16 November, 2015

A Reluctant Cyber Security Agreement between the US and China

Dr. Omair Anas *

Three months after the biggest data theft from the American networks, the US and China have agreed to cooperate in the field of cyber security.[1] The blame game continued for many years between China and the United States over cyber attacks on the American and Chinese networks, so much so that the United States decided to consider sanctions on individuals and firms involved in the cyber attacks. In August, the US had declared to formulate a set of economic sanctions to be slapped on Chinese businesses suspected of carrying out cyber-thefts. Experts think that these talks of sanctions have brought the two countries on the table for talks. The tension between China and America over continued cyber attacks escalated when thousands of accounts of the White House Office of Personnel Management were accessed by hackers over a period of time. According to an order passed in April 2015, the US Treasury can freeze or block assets belonging to those involved in cyber attacks on critical computer networks. The White House statement also said: "We've previously indicated our concerns [about] China's activity in cyberspace. These are concerns that the President has raised directly with his Chinese counterpart in the past. Certainly, the announcement by the Department of Justice last year to indict five Chinese military officials for their actions in cyberspace should be an indication that we take these concerns very seriously." Soon after the indictment, China had suspended the working group for cyber security cooperation established in 2013.[2] However, the joint statement issued by the two presidents clearly demonstrates the limitations of any cyber security

framework, which show states' inability to report each and every individual cyber violation. The US President, Barack Obama said:

> President Xi, during these discussions, indicated to me that, with 1.3 billion people, he can't guarantee the behavior of every single person on Chinese soil – which I completely understand. I can't guarantee the actions of every single American. What I can guarantee, though, and what I'm hoping President Xi will show me, is that we are not sponsoring these activities, and that when it comes to our attention that non-governmental entities or individuals are engaging in this stuff, that we take it seriously and we're cooperating to enforce the law.
>
> The last point I'll make on the cyber issue – because this is a global problem, and because, unlike some of the other areas of international cooperation, the rules in this area are not well developed, I think it's going to (be) very important for the United States and China, working with other nations and the United Nations and others – and the private sector, to start developing an architecture to govern behavior in cyberspace that is enforceable and clear.
>
> It doesn't mean that we're going (to) prevent every cyber-crime, but it does start to serve as a template whereby countries know what the rules are, they're held accountable, and we're able to jointly go after non-state actors in this area.[3]

The Chinese President Xi Jinping, in response, underlined the need to strengthen cooperation and avoid this issue leading to confrontation and politicization. What was agreed upon by the two leaders was not about any mechanism to detect and react against a cyber theft, it was mostly to work through a high level joint dialogue mechanism, provide investigation assistance and facilitate information-sharing. The joint statement reads:

> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[4]

Given the fact that the two giant nations occupy the greatest pie of the global e-commerce (55 percent of global e-commerce), they are also competitors. China, with its huge consumer base, is expected to dominate global e-commerce with $1 trillion e-commerce sales by 2018, accounting for more than 40 percent of the total worldwide. In the recent economic slowdown, the United States has retaken the first position from China with $349 billion e-commerce sales.[5] But in the long term, China will remain as the fastest growing e-commerce market. However, a fundamental difference between the US and Chinese market is that many of the Chinese companies are directly or indirectly linked with the state. The cyber security discourse has developed in the context of cyber security of their e-commerce stakeholders. With repeated cyber attacks on US companies, American politicians are under pressure to respond against these attacks, which, apparently, originate from China. China has used the sensational leaks by the former National Security Agency worker, Edward Snowden, in its defence, accusing the Americans for violating internet norms.[6] At a time when US trade data was vulnerable to cyber attacks and the US government was making an effort to develop some norms in order to protect trade secrets, Snowden's disclosures inflicted much damage on America's international credibility. The Chinese, Russians and many other countries have always used these disclosures against the US Despite being attacked repeatedly, the United States had failed to facilitate an international understanding on cyber security. This was mainly due to its support to the bilateral arrangements among countries and participation of non-state stakeholders including corporate and civil society. Unlike the United States, Russia, China and other Asian countries are looking for a more state controlled mechanism. Most of the regional as well as global cyber security agenda are framed around legal measures, technical and procedural measures, organizational structures, capacity building and international cooperation as advised by the International Telecommunication Union.[7] ASEAN countries, European Union, Gulf Countries and other regions are developing their regional cyber security.

At least 600 attacks on American computers have reportedly originated from China. The media reports say that these attacks were particularly targeting major companies and their customers, such as Apple iCloud users, and the U.S. aviation companies, such as

Boeing and Lockheed Martin. The latest and the most sensational cyber attack was the cyber-intrusion into the U.S. Office of Personnel Management (OPM) in April 2015. The OPM data breach provoked much of the American response, which required an effective deterrence and sanctions against individuals and entities involved in such intrusions. Given this backdrop of the US-China cyber security agreement, it can be said that the US-China cyber security cooperation may facilitate further clarification and definition of cyber security issues, which are still largely undefined.[8] This deal is more a beginning towards evolving more defined and globally acceptable cyber behaviour.

What is the agreement about?

According to the Council on Foreign Relations Senior Fellow, Robert Knake, the agreement will be enforced by something called CERT-to-CERT agreement – that is, direct cooperation between Chinese and American law enforcement officials. The agreement also establishes a Cabinet-level dialogue between the countries on espionage. The joint statement says:

> Both sides are committed to making common effort to further identify and promote appropriate norms of state behaviour in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace.

The two sides also agree to create a senior experts' group for further discussions on this topic. A high-level joint dialogue mechanism on fighting cyber crime and related issues will be established. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. The dialogue will take place twice a year starting from 2015. Experts at the Council for Foreign Relations say that the high-level joint dialogue involves the Ministry of Public Security, Ministry of State Security, Ministry of Justice and the State Internet and Information Office on the Chinese side, and the Secretary of Homeland Security, U.S. Attorney General, representatives of the intelligence community,

and FBI on the U.S. side.[9] From the US perspective, this deal was more about convincing China to stop engaging in economic espionage and to set up a CERT-to-CERT response in case any further theft happens. In a later agreement between China and the UK, commercial espionage again came as the main concern and it was agreed to be stopped.[10] This will also involve the establishment of ministerial level dialogue. The deal does not affect the US plans of sanctions against individuals and entities involved in data theft.[11] Interestingly, the deal does not talk about non-business data theft secured through traditional or cyber spying, which suggests that the two sides would maintain the status quo.

The White House Fact Sheet on US-China Cyber security states that the US and China have agreed "that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cyber crimes, collect electronic evidence and mitigate malicious cyber activity emanating from their territory."

The deal has received a mixed response from the optimists' camp and there still remains much pessimism. Those, who see this deal as a small but important step, think that the deal is important because it allows the United States to evolve an active policy discourse on developing the norm against economic espionage in other diplomatic contexts, including trade negotiations, regional and bilateral cooperation on cyber security. This deal may not stop the next cyber attack, but as David Fidler of CFR observes, the next "economic espionage will unfold in a different normative context,"[12] which will open up a new legal discourse on cyber security beyond the current blame game and politicization. The Chinese willingness to sign such an agreement is touted as a win-win situation by the Chinese state media, as the use of sanction by the US against Chinese individuals and entities, as declared, would have affected China's international credibility. The Chinese official media, the *People's Daily* underlines the fact that nearly 50 Chinese IT companies are listed in the U.S. stock market with a total worth of nearly US$ 500 billion. Similarly, nearly 1,000 U.S. investment funds' money has gone to Chinese high-tech companies.[13] The

size of common interests in cyber security is better protected by a joint mechanism, instead of persistent denial. From Chinese perspective, China is also a victim of data theft and hacking. According to the *People's Daily*, 40,186 Chinese websites were hacked and 24 percent of attacks originated from the US.[14] China's National Computer Network Emergency Response Technical Team Coordination Center (CNCERT or CNCERT/CC) is perhaps more consistent in reporting cyber attacks on Chinese networks with its weekly reports. It helps China not only as a victim of the cyber attack and espionage, but also as a crucial partner for the global cyber security.[15]

Mixed Reactions

Much of the US complains against Chinese cyber thefts are not about attacks on critical infrastructure, rather it is about theft of intellectual property, trade data, consumer base data, financial data. Those, who are sceptical about the current agreement, complain that this deal does not agree on norms of cyber behaviour by the international community. They understand the limitations of such an international agreement in pinpointing cyber crimes, such as "the geographic point of origin, the identity of the actual perpetrator doing the keystrokes, and who was responsible for directing the act."[16] The United States, indeed, has strengthened its position against China as the two countries have agreed to address the issue at the highest level at least on a commonly agreed program, such as infringement on intellectual properties, trade and other data. With this agreement, both countries are obliged to formally engage in future cyber breaches suspected of having originated from either country. The Commission on the Theft of American Intellectual Property has estimated annual losses of $300 billion of which more than 50 percent of were attributed to Chinese hackers.[17] For American business, this deal may facilitate a new cyber environment once further complains are treated by the joint mechanism. However, for traditional government to government spying, this does not offer much or they did not want anything either.

One major problem that this agreement may face is that it does not include, as of now, media, enterprises and other non-state stakeholders. Unlike the US cyber policy

making where non-state entities are far more influential than the state itself, China's cyber policy is predominantly controlled by the state. For this reason, cyber security debate in the US is heavily influenced by the non-state commercial entities and civil society. This will remain a major hindrance between China and the international community as China's cyber security policy is shaped by the principle of "cyber space sovereignty", a contested perception. As the characteristics of cyberspace face limitation of attribution, only an international norm can define how the principle of territorial sovereignty can guide international cyber space.[18] As of now, the Chinese perception of the cyber space restricts the role of other stakeholders in the governance of cyber space.[19] Global trade groups have been putting pressure on the US government to find a way to get Chinese cyber laws amended as they find their mobility hindered and their reach to the vast Chinese market restricted. This deal, though an important step, does not show much hope for liberal internet governance in China and, hence, in case of cyber security violations, the Chinese state will remain the central reference and their deniability will remain unchanged. The deal hopes only to get Chinese convinced for more changes in their cyber laws in conformity with the evolving international cyber security measures.

***

** Dr. Omair Anas is Research Fellow at the Indian Council of World Affairs, New Delhi*

Endnotes:

[1] "Fact Sheet: President Xi Jinping's State Visit to the United States", The White House, 25 September 2015. Retrieved: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[2] "China Halts Cybersecurity Cooperation after U.S. Spying Charges", 20 May 2014. Retrieved: http://www.bloomberg.com/news/articles/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.

[3] Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference 25 September 2015, The White House, https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

[4] "Fact Sheet: President Xi Jinping's State Visit to the United States", The White House, 25 September 2015. Retrieved: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[5] "Global e-Commerce Set to Grow 25% in 2015", 29 July 2015. Retrieved: https://www.internetretailer.com/2015/07/29/global-e-commerce-set-grow-25-2015

[6] Rupert Cornwell, "US Declares Cyber War on China: Chinese Military Hackers Charged with Trying to Steal Secrets from Companies Including Nuclear Energy Firm", 19 May 2014. Retrieved: http://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html.

[7] "Global Cybersecurity Agenda (GCA)", http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

[8] Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks", *Harvard National Security Journal,* Vol. 6, 2015.

[9] Adam Segal, "Attribution, Proxies, and U.S.-China Cybersecurity", 28 September 2015. Retrieved: Agreementhttp://blogs.cfr.org/cyber/2015/09/28/attribution-proxies-and-u-s-china-cybersecurity-agreement/.

[10] "UK/China Cyber Security Deal: National Security Attacks Still OK, It Seems", 22 October 2015, Retrieved online URL: http://www.theregister.co.uk/2015/10/22/uk_china_cyber_security_agreement_ip/.

[11] Robert Knake, "Quick Reactions to the U.S.-China Cybersecurity Agreement", 25 September 2015. Retrieved: http://blogs.cfr.org/cyber/2015/09/25/quick-reactions-to-the-u-s-china-cybersecurity-agreement/.

[12] http://blogs.cfr.org/cyber/2015/09/28/u-s-china-cyber-deal-takes-norm-against-economic-espionage-global/.

[13] "Commentary: China is a Staunch Defender of Cybersecurity", *The People's Daily*, 26 September 2015. Retrieved: http://en.people.cn/n/2015/0926/c90000-8955511.html.

[14] "Cyber Security a Common Task for China and US", *The People's Daily*, 21 September 2015. Retrieved: http://en.people.cn/n/2015/0921/c90000-8953083.html.

[15] Official website of National Computer Network Emergency Response Technical Team Coordination Center of China (CNCERT or CNCERT/CC) http://www.cert.org.cn/publish/english/index.html.

[16] "Top U.S. Spy Skeptical about U.S.-China Cyber Agreement", *Reuter*, 29 September 2015, Retrieved: http://www.reuters.com/article/2015/09/29/us-usa-cybersecurity-idUSKCN0RT1Q820150929.

[17] "Will the US-China Cybersecurity Pact Work?" *Voice of America*, 29 September 2015. Retrieved: http://www.voanews.com/content/will-the-us-china-cybersecurity-pact-work/2983685.html.

[18] Heinegg, Wolff Heintschel von, "Legal Implications of Territorial Sovereignty in Cyberspace", 2012, 4th International Conference on Cyber Conflict.

[19] "Chinese Response to White House: It's Cyber Sovereignty", https://www.uschina.org/media/inthenews/chinese-response-white-house-its-cyber-sovereignty.