: John Wiley & Sons, Inc., 2014.), p. 36.

since its reform and opening-up. Especially in recent years, it has achieved a number of breakthroughs in biomedicine, materials technology, information and communications, and so on. Such impressive progress, as some might argue, is in large part a result of China's economic espionage, including ECE activities.

The third assumption is that the Chinese government helps its state-owned enterprises (SOEs)[6] to acquire business secrets and technological talents through economic espionage. Under the socialist market economy in China, major industries of finance, telecommunications, transportation, and utilities, as well as most large enterprises are either state-sponsored or state-owned. Central and local governments provide all kinds of support for SOEs, including favorable policies in labor, tax, financing and other aspects. In this context, it seems quite logical that governments at all levels in China would employ ECE as a secret measure to enhance the competitiveness of SOEs.

The fourth assumption is that China's military intelligence agencies are key organizations that take on ECE tasks. According to a report released by Mandiant and Crowdstrike,[7] the People's Liberation Army (PLA) has assembled dozens of hacking troops charged with a variety of duties and tasks. Besides performing regular offensive and defensive operations in cyberspace, the report presumes that they are also tasked to attack and intrude into systems and databases of foreign businesses, enterprises and research institutions, in order to steal trade secrets, technical talents and any other useful data.

All these assumptions tend to lead people to believe that China has both the incentive and the capabilities to carry out ECE activities, an inference that seems to be further strengthened by cases and evidence put forward by cyber security firms and intelligence agencies.

It is presumed that China has both the incentive and capabilities to conduct ECE activities.

[6] As of the end of 2015, there were about 150,000 SOEs in China.

[7] "Private U.S. Report Accuses Another Chinese Military Unit of Hacking," *Reuters*, June 10, 2014, http://www.reuters.com/article/2014/06/10/us-cybersecurity-china-idUSKBN0EL0N420140610.

Cyber security firms — Mandiant, FireEye, and McAfee, etc. — are major contributors of cases and evidence of China's suspected participation in international ECE activities. For example, Mandiant released a report entitled "APT1: Exposing One of China's Cyber Espionage Units" on February 19, 2013, claiming that Unit APT1, one of the PLA hacking troops, had stolen hundreds of terabytes of data from at least 141 organizations, compromising a broad range of industries in the United States and other English-speaking countries. It further reported that Unit APT1 belonged to the 2nd Bureau of the 3rd Department of the PLA General Staff Department (GSD).[8] Mandiant released another report in 2014 asserting that "the Chinese government is expanding the scope of its cyber operations, and China-based advanced threat actors are keen to acquire data about how businesses operate — not just about how they make their products."[9]

FireEye also reported that Unit APT18, a hacker group sponsored by the Chinese government, was keen on the data and information of U.S. medical device manufacturers and pharmaceutical companies — an allegation echoed by the Federal Bureau of Investigation (FBI) on August 18, 2014, warning U.S. healthcare companies of malicious threats to steal their intellectual property rights (IPRs) and personally identifiable information.[10]

Intelligence agencies of other Western countries have also disclosed many cases of suspect Chinese ECE activities. In June 2007, a report by the Canadian intelligence claimed that some Chinese in Canada carried out industrial espionage activities frequently. In May 2009, the German Federal Office for the Protection of the Constitution accused the Chinese government of cyber attacks and espionage on German companies, institutions and the federal government. In October 2012, Canadian Security Intelligence Service (CSIS) asserted that state-sponsored espionage from China threatened Canada's infrastructure.[11] In 2014,

[8]Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 19, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[9]Mandiant, "M-Trends® 2014: Beyond the Breach," April 9, 2014, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

[10]FireEye, "State of the Hack: Spotlight on Healthcare," August 2014, https://www2.fireeye.com/WBNR-14Q3HealthcareWebinar.html.

[11]Angela Gendron and Martin Rudner, "Assessing Cyber Threats to Canadian Infrastructure: Report Prepared for the Canadian Security Intelligence Service," March 2012, http://publications.gc.ca/collections/collection_2013/scrs-csis/PS74-1-2012-eng.pdf.

Communications Security Establishment Canada (CSEC) claimed that a Chinese government-supported cyber hacker group had intruded into the computer system of the National Research Council (NRC) and stole data and information.[12]

Still, the majority of suspected Chinese ECE cases have been disclosed by U.S. intelligence agencies. Every year since 2001, the U.S.-China Economic and Security Review Commission (USCC) would submit a report to the U.S. Congress, providing analyses and policy recommendations about China. In its fifth annual report submitted in 2007, the USCC put forward the "China espionage threat theory," indicating that China has continued to spy on U.S. military and industrial sectors, collecting U. S. high-tech intelligence by any means to promote the development of its related industries. According to the report, "Chinese espionage in the United States is so extensive, posing the greatest threat to the U.S. technology security."[13]

If China's ECE activities have reached such an intolerable level, there must be many evident cases of invasions, losses and other details. It is therefore somewhat strange that those purported victims — companies, research institutions, and government sectors — have had few, if any, details made public. A possible explanation is that they are unwilling to share their experiences for fear of vengeance. As Mike Rogers, Chairman of the U.S. House Intelligence Committee, said at an open hearing at the U.S. House of Representatives, "That's just the tip of the iceberg. There are more companies that have been hit that won't talk about it in the press, for fear of provoking further Chinese attacks."[14]

However, no evidence has been conclusive in supporting those accusations so far. Even if the cyber attacks can be traced all the way to China, it

---

[12]Communications Security Establishment report, July 29, 2014, https://www.cse-cst.gc.ca/en.

[13]U.S.-China Economic and Security Review Commission, *2007 Annual Report to Congress*, November 15, 2007, http://www.uscc.gov/Annual_Reports/2007-annual-report-congress.

[14]Mike Rogers, "Statement to the U.S. House, Permanent Select Committee on Intelligence, Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation," October 4, 2011, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf.

remains uncertain as to whether the Chinese government is behind those attacks or is carrying out a long-term and large-scale ECE policy. To begin with, scientific and technological R&D is a systematic, fundamental and lasting process, while the technological secrets obtained through ECE activities are random and fragmented. It is inconceivable that China owes its significant economic and technological achievements over the past years mainly to economic espionage. Since ECE activities are not sustainable in promoting economic and social development, the accusation that China has employed an ECE-sponsoring policy is not so convincing, and the perception of China achieving breakthroughs in key technologies by ECE is by and large groundless.

Moreover, the chain of purported evidence cannot explain how business and technological secrets are delivered from PLA cyber hacking troops and coordinating agencies to SOEs, and finally incorporated into certain completed products. If China does carry out large-scale, long-term and well-organized ECE activities, there must be some agencies that direct and coordinate this sophisticated process, yet no such agency has been found till now. For example, the most popular Mandiant report did not only fail to prove whether the Chinese government had planned those ECE activities, it also could not explain how business secrets were transmitted to Chinese SOEs, how Chinese enterprises benefited from the business secrets, or how much U.S. enterprises suffered from the data losses.

Evidence provided by the U.S. intelligence-complex may be misleading due to its own vested interests and dubious research methods.

Undoubtedly, cyber security companies and intelligence agencies have their own incentives to exaggerate risks, threats and losses associated with cyber espionage, and thus may mislead policymakers and public opinion. With the growing strategic competition between China and the United States in recent years, it is likely that the so-called intelligence-complex, which consists of intelligence agencies, related Congress members and cyber security companies, plays a key role in fabricating an atmosphere of cyber threats from China. For example, in his first policy remarks on cyberspace security delivered in May 2009, President Obama said that "last year alone cyber criminals stole IPRs from

businesses worldwide worth up to $1 trillion."[15] The number was quoted from *Cyberspace Policy Review*, which originated from a McAfee report.[16] President Obama repeated this number of $1 trillion many times later. Yet in 2013, McAfee and CSIS modified the number to $100 billion and admitted the bug in their calculating methods.[17] It creates concerns about President Obama's claim and even the U.S. cyber policy have been based on this severely exaggerated number.

U.S. judgment is also influenced by the intrinsic tendency of American foreign policy to seek adversaries or enemies. Arguably, the United States has been pursuing a policy of containing potential challengers so as to maintain its leadership in the real world as well as in cyberspace. To the United States, China is an emerging power in the Asia Pacific; Iran is a potential threat in the Middle East; and Russia is the biggest challenger on the European continent. When these countries develop enough strengths, many Americans believe, they will become adversaries regardless of their actual intents. Thus, criticizing their involvement in ECE activities can serve as another means of containment.

Finally, it is doubtful that undertaking highly complex ECE activities is within China's technological capabilities. According to the Mandiant report and U.S. DOJ indictments against Chinese military officers, hackers from China used a few basic means of cyber espionage, such as spear phishing attacks, deception emails for passwords, as well as Trojans and other simple tools, yet the use of "Chinese-style English" and those variables and comments in the codes of compiled programs could easily be tracked. "Chinese top advanced hackers" as they were called, these alleged hackers were apparently not well-trained. Thus, even if these hackers are indeed from China, their maladroitness only proves that China's cyber intrusion technology and capabilities are well below the international level.

---

[15]"Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[16]"Assuring a Trusted and Resilient Information and Communications Infrastructure," *Cyberspace Policy Review*, May 29, 2009, p. 2.

[17]James Lewis and Stewart Baker, "The Economic Impact of Cybercrime and Cyber Espionage," July 23, 2013, http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

Given that there is little hard evidence to prove or negate those accusations against China, the key lies in whether the Chinese government demonstrates a positive attitude and adopts effective measures in countering international ECE activities. As major cyber powers have differed sharply on the basic norms and rules to regulate ECE activities, it is of urgent importance to foster consensus in this regard rather than make questionable accusations against each other.

China's Response to Western Accusations

Growing ECE activities worldwide harm the competitiveness and profits of attacked enterprises, research institutions and government sectors. In a broader sense, large-scale and long-term ECE activities will impair economic prosperity and technological innovations of a country.[18] As China has been a victim of ECE activities itself, the many accusations against it are not only unfair, but may also have far-reaching consequences on the country.

First, ECE accusations against China have tarnished China's international reputation and credibility. For the past decade, China has been portrayed as a thief of IPRs and trade secrets, a major threat to cyberspace security and stability. China's negative image with respect to Internet freedom is also deep-rooted due to its domestic Internet censorship and content filtering. This runs counter to the image of a "responsible major power," a keen supporter of international peace, and an active defender of the world order that the Chinese government has been trying to project. Despite the strenuous efforts of the Chinese government to win international acquittal and to reaffirm its stand against international ECE activities, suspicion from Western countries prevails, causing them to be very cautious when dealing with China in cyber-related business and, even worse, to cast doubts on every Chinese engagement in the international agenda. The situation seriously hinders China's ambition and endeavors to make more contributions to the international community.

Second, those accusations have greatly affected China's outbound investments in foreign markets, as the argument against Chinese investment has changed from concerns of IPRs protection to national security. For

[18]The White House, *National Security Strategy*, February 2015, p. 7.

example, Huawei, one of the leading Information Communications Technology (ICT) product and service providers in the world, has offices and research facilities in about one hundred countries spanning most of the continents. And it entered the U.S. market as early as in 2001. But in 2012 only 3.7 percent of Huawei's $35 billion sales revenue was from the U.S. market, largely due to the many barriers from IPRs disputes to information security audits. In 2012, the U.S. House of Representatives Permanent Select Committee on Intelligence even went so far as to claim that because of its "PLA background," Huawei would pose potential threats to U.S. national security interests if it was allowed to participate in the U.S. telecommunications infrastructure.[19]

Lenovo, one of the world's largest personal computer equipment manufacturers, also encountered many obstacles in the U.S. market. When Lenovo decided to purchase IBM's personal computer business in 2005, an acquisition worth $1.25 billion, it was placed under a 60-month investigation by the U.S. government. In 2007, when the U.S. Department of State was going to buy 16,000 computers from Lenovo, some questioned Lenovo's government background and appealed to the Congress for investigations. When the deal was completed, some members of the U.S.-China Economic and Security Review Commission continued to express their concerns over potential data leaks and national security threats. The U.S. government also spent a lot of time investigating Lenovo's acquisition of IBM ×86 low-end server business sectors in 2013. The acquisition finally succeeded only after Lenovo expended much additional time and efforts.

It can be seen from both cases above that endeavors of Chinese enterprises to expand into overseas markets like the U.S. are often impaired because they are suspected of being part of China's ECE plans, especially when they are funded by the government or have a military background. For China, expanding overseas investments is an important part of its economic restructuring. Chinese companies need a favorable investment environment that hinges on mutual trust between China and its business partners. The ECE accusations against China, however, have damaged the trust, which

[19]U.S. House Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," October 8, 2012, http://intelligence.house.gov/press-release/investigative- report-us-national-security-issues-posed-chinese-telecommunications.

ultimately undermines the potential for Chinese enterprises to participate in international markets and affects China's economic development.

ECE accusations against China have greatly harmed China's image and its overseas investment potential.

From China's perspective, the United States government and that of some other Western countries have joined their public media in a new wave of "anti-Chinese chorus" by capitalizing on the ECE issue. The first intensive media coverage on China's involvement in ECE activities occurred on February 8, 2007, when *The Mirror Newspapers* reported that Chinese hackers had taken a series of offensive actions.[20] Western mainstream media have swung into concerted actions of exposing and criticizing China's purported ECE activities since then, creating an image of the Chinese government as sponsor and beneficiary of those activities.

Especially after the release of the Mandiant report in February 2013, international ECE has grown to be a major issue in China-U.S. bilateral dialogues at all levels including the strategic and economic dialogue (S&ED) and other talks on defense, judicial and trade affairs, where the United States has been exerting political and diplomatic pressures on the Chinese government. Other Western countries have followed suit by bringing more charges against China. For instance, Stephen Harper, then Prime Minister of Canada, publicly blamed China for supporting cyber espionage in July 2014.

When diplomatic pressure fails to achieve expected results, Western countries tend to take judicial measures against China's purported ECE activities. On May 19, 2014, The U.S. DOJ charged five Chinese military officers of computer hacking, economic espionage, and other offenses directed at six victims in U.S. nuclear power, metals, and solar products industries — the first criminal charge filed against known state actors for hacking.[21] The United States also began to exercise economic sanctions. In April 2015,

[20]Jürgen Dahlkamp, *et al.*, "Die gelben Spione: Wie China deutsches Know-how ausspäht," *Der Spiegel*, Ausgabe 35, 2007, pp. 19–34.

[21]FBI: "Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.," May 19, 2014, http://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s.

the White House issued a presidential executive order named "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities."[22] According to the order, the U.S. Department of Treasury is entitled to freeze the property of hackers who intrude into the U.S. banking and power systems and steal credit card information.

China's responses to those accusations are consistent but evasive. The Chinese government has invariably denied all ECE charges that are without sound proof. Yet it is reluctant to clarify whether it did sponsor or participate in ECE activities; instead, it has emphasized that Chinese law forbids any form of cyber espionage and that China itself is a victim of cyber attacks.

China's Ministry of Defense did not make any clarification of those charged units, but declared that the Chinese military had never supported any hacking activities and accused the Mandiant report of lacking technical and legal grounds. It stated that the evidence provided by the Mandiant report linking the IP and building addresses to specific hackers "had no technical basis." Geng Yansheng, spokesman of the Ministry of Defense, further elaborated that the PLA terminal had also suffered from frequent attacks from the Internet and that while the IP addresses pointed to a considerable number of attacks from the United States, the PLA had never accused the U.S. government for hacking.[23]

In a similar tone, China's Ministry of Foreign Affairs (MFA) criticized the United States for using those accusations to promote its hegemony in cyberspace, saying that the U.S. indictment on Chinese military officers "is based on deliberately fabricated facts, grossly violates the basic norms governing international relations and jeopardizes China-U.S. cooperation and mutual trust," and that the United States should "immediately correct its mistake and withdraw the indictment."[24] When the Snowden leaks

---

[22]The White House, "Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

[23]"Chinese Military has never been Supporting Hacking Activities," *China's Ministry of National Defense Press Briefing*, February 28, 2013, http://www.mod.gov.cn/affair/2013-02/28/content_4439577.htm.

[24]"China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel," May 20, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157520.shtml.

indicated that the U.S. National Security Agency (NSA) had attacked the data center of Tsinghua University, invaded Huawei's internal network system and monitored communications of Chinese leaders, the MFA voiced harsh criticisms that the U.S. government "has an ulterior motive," "applies double standards," and is "a robber acting like a cop."

Furious about the U.S. DOJ indictment, China's MFA announced the suspension of the China-U.S. Cyber Working Group activities. This is not only because the indictment caused a sense of humiliation upon China, but also because the Chinese government wanted to safeguard the principle of sovereignty in cyberspace.

After more details were disclosed about the secret NSA Internet and communication surveillance program PRISM, the Chinese government declared

> *The United States should stop playing victim, because it [is] itself the empire of hackers, as is known to people from around the world...Instead of reflecting on and behaving itself, U.S. is still making groundless accusations and launching verbal attacks at others. It is not constructive at all.*[25]

Chinese scholars also sided with their government in denouncing the United States hyping up the ECE issue to its own benefit.[26] As some commentators believe, China has begun to regain the moral high ground on cyber security issues in China-U.S. relations.

China's Stakes in Countering International ECE

Although accusations from Western countries have cast China as a saboteur of peace and security in cyberspace, China has indeed never been immune

---

[25]China Foreign Ministry Spokesperson Hua Chunying's regular press conference, June 10, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1164254.shtml.

[26]See, for example, Xu Lei, "Cyber Espionage: The Robber Acts like a Cop," *People's Daily* (Overseas Edition), May 23, 2014, p. 12, and "Ridiculous Prosecution Injures Others and Ruins Oneself," *People's Daily*, May 24, 2014, p. 3.

from international cyber espionage including ECE activities. Some may argue that China does not enjoy much technological advantage and thus is not worthy of economic espionage. Yet China's rapid technological progress in recent years and its increasingly informatized economy have turned it into a potential target of economic espionage.

As Cai Mingzhao, China's former Director of the State Council Information Office (SCIO), pointed out at the Fourth World Cyberspace Cooperation Summit on November 5, 2013,

> *Between January and August this year, more than 20,000 websites based in China were modified by hackers and more than 8 million servers were compromised and controlled by overseas computers via zombie and Trojan programs. These activities have caused severe damage to our economy and the everyday life of the people. More than 80 percent of Chinese Internet users have fallen victim to cyber attacks at some time or other. The annual economic losses run to tens of billions of dollars a year.*[27]

In fact, China has long suffered from international ECE activities, and its numerous SOEs, especially giant enterprises, are the primary targets. Other than exclusive techniques in some traditional Chinese industries, information on the SOEs' negotiation tactics, procurement plans and other business secrets, as well as related government policies, are all of special interest to overseas business spies. In the Rio Tinto commercial espionage case, for instance, Australian miners obtained in advance the average gross margins and other key confidential information regarding the Chinese steel industry. As a result, China's steel enterprises had to pay hundreds of millions of dollars more for iron ores purchased from Australia.[28]

China itself has long been a victim of international ECE.

[27]Cai Mingzhao's Keynote speech on the Fourth World Cyberspace Cooperation Summit, November 5, 2013, http://transpacifica.net/2013/11/full-text-speech-by-minister-cai-mingzhao-at-cybersummit2013-nov-5-2013/.

[28]Tong Hao and Wang Linyan, "Govt: Proof against Rio Spies Sticks," *China Daily*, July 10, 2009, http://www.chinadaily.com.cn/bizchina/2009-07/10/content_8406487.htm.

China has also traced many cyber attacks to sources in the United States, and the Chinese government has been in strong opposition to the U.S.' aggressive cyber strategy, such as the NSA's intelligence program of surveillance and invasion of the global telecommunications system and the Internet.

However, blaming each other cannot eliminate international ECE activities, especially when such accusations have diminished the moral standing of both sides, and compromised their potential cooperation in countering ECE, without which it will be hardly possible to locate and identify the real sources of suspicious ECE activities. It is thus important for China, the United States and other countries to join hands in containing international ECE. The political willingness of related governments, rather than technological means or judicial approaches, is key to success of their cooperation.

As the world's strongest cyber powers, the United States and China should work together to formulate a set of common norms and rules and take consistent actions by promoting their mutual understanding and fostering a sense of shared responsibility. Fortunately, since 2015 they have begun expanding areas of cooperation in judicial assistance, technical information sharing and other anti-ECE measures through various bilateral mechanisms, which hopefully will serve as a solid basis for future global cyberspace governance.

China as a Key Stakeholder in Cyberspace

With growing capacity both in the real world and in cyberspace, China has been playing an ever more active role in countering international ECE activities. The Chinese government has been determined to strengthen its cyber security and become a responsible cyber power. This means that China will not only continue to explore appropriate policy measures to safeguard its national security and other interests, but also try to enhance mutual understanding and consensuses with other cyber powers. Acknowledging the detrimental effect of the ECE issue on China's development and its relationship with other countries, Chinese President Xi Jinping proclaimed that "We should manage well relations with other major

countries and build a sound and stable framework of major-country relations."[29]

In fact, China has made extensive effort to translate its diplomatic stance into national law and government policies. China's law forbids any form of cyber attacks or cyber espionage, regardless of its origin or target. China's Counter-espionage Law does permit national security agencies to taking technical reconnaissance measures,[30] but the scope of, and the authority for, such measures are limited to the sole purpose of countering espionage. Besides, a new National Security Law of China has been proposed to enhance measures to prevent and punish cyber attacks, cyber theft and illegal spread of harmful information.[31]

China's efficient decision-making and implementation mechanisms also contribute to its efforts to counter ECE activities. With the largest number of Internet users, and as the biggest e-commerce market and a major manufacturing base of IT products, China has become a key stakeholder in cyberspace. To maintain a safe and dynamic cyber environment, the Chinese government has established effective technological and administrative mechanisms for tracking almost all domestic activities in cyberspace, which is crucial to operations of tracing online behaviors, collecting suspect evidence and containing ECE activities.

Nevertheless, effective global cyberspace governance requires all countries to make best efforts separately as well as in cooperation, the key to which is to develop a whole set of common norms and rules in cyberspace.

Above all, countermeasures to international ECE activities should be placed under an intergovernmental cooperation regime. International ECE is a result of interactions between cyberspace and the real world, yet the governance of cyberspace is still under much controversy. China insists that the security and development of cyberspace is a domestic issue, and sovereignty

---

[29]"China Eyes More Enabling International Environment for Peaceful Development," *China Daily*, November 30, 2014, http://africa.chinadaily.com.cn/china/2014-11/30/content_18998582.htm.

[30]Counterespionage Law of the People's Republic of China, approved by the Standing Committee of the 12th National People's Congress of the People's Republic of China, November 1, 2014.

[31]National Security Law (draft) of the People's Republic of China, May 6, 2015, http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-05/06/content_1935766.htm.

should be exercised over cyberspace control, while the stance of the United States and other Western countries remains vague.[32] Since ECE activities are usually cross-border crimes, effective countermeasures to ECE necessarily hinge on the cooperation among related governments. Thus, a multilateral intergovernmental platform should be created for rule-making and dispute-resolution. The international society can either put the cyber security issues on the United Nations security cooperation agenda, or consider establishing a common network for coordination of government policies as well as for international investigation and attribution of suspect cybercrimes. The successful experience of the International Atomic Energy Agency (IAEA) in nuclear arms control serves as a good example in this regard.

Furthermore, major cyber powers — China, the United States, Russia, Iran, among others — must strive to achieve a consensus on the code of conduct in cyberspace, including that on acceptable forms of state-sponsored cyber espionage. China has been a strong advocate for international cyber cooperation, and measures have been taken to incrementally enhance such consensus. For example, in April 2015, China's Ministry of Public Security (MPS) and the U.S. Department of Homeland Security (DOHS) reached a common understanding on conducting closer cooperation on cyber-enabled crimes;[33] in May 2015, Russia and China also signed an agreement on cooperation for ensuring international information security, in which both countries pledged not to launch cyber attacks against each other, and agreed to jointly counteract technologies that may "destabilize the internal political and socio-economic atmosphere, disturb public order or interfere with the internal affairs of the state."[34]

---

[32]Some American specialists argue that the content of the Internet is not subject to sovereignty. See, for example, Christopher M. E. Painter, "Cyber Security: Setting the Rules for Responsible Global Behavior," Testimony before the Senate Foreign Relations Committee: Subcommittee on East Asia, the Pacific, and International Cyber Security Policy, May 14, 2015.

[33]U.S. Department of Homeland Security, "Fact Sheet: Meeting between U.S. Secretary of Homeland Security Jeh Johnson and China's Minister of Public Security Guo Shengkun," April 12, 2015, http://www.dhs.gov/news/2015/04/12/fact-sheet-meeting-between-us-secretary-homeland-security-jeh-johnson-and-chinas.

[34]Foreign Ministry of Russia, "Signing a Russian-Chinese Intergovernmental Agreement on Cooperation in Ensuring International Information Security," May 6, 2015, http://government.ru/en/docs/17952/.

Bearing similar significance to the Chinese pledge to not be the first to use nuclear weapons under any circumstances, the commitment of major cyber powers to refrain from launching cyber attacks against each other is a great breakthrough in global cyber security governance. In this sense, Russia and China are pioneers in building trust and mitigating hostility in cyberspace, and their mutual commitment serves as a good example for other cyber powers. For instance, shortly after China and the United States reached a consensus on controlling ECE activities in September 2015, China and the United Kingdom also struck a deal "not to conduct or support cyber-enabled theft of intellectual property, trade secrets, or confidential business information with the intent of providing competitive advantage."[35] In June 2016, a similar consensus was included in a joint statement during the fourth round of intergovernmental consultation between China and Germany as well.[36]

Finally, the cooperation between China and the United States should be a starting point of global counter-ECE campaigns, for the most bitter disputes and conflicts in cyberspace so far have occurred between these two countries. The United States should not make a set of rules unilaterally and expect China to merely accept. Nor is it constructive for the United States and its security partners to develop one set of rules while China, Russia and other countries develop another — that would inevitably undermine the freedom and connectivity of the Internet and divide the world into two confrontational blocs in cyberspace.

Major cyber powers should work together to lead international efforts to counter economic cyber espionage.

For China, ECE is not defined as a national security problem, but the U.S. government has regarded the ECE issue as a major national security threat, highlighting its severity in recent strategic documents such as the

[35]"China-UK Joint Declaration on Building a Global Comprehensive Strategic Partnership for the 21st Century," October 22, 2015, http://www.chinadaily.com.cn/world/2015xivisituk/2015-10/22/content_22257782.htm.

[36]Fraser Cameron, "Merkel's Ongoing Visit Focused Squarely on Economy," *China Daily*, June 13, 2016, http://www.chinadaily.com.cn/opinion/2016-06/13/content_25687491.htm.

National Security Strategy, National Intelligence Strategy, National Defense Strategy Report and the International Strategy for Cyberspace. Taking ECE as a national security issue rather than a legal one greatly reduces the possibility of international cooperation. Therefore, the U.S. government should exercise more restraint in dealing with the ECE issue so that it does not impair the mutual strategic trust and cooperation in broader areas with other major cyber powers.

The Chinese government's advocating for a new model of major power relationship, which aims to break the historical pattern of confrontation and conflicts between an emerging power and an established power, generates a promising prospect for a secure cyberspace. If all major cyber powers can join efforts to enhance global cyber security governance, it will be conducive not only to peace and cooperation among major powers, but also to economic and social development of the world in this information age.

Conclusion

Since early history, espionage has been a widely used instrument to enhance national security and other interests, and in recent years cyber espionage has brought about growing international concerns. Boundaries between economic cyber espionage, security cyber espionage, and open gathering of economic information in cyberspace remain blurry, and a global regime for cyber security governance has yet to be built. If unchecked, cross-border ECE activities will continue to pose great threats to peace, security and prosperity in cyberspace and the real world. Given that mutual understanding and a common code of conduct is required to tackle the issue more effectively, all cyber powers need to draw on the experience and expertise in global governance of other public spaces such as aerospace and international water in their cooperation to maintain an open and peaceful cyberspace.

Admittedly, effective governance of global public space is based on the consensus of major powers and the participation of various stakeholders. As Stephen D. Krasner pointed out, "Where there have been disagreements about basic principles and norms and where the distribution of power has been highly asymmetrical, international regimes have not developed.

Stronger states have simply done what they pleased."[37] This is a basic tenet in the international regime theory, and cyberspace is exactly such a globally shared space with diversified stakeholders and highly asymmetrical distribution of power.

Establishment of a global regime for cyber security governance depends on constructive interactions among major cyber powers — especially between the United States and China — to foster commonly shared basic principles in sovereign jurisdiction, the innocent passage, the freedom of expression, and other cyber-related issues. With growing capabilities and increasing stakes in countering ECE activities, China and other major cyber powers are expected to work more closely together to shape the future of cyberspace.

[37]Stephen D. Krasner, "Global Communications and National Power: Life on the Pareto Frontier," *World Politics*, April 1991, 43(3), p. 337.