

## **Towards a Common Security Platform for Sino-US Cyber Relations**

**Dr. Panayotis A. Yannakogeorgos**

### **Introduction**

Cyberspace, and its sub component, the Internet is the 21<sup>st</sup> century's powder keg. Competing interests and ideologies have emerged over the past decade to carve out digital spheres of influence within a domain that was supposed to represent the epitome of a project forging a global Information Society. Today the domain is dominated by cyber criminals, terrorists, and other malicious actors who take advantage of a lack of international cyber cooperation and strain relations between great powers. Instead of focusing on ways to enhance cooperation, states are competing on ideological grounds to define what the norms of cooperative behavior should be.

The Internet is not a luxury. It is a critical tool that when unrestricted allows information to flow freely across the globe, opening the door to economic development, knowledge exchanges, and innovation. American technological innovation in the development and maintenance of the Internet's backbone is unquestioned. However, American "leadership" as first among equals on cyber norms has led to a succession of dead ends with the US dictating the terms of global cybersecurity norms. Ironically – to use some of the jargon of the social sciences – an inability to generate a suitable global norm has only enhanced insecurity for all actors, as has the failure to agree over how to protect a non-excludable global public good. This has therefore, led to a negative-sum outcome.

Cyber crime and espionage will continue its upward trend. As more and more people gain access to advanced ICT and enter the digital Information Society, the consequences of how states direct and respond to malicious cyber incidents targeting both business systems and critical infrastructure are unclear.

There is more to fear from confusion than from disagreement. My objective here is to help provide some clarity to the discussion that may lead to Sino-US cyber relations of mutually assure security. I myself cannot do what most needs to be done, which is to state the solution. Yet, I hope to state the problems before us, recognize the nature of the problem, and provide some proposals that can be judged. This is more than half the battle for our nations to have the benefit of cyber power. But neither China nor the US can share these benefits in a world in which cyberwar may come.

### **A Brief History of Sino-US Cooperation in Cyberspace**

#### **The "OX" Meeting**

One of the reasons that overall prospects for US-China cooperation are positive ties directly to the increasingly intimate economic and financial relationship in which China holds more than \$1 trillion of American sovereign debt—helping to fill the shelves of Wal-Mart and Target while

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

employing millions of Chinese.<sup>1</sup> Without diving into the balance sheets, it is important to keep this context in mind as we explore the political statements of leaders.

When President Obama and President Xi met in California June 7-8, 2013 to discuss, among other issues, cyber conflict. Both leaders expressed a desire for closer cooperation. President Xi stated: “We need to pay close attention to this issue and study ways to effectively resolve this issue. And this matter can actually be an area for China and the United States to work together with each other in a pragmatic way.”<sup>2</sup> President Obama acknowledged that: “When it comes to those cybersecurity issues like hacking or theft, those are not issues that are unique to the U.S.-China relationship. Those are issues that are of international concern. Oftentimes it’s non-state actors who are engaging in these issues as well. And we’re going to have to work very hard to build a system of defenses and protections, both in the private sector and in the public sector, even as we negotiate with other countries around setting up common rules of the road.”

Given their leadership in both developing technology, number of users, and great power status, the Obama-Xi, or OX, duo will have pull the world cart and lead by example to begin resolving the greatest security dilemma of the early 21<sup>st</sup> century. The opportunity for China and the US to make marked progress toward cyber-cooperation will be evident in the months and years to come. Presidents Obama and Xi have already agreed to create a high level working group to address cyber issues. Examples of greater cyber-cooperation should take the form of a reduction in attempted intrusions targeting intellectual property. Improved and timely sharing of information between China and US computer emergency response teams along with enhanced law enforcement activities would also serve as a clear indicator of increased cooperation.

### ***Building Towards the Current Cooperative Spirit***

The current optimistic atmosphere of Sino-US cooperation is not new. Gen Joseph Ralston, USAF (ret), former vice-chairman of the Joint Chiefs of Staff, makes a compelling case for the long-term benefits of building trust with China through military-to-military contacts. A similar argument can be constructed for building trust with China regarding the areas of computer security and critical infrastructure protection.<sup>3</sup> Vice Adm Mike McConnell, USN (ret) suggests Sino-US cooperation would help “clean up” malevolent cyber activity and minimize hostile intrusions and disruptions caused by hacking and cyber-crime.<sup>4</sup>

The visit of US Deputy Secretary of State James Steinberg to Beijing in 2010 signaled a bilateral thaw after a series of intensifying controversies over US weapons transfers to Taiwan; UN sanctions on Iran; and Internet freedom—heightened by the Google flap.

---

<sup>1</sup> Stephen Cohen and J. Bradford DeLong, *The End of Influence: What Happens When Other Countries Have the Money* (New York: Basic Books, 2010). Also see Niall Ferguson, “Complexity and Collapse: Empires on the Edge of Chaos,” *Foreign Affairs*, March 2010.

<sup>2</sup> Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting: <http://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china>

<sup>3</sup> Joseph W. Ralston, “Why the Pentagon Needs Friends in Beijing,” *Wall Street Journal*, 5 March 2010.

<sup>4</sup> James Fallows, “Cyber Warriors,” *Atlantic*, March 2010, 58–63. Also see “Mike McConnell on How to Win the Cyber-War We’re Losing,” *Washington Post*, 28 February 2010, B01.

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

The April 2013 visit of Secretary of State John Kerry to Beijing was an early sign of what was hoped would be a bilateral thaw after a series of intensifying disagreements surrounding: US weapons transfers to Taiwan, UN sanctions on Iran, , and the United States' Internet freedom agenda.<sup>5</sup> Kerry's visit was less successful than desired as it has done did little to slow China's cyber espionage efforts, lending credence to Brad DeLong's suggestion that the balance of influence in China-US relations has changed dramatically due to fundamental economic factors. Clearly, there will be fluctuations in this bilateral relationship—with the most recent “downs” linked to continued Chinese support for pervasive PLA sponsored industrial espionage, and China's growing assertiveness in the South China Sea.<sup>6</sup>

Additionally, several track-two diplomatic initiatives have been undertaken by the East-West Institute to build trust, and more recently in this past June track .5 began. This later meeting is the outcome of an April 2013, announcement by US Secretary of State John Kerry, while in Beijing, to launch a formal initiative to begin building a foundation for cooperation between the US and PRC. In his statement, Secretary Kerry said:

We will create an immediate working group because cyber security affects everybody. It affects airplanes in the sky, trains on their tracks. It affects the flow of water through dams. It affects transportation networks, power plants. It affects the financial sector, banks, and financial transactions. Every aspect of nations in modern times are affected by use of cyber networking, and obviously all of us, every nation, has an interest in protecting its people, protecting its rights, protecting its infrastructure. And so we are going to work immediately on an accelerated basis on cyber.<sup>7</sup>

If the US and Chinese leadership's public statements are sincere, this is a positive step in the US-China relationship in cyberspace.

### ***Beyond the Rhetoric***

While the words of politicians are good, we can also see a positive increase in the real cooperation between US and Chinese law enforcement authorities to tackle cybercrime. Chinese authorities criminalize malicious hacking—putting culprits in jail if they are found guilty of creating damage through illegal actions involving intrusions in computer systems and networks—and China's law enforcement services have cooperated with their American counterparts.<sup>8</sup> In a recent case, this was in the combating of Chinese language websites hosting Child pornography where the Federal Bureau of Investigation and Chinese Ministry of Public

---

<sup>5</sup> Hillary Rodham Clinton, “Internet Freedom” (Prepared Remarks, Newseum, Washington, DC, 21 January 2010). John Pomfret, “China Suspends U.S. Military Exchanges in Wake of Taiwan Arms Deal,” *Washington Post* (29 January 2010), [http://articles.washingtonpost.com/2010-01-29/world/36893526\\_1\\_china-s-defense-ministry-chinese-energy-companies-china-over-internet-censorship](http://articles.washingtonpost.com/2010-01-29/world/36893526_1_china-s-defense-ministry-chinese-energy-companies-china-over-internet-censorship).

<sup>6</sup> See Richard Rosecrance and Gu Guoliang, *Power and Restraint: A Shared Vision for the U.S.-China Relationship* (New York: Public Affairs, 2009).

<sup>7</sup> John Kerry, Solo Press Availability in Beijing, China <http://www.state.gov/secretary/remarks/2013/04/207469.htm>

<sup>8</sup> James Areddy, “People's Republic of Hacking,” *Wall Street Journal*, 20 February 2010, p. A1, which describes the 3-year imprisonment of a convicted Chinese hacker.

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

Security cooperated and provided each other assistance.<sup>9</sup> This continues a spirit of limited cooperation in criminal cases in recent years. Recall the 2010 Congressional testimony by Larry Wortzel, a member of the US-China Economic and Security Review Commission, also makes clear that cooperation in cyberspace is possible, as evidenced by supportive activities for specific law enforcement purposes “...in some areas of cyber crime, such as credit card theft rings and the theft of banking information, China’s law enforcement services have cooperated with the United States.”<sup>10</sup> This common history of dealing with cybercrime may help increase strategic trust and paves the way for serious US-China discussions (and ultimately formal bilateral negotiations) on approaches for building a strong code of conduct dealing with criminality, national security and military operations in cyberspace. Common ground exists for bilateral discussions and ultimately negotiations about US-China cooperation on cyber security.

Overall, US-China cooperation in cybersecurity needs to encompass both military and non-military aspects of cyberspace. An informed focus on the military sector is just as important as focus on its non-military counterpart in this field of interest.

### **The Quest for Mutual Cybersecurity**

Now, I feel it my obligation to say something about individual proposal which might lead to building confidence and allowing the two great powers to move towards a mutually assured security (MAS) relationship in cyberspace. I will offer three proposals that I think should be the first steps in what will be a long march of the two great powers to lead the world and create formal international treaties.

#### **Proposal One: Develop a Common Lexicon for Malicious Actions in Cyberspace**

Participants in debates about air, land, sea, and space power all know what they mean by armed attack. Definitions and a common lexicon are the basis of all these debates and while none of these domains have settled on a singular definition, what little argument that takes place about definitions usually revolves around two or three assertions that more-or-less mean the same thing. The United States, its allies, and other nations around the world invest vast sums into cyberspace, a domain that is identified not only as a critical national infrastructure with myriad vulnerabilities, but also a warfighting domain that is increasingly critical to Air Force and sister service operations and capabilities. My purpose here is to encourage a formal debate to forge common cyberspace terms, definitions, that will eventually lead to more coherent domestic and international cyber policy, strategy, and doctrine. This is not a topic of mere academic semantics. In 1911 the British maritime theorist Sir Julian Corbett wrote about the importance of definitions thus: “Without such an apparatus no two men can even think on the same line; much less can

---

<sup>9</sup> <http://www.justice.gov/usao/nys/pressreleases/May13/WangYongPleaPR/Wang,%20Yong%20Indictment.pdf>

<sup>10</sup> Larry M. Wortzel, “China’s Approach to Cyber Operations: Implications for the United States,” Testimony to the Committee on Foreign Affairs, U.S. House of Representatives, 10 March 2010.

they ever hope to detach the real point of difference that divides them and isolate it for quiet resolution.”<sup>11</sup>

### ***Critical Infrastructure***

In popular discourse, policy debates, and doctrine, people tend to conflate the terms “cyberspace” with the “Internet,” and “cyber attack” with “cyber exploitation” or “denial of service disruption” This is, in part, due to a conflation of information and communication technologies (ICT) that are used daily by people globally with the industrial control systems (ICS) upon which the operations of a nation’s critical infrastructure depends. Societies rely on these systems to deliver utilities and other services on which life in the twenty-first century depends. A recent executive order issued by President Obama takes a necessary step toward distinguishing between ICT and ICS systems, but confusion still remains. Let me offer some further clarification.<sup>12</sup>

Cyberspace includes both open-multifunction networks like the Internet, and closed-fixed-function networks like industrial or building control systems. The functioning of open networks is defined by the number of users on them. The two types of networks are fundamentally different. On the one hand, open multifunction networks have greater utility as the number of users increases. This is the principle of network utility maximization, that is: users tend to join if they trust an open network, and believe their privacy is protected. On the other hand closed fixed-function networks must assure that information travelling from sensors to operators is available, trusted and authenticated. The focus of ICS is on availability defined by the ability of the system to provide control to operators of machine processes in critical infrastructures and key resources.

By their nature, ICS were not designed with security in mind, and as Stuxnet and other recent events show, they are military targets. Should ICS processes fail, equipment damage, physical destruction, and possibly loss of life will occur. Indeed, several incidents have already taken place where widespread destruction was the result of poor system design. One such example is the 2009 Sayano-Shushenskaya hydroelectric dam explosion. This disaster caused by a computer misconfiguration that resulted in a massive explosion and environmental damage, is indicative of plausible destruction that could be caused by a cyber attack.<sup>13</sup> A cyber attack against such systems may utilize the Internet if an inattentive system administrator has not properly isolated the system. However, the specialized communications protocols, software, equipment configurations, and standards on which these systems operate require a much higher skill set to successfully attack. A threat to power generators is real, due to the Aurora vulnerability. During a DHS exercise, hackers succeeding in gaining remote access to a generator’s SCADA control system and were able to physically destroy it—lending support for the need to distinguish between cybercrime/espionage and cyber warfare. Many ICS vulnerabilities are hard-coded into

---

<sup>11</sup> Julian S. Corbett, *Some Principles of Maritime Strategy*, with (Annapolis, MD: Naval Institute Press, 1988; first published in 1911), p. 7.

<sup>12</sup> Executive Order -- Improving Critical Infrastructure Cybersecurity : <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

<sup>13</sup> "Insulating oil spreads along Siberian river after hydro disaster". RIA Novosti. 18 August 2009. <http://en.rian.ru/russia/20090818/155846126.html>.

the programmable logic controllers (PLCs) and Remote Terminal Units (RTUs) and other components of an ICS, making patching more difficult than in business systems.

### ***Define Cyber Armed Attacks and Cyberweapons***

Existing international legal frameworks provide clarity on how law and policy should treat instances of cyber warfare. The *Tallinn Manual on the International Law Applicable to Cyber Warfare*, perhaps the most comprehensive work on the issue today, offers the definition of a cyber attack as a “cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”<sup>14</sup>

Cyber events breaching the threshold of armed attack require the use of cyberweapons, which differ substantially from espionage or crime tools such as Flame, Zeus, Gauss or other malicious code. While a cyberweapon can be software code designed to attack ICS, it can also be hardware flaws introduced into critical systems. Due to the complexity of ICS, the skill level required to discover vulnerabilities (so-called zero day vulnerabilities), as well as the infrastructure required to find targets, gain access, and execute the attack requires significant financial and human capital. To date, only Stuxnet has risen to the level of a cyber incident that could be considered an armed attack under international law as it caused the physical destruction of objects. One could argue for the Shamoon virus impacting the oil sector is a close second as it destroyed virtual records, which were restored without widespread destruction or physical injury. However, the impact of Shamoon was on the business applications of cyberspace, and not the ICS systems that could cause national security concerns.

One could argue that software or hardware designed to gain elicited access to a system could, at the flip of a switch, cause destruction, which is what makes cyber warfare “different.” This oft cited claim is groundless. Access software, such as Flame or Duqu, might serve the same function as a laser guiding a weapon to the final target. However, a targeting laser is only part of a weapons system. A missile’s payload is the actual object in the weapon system creating destructive effects. Similarly, in the case of a cyberweapons, operators may use previous access to guide a weapon towards a designated target. However, a separate package will have to be developed to exploit vulnerabilities and cause physical effects resulting in death or destruction.

One might further argue that the package could be contained within the set of tools conducting reconnaissance, hence the “cyber attack at a flip of a switch” arguments. However, given the unique characteristics of an ICS, a cyberweapon could not create an effect without being tailor made for a specific target’s digital and physical environment. In short, this requires ICS schematics, network maps, teams of coders, cryptographers, and a virtual environment replicating the target on which to test the effects of the weapon before deployment. To argue otherwise is akin to making a claim that a SEAL commander would turn a reconnaissance mission on its first foray into tracking Bin Laden into an all out assault against the complex in Abbottabad, and expect a high-likelihood of success. Both instances require diligent preparation prior to execution.

### ***Threats to Peace and Acts of Aggression***

---

<sup>14</sup> *The Tallinn Manual on the International Law Applicable to Cyber Warfare*: <http://www.ccdcoe.org/249.html>

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

Below the threshold of cyber attack are incidents and events that, while malicious and disruptive, are aggressive but do not rise to the level of attack. The oft cited cases of Distributed Denial of Service (DDOS) disruptions are an example of cyber crime, not cyber warfare. The theft of US intellectual property by Chinese hackers is an example of cyber espionage or theft.<sup>15</sup> While instances of cyber espionage may have long term negative consequences for national security, the act of stealing the data itself is not an armed attack.

Despite private-sector arguments to the contrary, industrial espionage is not an act of war and would not require a Title 10 response by the government. Instead, a crime has occurred that may have been prevented with better information security. Federal reform to laws such as the Computer Fraud and Abuse Act would allow the private sector firms to protect themselves by actively responding to thefts of data—to include destroying what was stolen.

The Department of Defense Dictionary of Military and Related Terms defines non-lethal weapons as “A weapon that is explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment.” Distributed Denial of Service disruptions, manipulating data in logistics networks, and other software or hardware incidents would fall into this category.

The kinds of methods that were used in Estonia and Georgia, and the US financial sector in late 2012, certainly did not rise to the level of an armed attack. These disruptions, however, were targeting the network layer of the Internet. This is not true of all denial of service events. So-called “SNMP overloads” are an example of non-network overload DOS attacks. For example, computers running Windows 2000 to program PLCs on an ICS network could be targeted by malicious code that exploited an unpatched vulnerability, causing an “SNMP overload.” In this case, a computer’s memory, not the network connection, would fail.

By exploiting this vulnerability, a malicious actor would cause a hiccup in the system which would prevent *any* new processes to start on a target machine. The machine would have to be powered down, and restarted in order for it to operate again. In critical infrastructure, availability of system is essential otherwise incidents of national security concern could ensue. Thus, denial of service attacks are more than just attacks targeting the network layer leaving websites inaccessible, but also the application layer of specific targeted computers that could cause a power plant to shut down.

The conclusion seems straightforward. Discussions of cyber crime and cyber espionage must be clearly separated from discussions of cyber warfare. By continuing to employ these terms interchangeably the current discussion is drifting from issues of information system protection to issues of national security that warrant a military response. The paradigm required to address cyber crime and cyber espionage is not the same as that required to succeed in cyber warfare. Developing a clear distinction between various types of malicious cyber activity is critical as the Sino-US cyber relationship matures to protect valuable information and critical infrastructure alike. The time for gross generalizations and sweeping assertions is at an end.

---

<sup>15</sup>Mandiant Report: <http://intelreport.mandiant.com/>

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

Although the United States has been the technological pioneer in cyberspace, China is proving itself to be a pioneer in strategic thinking. One Chinese military theorist has stated that “in confrontations on the future battlefield, what is scarier than inferior technology is inferior thinking.”<sup>16</sup> On the other hand, the US has focused on using technology to resolve issues without strategically thinking through the dilemma to make sure the technology is the right fit for the problem at hand.<sup>17</sup> Thus, China’s approach to cyber espionage is proving highly effective.

## **Proposal Two: US Should Cease the Internet Freedom Agenda**

US policy to date has focused on freedom of speech on the Internet as a main policy priority for our international engagement. Given inconsistencies within the US on the topic, and the friction it causes in global cybersecurity dialogues, continuing to focus on international Internet freedom as will only inhibit the building of trust within the international community. American attempts to lead the “Internet Freedom Agenda” have resulted in everyone being worse off. Creating the Internet, and policing it, are two very different problems.

While freedom of speech is a core American value, it is a narrative when placed in the context of the Arab Spring that shakes governments from the European Union to China.

Instead of Internet freedom of speech for the sake of free speech, the world should recognize the economic benefits of a free, open and stable Internet.

Internet prosperity may be a better narrative than the current emphasis on freedom of speech. Such an approach would need to be more mindful of the economic benefits that many be lost in debates focusing on the right to express oneself online.

Furthermore, American involvement in *openly* promoting and organizing “digital activists” in the fight for free flows of information as a human rights issue generates international friction that is counterproductive to the promotion of international cooperation on cybersecurity issues. Illustrative of this is the “Internet Freedom Agenda.” The Department of State openly distributes “activist” software designed to circumvent cybersecurity measures within authoritarian regimes. Such technology effectively allows citizen-activists to hack past government digital sentries to spread forbidden information. To officials in Russia, China, and other non-democratic countries, these activities have been declared as tantamount to spearheading digitized regime change. From their perspective, the US is aiding and abetting criminal activity. This does not contribute to US efforts to secure cyberspace.

Because of the focus on the Internet freedom narrative, we are not finding willing partners in countries where the misuse of information technology—to steal our data, corrupt our computers and potentially worse—is prevalent. For many countries, the content the Department of State is

---

<sup>16</sup> Timothy Thomas, *The Dragons Quantum Leap*, (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 238.

<sup>17</sup> US history is replete with examples. World War II was won on technological superiority, not better strategy. When US-German forces were on parity earlier in the war, the Germans would typically win. The invasion of Iraq is a more recent example. Entering the war with the wrong strategy, the situation on the ground did not improve until strategy caught up with technology, and the “surge” was implemented. *Ibid*, 13-33.

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

enabling to spread is just as dangerous from their perspective as malicious code or intellectual property theft is to the US.

What governments around the world need to understand is that free flowing information will have a direct positive impact on their nation's prosperity if the Internet is allowed to function as it does today. This American invention was shared with the rest of the world, and today serves as the foundation of an inclusive information society that enables socio-economic development globally. These benefits can only continue if the Internet allows for free information flows within the limits of legitimate sovereign national security concerns.

### **Three: Chinese State Owned Corporations Should Increase Transparency to Curtail US Suspicion**

China is making a great leap forward in terms of computer science and engineering. As reported by the US-China Economic and Security Review Commission, "If current trends continue, China (combined with proxy interests) will effectively become the principal market driver in many sectors, including telecom, on the basis of consumption, production, and innovation."<sup>18</sup> US policymakers worry reliance on China as a manufacturer of computer chips and other information and communications technology (ICT) hardware has allowed viruses and backdoors in equipment used by US-based entities, including the military. Extraordinarily low-priced Chinese-made computer hardware is a lucrative buy in Asia and the developing world.<sup>19</sup> Furthermore, Chinese entities, such as Huawei, are on the leading edge of developing the standards of next-generation mobile 4G LTE networks.<sup>20</sup> Indeed, Changhsa is the home of the both the fastest supercomputer in the world, Tianhe-2 and the Chinese designed open source software Kylin Linux operating system.<sup>21</sup> While US-based entities have traditionally set the standards for Internet technology, China-based entities, such as the ZTE Corporation, are increasingly taking on roles within the ITU to draft important international standards that will shape the world's next-generation networks.

China of course has a right to compete in the global marketplace for its share of the information technology sector. What decreases trust are unfortunate accidents such as the April 8, 2010 traffic misrouting affecting US government and military networks when: "China Telecom's servers erroneously started advertising themselves as the best routes for a large chunk of Internet traffic. Such rerouting has happened before from simple configuration errors, though it can certainly be caused by deliberate actions as well."<sup>22</sup> Incidents such as this, and the lack of public

---

<sup>18</sup>. *The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector*, U.S.-China Economic and Security Review Commission Staff Report, January 2011, 7, [http://www.uscc.gov/RFP/2011/FINALREPORT\\_TheNationalSecurityImplicationsOfInvestmentsandProductsFromThePRCintheTelecommunicationsSector.pdf](http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsOfInvestmentsandProductsFromThePRCintheTelecommunicationsSector.pdf).

<sup>19</sup>. LCDR A. Anand, "Threats to India's Information Environment," in *Information Technology: The Future Warfare Weapon* (New Delhi: Ocean Books Pvt. Ltd., 2000), 56-62.

<sup>20</sup>. "Huawei Conducts World's First Commercial Network LTE Category 4 Trial," *Cellular News*, 9 May 2012, <http://www.cellular-news.com/story/54329.php>.

<sup>21</sup> China to create home-grown operating system <http://www.bbc.co.uk/news/technology-21895723>

<sup>22</sup>

[http://www.computerworld.com/s/article/9197019/Update\\_Report\\_sounds\\_alarm\\_on\\_China\\_s\\_rerouting\\_of\\_U.S.\\_Internet\\_traffic](http://www.computerworld.com/s/article/9197019/Update_Report_sounds_alarm_on_China_s_rerouting_of_U.S._Internet_traffic)

punishment lead some in the US to worry about Chinese companies involvement in the telecommunications sector within the US and allied countries. Because they are seen as potentially irresponsible, telecommunication companies are prevented from entering the US domestic market as a result of less corporate transparency and accountability for technology accidents. So, for China, this is one area where a little transparency will help the prosperity of Chinese telecommunications firms, and allay the fears of US companies.

#### Proposal Four: Clearly Define Differences in Understanding State Espionage

Perhaps the most critical area that may curtail cooperation is the perception and misperceptions about espionage by both the United States and China. One might argue that recent indictments by the US of Chinese military officers, and further revelations by private sector actor Crowd Strike will strike a blow to further Sino-US cooperation in cyberspace.<sup>23</sup> Indeed, the week prior General Martin Dempsey, the chairman of the Joint Chiefs of Staff, welcomed his PLA counterpart, General Fang to the Pentagon. During that visit, it was noted by China that: “At present, China and United States are actively building the new model of major country relationship according to the important consensus of our presidents. It is not easy for our relationship to take one step after another to reach where it is today. In our military relationship, it is showing a positive momentum, which would benefit the Chinese and American people and help to secure the peace, stability, and prosperity of the region and the world.”<sup>24</sup> The next week the US Department indicted Chinese military officers under US domestic law for intellectual property theft targeting US companies. “When a foreign nation uses military or intelligence resources and tools against an American executive or corporation to obtain trade secrets or sensitive business information for the benefit of its state-owned companies, we must say, ‘enough is enough.’ This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market. This case should serve as a wake-up call to the seriousness of the ongoing cyberthreat. These criminal charges represent a groundbreaking step forward in addressing that threat.”<sup>25</sup> While the targets of the charges are the PRC government and the PLA, the text of the indictments, with its details of the means and scope of the violation can be interpreted as drawing US redlines for governmental behavior in cyberspace.

The misperception on the issue of nation-state espionage became apparent shortly after the indictments when the China based Internet Media Research Center published a response to the

---

<sup>23</sup> <http://www.justice.gov/opa/pr/2014/May/14-ag-528.html>  
<http://www.wtae.com/blob/view/-/26051954/data/1/-/mbff4iz/-/Indictment--PDF.pdf>

<sup>24</sup> <http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5432>

<sup>25</sup> <http://www.justice.gov/iso/opa/ag/speeches/2014/ag-speech-140519.html>

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

US allegations of Chinese state-sponsored industrial espionage.<sup>26</sup> The reiterated the revelations of a former US contractor who leaked information purportedly describing classified US programs. Analytically however, the paper did not address the US position of the United States that led to the indictments. That is: there is a line between cyber espionage for the purpose of national security, and by the state to collect information on behalf of domestic corporations to compete globally. Indeed, the paper confirms the US distinction between the two types of activities, while raising legitimate concerns about privacy of individuals in the digital age.

With the recent indictments of Chinese military officers under US domestic law for alleged intellectual property theft via the cyber domain one might argue that US/Chinese cooperation in cyberspace is no longer possible. However, this is a very short-sighted view. Great powers, when faced with strategic challenges, need time to react and cool-off. Although the US-China Cybersecurity dialogue is (as of this writing) postponed, it will surely restart again at some point in the future if past Sino-US cooperative efforts are any indication. Evidence for this is seen in several non-cyber dialogue related issues. First, on June 5-6 the Chinese Ministry of Foreign Affairs hosted a conference in Beijing titled “The International Workshop on Information and Cyber Security,” which was attended by a US delegation. In the non-cyber arena, China was invited, and took part in the Rim of the Pacific (RIMPAC) - the world largest international maritime exercise. Furthermore, when China and Russia, along with other states proposed an “international code of conduct on information security” within the United Nations General Assembly, the US did not support this. This was due to existing and continuing disagreements on international norms of behavior in cyberspace, which will require dialogue and engagement if the two powers are to lead the world towards a cyber environment where commerce and prosperity rather than conflict and mistrust prevail. US objection on the UNGA proposal was that it would allow for more government control of the Internet. China continues to object to allegations of intellectual property theft by the State. The U.S. has not shown support for the Russo-Chinese initiatives, and vice versa, however, the US-China Cybersecurity intergovernmental dialogue was still launched to discuss and negotiate a common ground on these topics of mutual concern. As these issues persist, and both sides recognize the importance of dialogue to resolve issues, these dialogues should continue on the foundations built over the past decade.

---

<sup>26</sup> China Internet Media Research Center, “America's Global Surveillance Record” [http://www.chinadaily.com.cn/America's Global Surveillance Record/world/2014-05/26/content\\_17539247\\_5.htm](http://www.chinadaily.com.cn/America's%20Global%20Surveillance%20Record/world/2014-05/26/content_17539247_5.htm) (26 May 2014).

*The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University*

## **Conclusion**

Cyber conflict, ranging from access to disruption to armed attack constitutes a new form of power. There is a common interest of all in the prevention of cyberwarfare that should overshadow any purely national interest of welfare or security. True cybersecurity will be found not only in Sino-US cooperation, but in the collective efforts of all. The Sino-US relationship will be seen by all as a positive first step. It will require, and does today require, a real renunciation of the steps by which past cybersecurity has been sought. It is clear that in a very real sense past patterns of national security are inconsistent with the attainment of effective security in cyberspace-- a domain which contains many interdependencies.