The Suspect and the Victim: China's Alternative Roles in Controlling Economic Cyber Espionage

Wang Xiaofeng*

Introduction

In recent years, economic cyber espionage (ECE) has been of great international concern and has become a major problem in the U.S.-China relations. The Chinese government has been frequently accused of stealing technology talents and business secrets from or through the Internet, while it invariably denied such activities or policies. When the U.S. Department of Justice (DOJ) brought prosecution against five Chinese military officers in May 2014, the dispute intensified and the U.S.-China cyber dialogue came to a deadlock.[1]

Simultaneously, China has suffered more and more from ECE and other kinds of cyber attacks, against which some measures have been taken by the Chinese government to secure cyberspace and protect data, including constructing independent and controllable information infrastructure, removing some foreign technology companies from the procurement list of the central government, and requesting companies that provide products or services to Chinese banks to submit their source codes and provide access ports which enable government officers to manage and monitor operating data.

ECE is widely acknowledged as a new global public issue many countries are facing nowadays. International cooperation in controlling ECE is insufficient and there is no immediate prospect of a widely acceptable resolution. The linkage between the rules of major cyber countries is weak if not absent. The U.S. insists on differentiating ECE from security cyber intelligence gathering, while China asserts that all cyber espionage is unacceptable.

This paper will analyze the logic of the accusation that China is a suspect and of the argument that China is also the victim of ECE. Does China really pursue a policy of promoting ECE? Why do the U.S. and other countries assert that China pursue such

* Assistant Research Fellow, Center for American Studies, Fudan University, Shanghai, China.

[1] China decided to suspend activities of the China-U.S. Cyber Working Group when U.S. DOJ sued Chinese military officers. 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

a policy? And how will China play a positive role in controlling ECE?

1. China as a Suspect of ECE

Despite its repeated denials, the People's Republic of China is deemed at the forefront of nation-state sponsored ECE. This section will examine the rationales for the suspicions and assumptions that the Chinese government pursues a long-term and systematic policy to acquire technology patents and business secrets from and through cyberspace to help its state-owned enterprises (SOEs), and will point out a few flaws in the logic of the accusations against China.

A. Suspicions and Assumptions

The accusations that the Chinese government sponsors or participates in ECE have been discussed for many years. Generally, these accusations are mainly based on certain suspicions and assumptions.

The first assumption is that China pursues a national policy of sponsoring or participating in ECE. Its purpose is to get advanced technology from other countries, mainly from Western countries, to help its high-tech industry. Because of ideological and political differences, Western countries have followed technology export control policies against China.[2] For a long time, China has budgeted low expenditure vis-à-vis the high prices of some advanced technology and equipment. And some companies are unwilling to transfer core technology and patents to China in order to maintain competitive advantage. These facts prevent China from obtaining advanced technologies through legal channels and in conventional ways. Some argue that China's frog-leap development strategy in science and technology implies using unscrupulous means to achieve its goals. Some even view the whole "863 Project" as an espionage program.[3] Most of the suspicions and assumptions presume that it is the Chinese government's policy or at least Chinese government supports such activities.

The second assumption is that the Chinese government helps its SOEs to acquire business secrets and technology talents through economic espionage. China has established a socialist market economy. To meet the requirements for government control, those major industries of finance, telecommunications, transportation and utilities and other large enterprises are either state sponsored or state owned. It is

[2] The export control policies include the Paris Coordinating Committee during the cold war and Wassenaar Arrangement since 1996.

[3] "The Emergence of the Cyber Nation-State and Technology Espionage Red China Rising and Its Global Cyber Theft Strategy", in Ulsch N. MacDonnell ed., *Cyber Threat: How to Manage the Growing Risk of Cyber Attacks*, John Wiley & Sons, Inc., 2014. p36.

reasonable for central and local governments to provide all kinds of support to SOEs. Since the Chinese government used to help SOEs in labor, tax, financing and other issues, it is undoubtedly logical for governments at all levels in China to take ECE as one of the secret measures to enhance the competitiveness of SOEs.

The third assumption is that China has achieved fast improvement and successful innovations in high-tech fields through economic espionage. Since the implementation of the reform and opening policy, China has achieved sustainable and remarkable economic growth. The progress in the fields of science and technology and the unusually greater product competitiveness are also prominent. In recent years, a series of high-tech breakthroughs have been made in the fields of biomedicine, materials technology, information and communications, and so on. Some argue that China's achievements have benefited much from economic espionage,as well as ECE.

The fourth assumption is that China's military intelligence agencies are the primary functional units that take on ECE tasks. According to the reports released by Mandiant and Crowdstrike,[4] the military units 61398 and 61486 are two of the dozens of the People's Liberation Army (PLA) hacking troops. It is assumed that these PLA hacking troops are charged with a variety of duties and tasks. Besides undertaking regular offensive and defensive operations in cyberspace, they are also asked to attack and intrude into the system and database of business enterprises and research institutions in order to steal trade secrets, technical talents and any useful data from and through the Internet.

These suspicions and assumptions represent the cognitive basis for China's ECE activities. It is therefore assumed that China both has incentives to and carry out operations of ECE.

B. Cases and Evidence

It is the existing cases and evidence that lead to the conviction that Chinese government is involved in the cyber conspiracy. These cases and evidence have been raised by many sources, mainly by cyber security firms and intelligence agencies.

Due to technical complexity and behavioral invisibility, the cases and evidence of China's participation in ECE are mainly revealed by cyber security firms. FireEye & Mandiant and McAfee are active and provide many comprehensive disclosure reports. Mandiant's most noticeable report was released on February 19, 2013, titled

[4] "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

APT1: Exposing One of China's Cyber Espionage Units, [5]which announced that Mandiant had dug out the APT1, a Chinese PLA hacking unit, which had systematically stolen hundreds of terabytes of data from at least 141 organizations and focuses on compromising organizations across a broad range of industries in the U.S. and other English speaking countries.[6] Cyber experts from Mandiant had tracked more than 20 known Chinese APT hacker groups, one of which is unit 61398 - the most persistent of China's cyber threat actors. The report concludes that APT1 is government sponsored and belongs to the 2nd Bureau of the 3rd Department of PLA General Staff Department's (GSD).

Mandiant published another report in 2014 to continue revealing China's ECE activities, asserting that "[t]he 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."[7] When the FBI warned on August 18, 2014, healthcare companies that malicious threat actors are targeting them in an attempt to steal intellectual property and personally identifiable information, Fireeye soon revealed the hacker group APT18, one of Chinese nation-state actors who were keen on the data and information of the U.S. medical device manufacturers and pharmaceutical companies.[8]

Intelligence agencies also have the technical capacity, investigative techniques, and more importantly the authority and credibility. Since 2007, intelligence agencies of Western countries have disclosed many cases of China's ECE activities. In June 2007, a Canadian intelligence report 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) pointed out that state-sponsored espionage from China threatened Canada's infrastructure.[9] In 2014, Communications Security Establishment Canada (CSEC) claimed a highly complex

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

[6] "Chinese military unit 'behind prolific and sustained hacking'", February 19, 2013, http://www.bbc.com/news/world-asia-china-21502088

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

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

[9] "Assessing Cyber Threats to Canadian Infrastructure: Report Prepared for the Canadian Security Intelligence Service", October 1, 2012. http://publications.gc.ca/collections/collection_2013/scrs-csis/PS74-1-2012-eng.pdf

Chinese government supported cyber hacker group had intruded into the computer system of the National Research Council (NRC) and stolen data and information.[10]

Still, most of the Chinese ECE cases are disclosed by the U.S. intelligence agencies. Every year since 2001, the Congress U.S.-China Economic and Security Review Commission (USCC) would submit a report to Congress, providing the appropriate basis for policy recommendations toward China. In the fifth report in 2007, USCC produced the "China espionage threat theory", indicating that China continued to spy in the U.S. military and industrial fields. China used all means to collect the U.S. high-tech intelligence to promote the development of related industries. The report stated that "Chinese espionage in the United States is so extensive, pose the greatest threat to the U.S. technology security." [11]

It is somewhat curious that the companies and institutions, the purported victims, have no details made public. Since China's ECE has reached an intolerable level, there must be a lot of cases of invasions, losses and other details. One explanation is that those companies and institutions are not willing to publicize their experiences for fear of credit damage and trust loss. Once at an open House hearing, Reprehensive Mike Rogers, Chairman of the U.S. House Intelligence Committee said, "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." "When you talk to these companies behind closed doors, they describe attacks that originate in China, and have a level of sophistication and are clearly supported by a level of resources that can only be a nation-state entity."[12]

C. Actions and Responses

① Actions by U.S and other Western Countries

From China's point of view, the governments of the U.S.-led Western countries and their media have joined a new wave of anti-Chinese chorus by making use of the ECE issue.

The Western media have special interest and enthusiasm in the topic of China's purported ECE activities. The first intensive media coverage on China's involvement

[10] July 29, 2014. https://www.cse-cst.gc.ca/en , http://publications.gc.ca/collections/collection_2013/scrs-csis/PS74-1-2012-eng.pdf

[11] 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

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

in ECE occurred in 2007. On February 8, 2007, The Mirror Newspapers reported that Chinese hackers had taken many more offensive actions. Western mainstream media then swung into concerted actions of exposing and criticizing China's purported ECE activities, trying to convince the public that China pursued a policy of promoting ECE. From the Mandiant report in 2013 till now, China's purported ECE activities have attracted a new wave of coverage from the Western media. It is the media that had the image of China deeply embedded in the public opinion in the U.S. and other western countries.

The U.S. tried to exert political and diplomatic pressures on the Chinese government. Nearly all the U.S. departments and agencies expressed to their Chinese counterparts their concern over ECE activities. Since February 2013, when the Mandiant report was released, ECE has always been an important and inescapable issue in the U.S.-China bilateral dialogues at all levels, such as the strategic and economic dialogue, the defense dialogue, judicial dialogue and trade dialogue,. The U.S. officials, from President to Secretary of State, Secretary of Defense, Secretary of Commerce, etc, continue exerting pressures on the Chinese government. Other Western countries followed suit and made more accusations against China. Stephen Harper, the Prime Minister of Canada, publicly accused China's cyber espionage in July 2014.

Since diplomatic pressures didn't match the expectation, the U.S. decided to take judicial measures against China's purported ECE activities. On May 19, 2014, five Chinese military hackers were charged by the U.S. DOJ with cyber espionage against the U.S. In a case before the Federal Court Western District of Pennsylvania, five Chinese military hackers were indicted on charges of computer hacking, economic espionage, and other offenses directed at six victims in the U.S. nuclear power, metals, and solar products industries. This marked the first criminal charges filed against known state actors for hacking.[13]

Economic sanctions are also under consideration. In April 2015, the White House issued a presidential executive order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". [14]According to this

[13] "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

[14] Barack Obama, "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

sanction policy, the U.S. Department of Treasury will be able to freeze the property of the hackers who intrude in the U.S. banking system and power system and steal credit card information. In a statement for the executive order, The U.S. President Obama intentionally singled out ECE hackers from China, Russia and Iran.

② Defenses and Response of China

China's defenses against and response to the ECE accusations are consistent but evasive. The Chinese government denied all the accusations of ECE without any investigations. Facing the growing chorus of accusations and criticism about ECE from the U.S. and other Western countries, the Chinese government did not clarify whether or not it participated in ECE; it instead only stated that its law forbids any form of cyber espionage activities and that China itself is a victim of cyber attacks.

China's Ministry of Foreign Affairs stated that the purpose of the U.S. is to seek hegemony in cyberspace. The indictment "is based on deliberately fabricated facts, grossly violates the basic norms governing international relations and jeopardizes China-U.S. cooperation and mutual trust." The U.S. should "immediately correct its mistake and withdraw the indictment."[15] When Snowden leaks indicate that NSA had attacked the data center in Tsinghua University, invaded Huawei's internal network system and monitored Chinese leaders' communications, China's Ministry of Foreign Affairs voiced severe criticisms that the U.S. government "has an ulterior motive", "applies double standards", and is "a robber acting like a cop".

China's Ministry of National Defense did not make any clarification on the existence/absence of unit 61398 and its mission, but declared that the Chinese military had never supported any hacking activities and accused the Mandiant report of lacking technical and legal grounds. It asserted that Mandiant's evidence linking the IP address, the building and the hackers had no technical basis. Geng Yansheng, spokesman of the Ministry of National Defense, said that the PLA terminal had suffered a lot of outside attacks from Internet and that while the IP addresses pointed to a considerable number of attacks from the U.S., the PLA had never blamed the U.S. for the hacking.[16]

Furious about the U.S. DOJ indictments against five Chinese military officers, China's Ministry of Foreign Affairs announced the suspension of the U.S.-China

[15] "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

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

Cyber Working Group activities. The direct cause was that the indictments resulted in a sense of losing face on the part of the Chinese government, and the indirect cause was that the Chinese government wanted to defend the principle of sovereignty in cyberspace, which does not mean that the Chinese government sponsors or sustatins network theft activities.

After Edward Snowden disclosed the secret NSA telecommunication and internet surveillance program PRISM, China made a new set of defenses to the accusations. "The U.S. is not entitled to irresponsible remarks." "The U.S. should stop playing victim, because it itself is the empire of hackers, as is known to people from around the world. Instead of reflecting on and behaving itself, the U.S. is still making groundless accusations and launching verbal attacks at others. It is not constructive at all."[17] Some commentators believed that China has regained the moral high ground on cyberspace security issues in the U.S.-China relations.

Chinese media and scholars are generally in step with the government. There is nearly no one admitting China's participation in ECE activities. Although the media and scholars in China may sometimes demonstrate their independence to some extent, they are in close line with the central government on the ECE issue. In the case of DOJ indictments against Chinese military officers, Chinese media and scholars mainly focus on the legitimacy of the indictments against foreign public officials, the differences between security espionage and economic espionage, the negative effect on the U.S.-China diplomatic and military relations, etc.[18] There is a consensus among Chinese scholars that the U.S. government mainly wants to exert pressures on China by means of the ECE issue.

D. Flaws in the Logic

Although the accusations have been supported by cases and evidence, it is still questionable that the Chinese government carries out a long-term, large-scale and systematic ECE policy.

First, science and technology R&D is systematic, fundamental and permanent, while the stolen secrets are fragmented and casual. It is inconceivable that China's economic and technological achievements mainly depend on economic espionage.

Secondly, the chain of evidence cannot explain how the business secrets are

[17] 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

[18] Xu Lei, "Cyber Espionage: the Robber Acts like a Cop", *People's Daily* Overseas Edtion, May 23, 2014. p12. "Ridiculous Prosecution Injures others and Ruins oneself", *People's Daily*, May 24, 2014. p3.

delivered from PLA cyber hacking troops and coordinating agencies to the SOEs and finally incorporated into certain completed products. If ECE is large-scale, long-term and well-organized, there must be some agencies that arrange such delivery. But none of such units has been revealed till now.

Thirdly, the cyber security companies and intelligence agencies have their own incentives to exaggerate the risks, threats and losses associated with cyber espionage, and may mislead policy-makers. It is likely that the so-called intelligence-complex, which consists of intelligence agencies, related Congressmen and cyber security companies, plays a key role in creating an atmosphere of cyber threats and disclosing China's ECE activities. For example, when President Barack Obama delivered his first policy remarks on cyberspace security in 2009, he said that "last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion."[19] The number is from the *Cyberspace Policy Review* and its original source is a McAfee report.[20] Obama repeated this number of $1 trillion many times later. But in 2013, McAfee and CSIS modified the number to $100 billion and admitted the bug of the calculating method.[21] It causes concern over whether Obama's judgments about and the U.S. policies on cyberspace security have been misled by this severely exaggerated number.

Fourthly, the ideology of seeking adversaries or enemies affects the judgment. The U.S. pursues a policy of containing potential challengers so as to maintain its leadership in the world as well as in cyberspace. According to this logic, China is an emerging power in the Asia Pacific, Iran is a potential threat in the Middle East, and Russia is the current challenger to the U.S. leadership in the European region. The real intent of these countries is not relevant. When these countries gain strength to a certain extent, they will become adversaries of the U.S. It is a new means of containment by criticizing opponents' involvement in ECE.

Fifthly, it is doubtful that undertaking highly complex ECE activities is within China's capabilities for research and development in information technology. China is now a major actor in cyberspace, but far from being a cyber power. In the Mandiant report and DOJ indictments against Chinese military officers, hackers from China

[19] "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

[20] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", May 29, 2009. p2.

[21] James Lewis, 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

used a few basic means of cyber espionage, such as spear phishing attacks, deception emails for passwords, Trojans and other simple means, and the use of Chinese-style English and the variables and comments in the codes of compiled programs can easily be tracked. These hackers are not well-trained, despites of the title of "Chinese top advanced hackers". This demonstrates that China's cyber intrusion technology and capabilities are well below decent international standard.

It is a dilemma for the Chinese government to admit or deny its involvement in ECE activities. The key is its attitude and appropriate countermeasures. Since major cyber countries have not reached a consensus on the norms and rules to regulate ECE activities, the most important thing right now is to reach such consensus rather than make mutual accusations.

2. China as the Victim of Economic Cyber Espionage

ECE has undermined the competitiveness and reduced the profits of attacked enterprises, companies and research institutions. In a broader sense, large-scale and long-term ECE will adversely affect economic prosperity and technical innovations of a country and the world. The U.S. government even claimed that ECE has been threatening its national security.[22] Despite facing many ECE accusations, China is also suffering from ECE. No matter whether such accusations against China are reasonable or not, they have made and will make greater impacts on China in many aspects.

A. Damage to China's International Reputation

ECE accusations against China have tarnished China's international reputation and credibility from two aspects.

On the one hand, China is portrayed as a major threat to cyberspace security and stability. China is the country most frequently blamed for ECE. Although the Chinese government usually rejects any such accusations, China has a negative image with respect to internet freedom due to its domestic internet governance policies of access blocking 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,.

On the other hand, China is described as a thief of intellectual property and trade secrets. The diplomatic position of the Chinese government is to oppose ECE and any

[22] U.S. White House, "National Security Strategy", February 2015. p7.

other kind of cyber attacks since China is also a victim of ECE, and China is willing to cooperate with the international community in dealing with cyber attacks. But no matter whether the Chinese government is really involved in ECE activities, such accusations have enhanced China's image as an actor of cyber espionage. Some countries thus keep precautious when dealing with cyber-related business with China.

On April 3, 2013, I talked with members of a visiting delegation of the U.S. congressional aides about the Mandiant report. All delegation members thought that the report was credible and that unit 61398 was one of the Chinese military elite cyber forces. As to the allegation against the Chinese military for its participation in ECE activities, most of them thought it is reasonable. It shows that China's denials have not alleviated the international concern.

The ECE accusations have weakened China's soft power. The international community began to believe that the Chinese government sponsors or participates in ECE activities, which has undermined the ambition of China to participate in the international agenda and shape international rules. The situation does not live up to China's aspirations to become a responsible participant in the international society.

B. Barriers to Market Access

ECE accusations have adversely affected the outbound investments in overseas markets by Chinese enterprises. Although the Chinese government never admitted ECE accusations, the tensions persist. And the barriers against Chinese companies have moved from intellectual property protection to national security.

Huawei, one of the leading ICT product and service providers in the world, has offices and research facilities in about one hundred countries spanning most of the continents. But in 2012 only 3.7% percent of Huawei's $35 billion annual sales revenue was from the U.S. market. It is well known that Huawei has encountered many barriers, from intellectual property disputes to information security audits, when it tried to enter the U.S. market. In 2001, Huawei officially entered the U.S. market. In 2003, Cisco sued Huawei for software and patent infringement. Although the two entered into a definitive settlement agreement in 2004, many pending contracts were suspended or cancelled. When Huawei tried to purchase the telecommunication businesses of 3Com, 2Wire and Motorola, these transactions were all denied by the U.S. Committee on Foreign Investment in the United States for reasons of national security. In 2012, the U.S. House of Representatives Permanent Select Committee on Intelligence claimed that Huawei and ZTE may be a potential threat to the U.S.

national security interests if they hand a hand in the U.S. telecommunications infrastructure.[23] A common theory is that Huawei has PLA background, and Huawei will help China to steal sensitive and business secrets from the U.S.

Lenovo, now one of the largest personal computer equipment manufactures, also has encountered many obstacles in the U.S. market. When Lenovo was going 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 Congress for investigations. When the deal was completed, some members of the U.S.-China Economic and Security Review Commission continued to express their concern over potential data leaks and national security threats. The U.S. government also has spent a lot of time investigating Lenovo's acquisition of IBM x86 low-end server business sectors in 2013. Although the acquisition was finally completed, much additional time and efforts have been paid by Lenovo.

For China, the expansion of overseas investments is an important part of the successful transformation of the economic structure. Chinese companies need a favorable investment environment, which hinges much on the political atmosphere affecting target countries and China. The ECE accusations against China have largely damaged mutual trust, e.g., between the U.S. and China. Because of their intimate relationship with the government, Chinese SOEs are easily regarded as accomplices of the Chinese government in ECE, especially those that are funded by the government or have a military background. In any case, the ECE accusations greatly affect the potential for Chinese enterprises to participate in international markets.

C. Losses Resulting from Cyber Espionage

China, as officially claimed, has also suffered much from economic and cyber espionage. Some may argue that China is not a leading technological power. It is not worth economic espionage. In recent years, along with China's rising economic capacity and market share in international trade, China has become the potential target of economic espionage. Rapid progress has narrowed the gap between China and the West in the industries of telecommunications, information technology, biotechnology

[23] 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

and aerospace. The popularization of the Internet and the informationization of the economy in China made ECE not only possible but also profitable.

In fact, overseas espionage activities targeting China have been in existence for a long time. Foreign countries mainly want to gain competitive advantages and reap monopoly profits. China's state-owned enterprises, especially large enterprises under direct control of the central government having enormous resources, often become the targets of economic espionage. The usual targets include the national policies, negotiation tactics and procurement reserve price. In the Rio Tinto commercial espionage case, because Australian miners had obtained in advance average gross margins and other key confidential information regarding the Chinese steel industry, China's steel enterprises had to pay more than 700B RMB in excess. Some unique traditional Chinese techniques and industries also suffered much from economic espionage. For example, as Financial Times reported, Japanese enterprises had stolen Chinese technology and craftsmanship of Cloisonne and Xuan paper.

China suffers numerous overseas cyber attacks everyday, among which the U.S. IP based attacks are on the top of the list. Cai Mingzhao, former Minister of State Council Information Office of China, delivered a keynote speech at the Fourth World Cyberspace Cooperation Summit on November 5, 2013. Cai pointed out that China faces serious cyber threats. "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."[24]

D. Potential for Science and Technology Undermined

Insufficiency in intellectual property protection resulted in the weakness of related industries and fields. With the rapid development of the Chinese economy and escalation of the industrial structure, extraordinary progress has been made in the high-tech industry. After China joined the WTO in 2001, the protection of intellectual property has become an important means for the improvement of the investment environment and market environment.

[24] Cai Mingzhao, "Keynote speech at the Fourth World Cyberspace Cooperation Summit", November 5, 2013. http://siepr.stanford.edu/cyberspace.cooperation.summit. http://transpacifica.net/2013/11/full-text-speech-by-minister-cai-mingzhao-at-cybersummit2013-nov-5-2013/

Failure to protect intellectual property will hinder industrial development. A good example is the development of personal computer operating system with self-owned intellectual property in China (it is mainly due to piracy rather than espionage, but the case well indicates the importance of intellectual property protection for the sustainable economic development and technological innovations). The Chinese government has allocated large budgets for the research and development of operating systems since the 1990s. Many companies and research institutions have developed dozens of different types of operating systems. But when the users can effortlessly get the Windows operating system without having to pay for it, domestic operating system manufacturers have lost their competitiveness obviously. Software piracy thus not only considerably reduces the profits Microsoft should have reaped but also hinders the development of the software industry.

ECE will produce similar results. Some argue that China can develop independent research and development capabilities as a long-term strategy and obtain secrets and know-how through ECE to satisfy short-term needs only. But when an opportunistic development model comes into being under which opportunists are encouraged, a legitimate and innovative culture will soon be damaged.

Intellectual property protection and scientific innovations are complementary and inseparable. Only those industries and fields boosted by independent innovations can go further. Without adequate and effective intellectual property protection and outright opposition to ECE, China's ambitions with respect to scientific and technological innovations will remain empty talk and China's core competitiveness will be difficult to improve. China has benefited much from the global markets and shared rules of WTO, and will benefit more if similar rules can be formulated at home for conduct and behaviors in cyberspace.

3. China’s Alternative Roles in Controlling Economic Cyber Espionage

The fast growth of cyberspace and its deep integration with the economy and society have fundamentally changed the nature of the world. China has also benefited greatly from the development and popularization of the Internet. It is clear that the spread of ECE has posed a potential threat to China's economic development and technological innovations. This section will analyze China’s willingness and responsibility to play a positive role in controlling ECE.

A. Necessity of China’s Participation

Accusations alone make no contribution to the elimination and control of ECE. Along with the U.S. accusations against China for ECE, China has also made accusations against the U.S. for its aggressive cyber strategy, especially the NSA intelligence program of surveillance and invasion of the global telecommunications system and the Internet. Mutual accusations have diminished the moral standing of both sides and undermined the cooperation in the control of ECE.

Overstating cyber threats from China will deepen the distrust between the U.S. and China. Presuming that China poses serious cyber threats and compromises U.S. national security, the U.S. policy is to contain or combat China in or through cyberspace. And when China believes that its military's capabilities do not match its ambitions, it will improve its offensive cyber weapons. The situation will become worse if the disputes and conflicts between the U.S. and China continue, for both countries have real or potential capabilities for mutual disruption and destruction in cyberspace.

It is important for the control of ECE to locate the sources of suspicious cyber activities, but it is impossible to identify the attackers without cooperation among the countries pertaining to the victims, the conduct, and the attacking routes. When an ECE case is revealed and accusations are made against one government, the possible response would be to use sovereignty as an excuse, obstructing further investigations. The political willingness, rather than technical means or legal clause, would be the basis to determine who should be responsible for ECE.

The U.S. and China should work together to formulate norms and rules and take consistent actions. China is one of the major nation-state cyber actors. What should be done is to promote mutual understanding of the common interests of China and the U.S., delegate shared responsibility and create a common mission to promote the security and the development of cyberspace. As the two largest countries in the cyberspace, the potential for cooperation between the U.S. and China takes priority over the contradictions and conflicts between the two countries. It is an important basis for the global governance of cyberspace if China and the U.S. can reach consensus on the principles of security and code of conduct in cyberspace. U.S. DOJ indictments against Chinese military officers caused the suspension of U.S.-China cyber working group activities, and it is difficult for either side to make substantial concessions. Nevertheless, the U.S. and China can utilize bilateral cooperation dialogue mechanisms among government departments and professional organizations to expand the areas of cooperation, such as judicial assistance, counterterrorism and

technical information sharing.

B. Feasibility of China's Positive Role

First, China has the willingness to take greater responsibility in international relations as well as in cyberspace. As a rising economic and political major power, China is going to act more positively in the world. China's central government expects to broaden the agenda for China's diplomatic strategy under new conditions. "We should manage well relations with other major countries and build a sound and stable framework of major-country relations."[25]

Chinese policy-makers will realize that ECE will become a problem for China's economic development and technology innovations, and that China should cooperate with other countries to solve this global public issue. Therefore, international responsibility entails all the countries following the same rules in addition to taking responsibility for their actions.

Secondly, the Chinese government officially states that China is a victim of cyber espionage and opposes any form of cyber espionage. Then the question is how the Chinese government would translate its diplomatic position into national laws and policies as well as international commitment. Theoretically, ECE is illegal in China. China's laws and regulations forbid any form of cyber attacks and cyber espionage, regardless of its origin or target. Although China's Counterespionage Law allows national security agencies to take technical reconnaissance measures,[26] which means some Chinese governmental agencies can perform hacking and espionage activities, but the scope of and the authority for such activities are very strictly limited for the sole purpose of countering espionage. The current proposed National Security Law of China provides measures for preventing and punishing cyber attacks, cyber theft and illegal spread of harmful information. [27]Therefore, ECE is illegal in China, which shows that there is no fundamental barrier to bringing China's rules into line with international rules.

Thirdly, China's fast-growing capabilities in cyberspace give it not only interests but also responsibility and influence to be a positive partner, participant and supporter. With the largest number of Internet users and as the biggest e-commerce market and a

---

[25] "China eyes more enabling intl environment for peaceful development", http://africa.chinadaily.com.cn/china/2014-11/30/content_18998582.htm

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

[27] "National Security Law (draft)", May 6, 2015, http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-05/06/content_1935766.htm

major manufacturing base of IT products, China is now one of the major players and important stakeholders in cyberspace.

Fourthly, China's centralized power structure and efficient decision-making and implementation mechanisms contribute to the control of ECE activities. Once the central government recognizes that the long-term damage by its involvement in ECE on its reputation, economy and innovations would offset short-term gains, it can quickly prohibit all levels of government departments from participating in ECE activities and mobilize necessary resources with strong determination to combat non-governmental actors engaged in ECE crimes. In addition, China has established effective technological, administrative and legal mechanisms for tracking almost all domestic activities in cyberspace, which is useful for operations of tracing behaviors, collecting evidence and controlling ECE. The issue of bureaucratic and group interests associated with ECE, if present, can be well resolved.

C. Approaches for China as a Stakeholder

It is unfair to ignore China's responsibility for and interests in controlling ECE. The constructive approach is to incorporate China into international mechanisms and encourage China to play as a stakeholder.

First, the control of ECE activities should be placed under an intergovernmental cooperation regime. ECE is the result of interactions between the cyberspace and the real space. As a principle, China insists that the security and development of cyberspace is a domestic issue and sovereignty should be exercised over cyberspace control. The positions of the U.S. and other Western countries in this respect are not so clear. According to Christopher Painter, a coordinator for cyber issues, sovereignty over cyberspace should be divided into two categories. The content of the Internet is not subject to sovereignty.[28] But there is no doubt that ECE control hinges on cooperation among relevant governments.

Secondly, the cooperation between the U.S. and China should be a starting point of controlling ECE. Till now, the most bitter quarrels and conflicts occurred between these two countries. The U.S. should not expect to develop a set of rules unilaterally and compel China's compliance. And it will lead to an unpleasant future for the cyberspace if the U.S. and its allies and partners develop one set of rules while China, Russia and other countries develop another, which would undermine the unity and

[28] Christopher M. E. Painter, Testimony Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy Hearing Titled: "Cybersecurity: Setting the Rules for Responsible Global Behavior", May 14, 2015.

connectivity of the Internet and divide the world into two confrontational groups in cyberspace.

The U.S. government should attach less importance to the ECE issue in U.S.-China relations, or treating it as a transnational crime issue rather than a national security one. For China, national security is a sensitive issue. In recent years, the U.S. government has been associating the ECE issue with national security threats. In recent strategic documents, such as National Security Strategy, National Intelligence Strategy, National Defense Strategy Report and the International Strategy for Cyberspace, the ECE issue has been highlighted. But for China, ECE has not become a national security problem and out of strategic consideration. Taking ECE as a national security issue rather than merely a legal one reduces the possibility of international cooperation. China used to reject any unacceptable outside pressures and believes that the unstated goal of accusations by the U.S. against China is to achieve its hegemony in cyberspace. China increasingly seeks an equal footing with the U.S. in bilateral relations. That is why China denounced the indictments against Chinese military officers as violation of basic norms of international relations. "This move grossly violates the basic norms governing international relations and jeopardizes U.S.-China cooperation and mutual trust".[29] China's Ministry of Justice and the United States signed the "Agreement on Mutual Legal Assistance in Criminal Matters" in 2000.[30] There is no indication that the two governments have tried to solve ECE disputes through this bilateral judicial consultation and cooperation mechanism.

Thirdly, some major cyber countries should achieve consensus on what cyber espionage is acceptable and what is not and how to regulate acts of countries in cyberspace. Those major cyber players include U.S., China, EU, Russia and Iran. But till now the consensus and agreement among those major cyber countries are rare. In April 2015, China's Ministry of Public Security and U.S. Department of Homeland Security achieved a consensus that greater cooperation is needed on cyber-enabled crimes.[31] In May 2015, Russia and China signed an intergovernmental agreement on

[29] "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference", May 20, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1157859.shtml

[30] "Agreement between the Government of the United States of America and the Government of the People's Republic of China on Mutual Legal Assistance in Criminal Matters", June 19, 2000, http://www.state.gov/documents/organization/126977.pdf

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

cooperation in ensuring international information security, in which Russia and China agree not to launch cyber-attacks against each other, as well as jointly counteract technology that may "destabilize the internal political and socio-economic atmosphere, disturb public order or interfere with the internal affairs of the state".[32] The commitment not to hack each other between major cyber countries is a great breakthrough and has similar great significance to the commitment no to use nuclear weapons first under any circumstances. In a word, Russia and China has created and practiced a valuable model of building up trust and reducing hostility in cyberspace. These interactions among major players in cyberspace will help to encourage cooperation.

Fourthly, a multilateral inter-governmental platform should be created as a rulemaking and dispute-resolving mechanism. The international society should jointly work to put the cyberspace security issues on the United Nations security cooperation agenda, or to consider the creation of a common network of international multilateral security coordination mechanisms. An international inspection and attribution mechanism is an option for the ECE issue. The Attribution and investigation of cyber espionage activities involve complex factors in technology, law, sovereignty and jurisdiction. As a successful intergovernmental and professional institute for nuclear arms control, the International Atomic Energy Agency (IAEA) may provide experience and reference.

The Chinese government advocates a new model of major-country relations between the U.S. and China. This new model is aimed at breaking the historical pattern of confrontation and conflicts between an emerging power and an established power. The change of interests and the shift in power balance were invariably accompanied by conflicts, culminating in the reconstruction of the power structure by wars. Cyberspace is an important foundation for global economic and social in the information age. Whether it can avoid the historical pattern of being a field for great powers to compete for the control of core resources, and instead become a peaceful new space for cooperation, will serves as a touchstone of whether the new model of major-country relations can resolve broader issues of international peace and development.

---

and-chinas

[32] "Signing a Russian-Chinese intergovernmental agreement on cooperation in ensuring international information security", May 6, 2015, http://government.ru/en/docs/17952/

Conclusion

Espionage is a widely used foreign policy instrument and espionage issues have been in the gray area in international relations for a long time. Cyber espionage, as an emerging intelligence activity, has attracted more and more attention in recent years. The differences among economic cyber espionage, security cyber espionage, and open collecting of economic information in cyberspace are not so obvious and the boundaries are not clear-cut, so shared understanding, common interests and coincident rules are very important for resolving this problem.

The international governance of cyberspace is at low level and is in the process of institutionalization. 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".[33] It provides a basic judgment from the perspective of international regime theory, and cyberspace is exactly such a globally shared space with diversified stakeholders and highly asymmetrical distribution of power. The establishment of the regime in cyberspace depends on equal power distribution and the interactions of major cyber players. Therefore the balance of power and the convergence of interests between the U.S. and China may provide favorable conditions for better governance of ECE.

ECE would be a real threat to the prosperity, peace and security of cyberspace and the real world if it remains unregulated. Since ECE is a global problem, we should draw on the ideas and approaches for the international governance of other global public spaces, such as the aerospace and international waters. Historically, the governance of global public space is based on the consensus of major powers and the participation of various stakeholders. The creation of the norms and rules for cyberspace also need major countries to reach a consensus on the basic principles, such as the sovereign jurisdiction, the innocent passage, the freedom express and so on. The U.S. should not expect other major countries to acknowledge that the U.S. has the right to freely access and monitor others' communication networks and the Internet in the name of anti-terrorism and at the same time prohibit, in the name of ECE control, other countries from engaging in similar activities. And China, with its increasing interests, capabilities, dependence and vulnerability with respect to cyberspace, will also be involved in the process of common governance, playing a

[33] Stephen D. Krasner, "Global Communications and National Power: Life on the Pareto Frontier," *World Politics*, Vol. 43 Issue 3, April 1991. p337.

more positive role. China is one of the major players in cyberspace, with its own unique preference as well as common interests shared with the international community. China's role will exert an important impact on the future of cyberspace, as well as the prospect of ECE control.