CSS Analyses in Security Policy
No. 224, April 2018, Editor: Christian Nünlist

Cybersecurity in Sino-American Relations

Cyberspace and cyberespionage represent a source of disagreements and tensions between the US and China. Nevertheless, in 2015, the two powers managed to find an agreement on cybersecurity to stabilize their relationship and reduce risks of misperceptions in cyberspace.

By Marie Baezner

The relationship between China and the US follows the dynamic of competitive interactions between great powers. The two states are in competition militarily, politically, and economically. This relationship has evolved and changed over the years. The China policy of the new US administration has a more narrow focus than that of its predecessor. President Donald Trump's administration also lacks an overarching strategy in dealing with issues related to China. This relationship continues to be regularly punctuated with provocations in the physical world (Chinese territorial claims in the South and East China Seas that threaten US allies and partners in the regions) and in cyberspace (cyberespionage campaigns).

Over the last two decades, the tensions between the two powers have specifically grown over the following issues of cybersecurity: China and the US have conducted cyberespionage against one another (see list); China's growing military and cyber capabilities are used in the establishment of Anti-Access/Area Denial zones; and China disagrees with the US model of internet governance. To reduce growing tensions, both states agreed to a binding bilateral accord on cybersecurity in September 2015, in which they pledge not to commit or support economic cyberespionage.

The building of the military hacker unit «61398» in Shanghai. *Carlos Barria / Reuters*

Cyberespionage Campaigns

The first cyberespionage campaign in the US attributed to a Chinese state actor was discovered in 2004 and had targeted the US Department of Defense and defense contractors. To date, a least 14 cyberespionage campaigns in the US have been attributed to Chinese state actors. In these campaigns, the targets were state institutions, the military, information technology firms, telecommunications, the energy sector, journalists, and activists. Sensitive information and intellectual property were stolen. A 2014 report estimated the economic loss through stolen intellectual property to the US economy at US$250 billion per year. This amount needs to be put into perspective, as it does not include

Cyberespionage Campaigns

2003–2006: Titan Rain – China spying on US military and US institutions.

2006–2010: Shady RAT (spying by China).

2007–2009: GhostNet – China spying on Tibetan missions and NGOs.

2008–2014: Hikit – China spying on journalists, IT firms, academics, and government institutions worldwide.

2008–2011: Byzantine series – China spying on US institutions.

2009–2011: Night Dragons – China spying on US critical infrastructure.

2009–2010: Operation Aurora – China spying on Google, Adobe, and other IT firms.

2009–(believed to be ongoing): NSA fourth-party collection – USA spying on Chinese hackers targeting the US Department of Defense.

2010–2014: Operation Shotgiant – USA spying on Huawei.

2011–2013: Operation Beebus – China spying on contractors of the US Department of Defense.

2013–2015: Operation Iron Tiger – China spying on US and Asian IT, telecommunication, and energy companies.

2014–2015: Chinese campaign spying on the US Office of Personnel Management.

damage to the firms' reputation, the loss in comparative advantages, and investment in cybersecurity to stop the intrusions. It is also possible that more companies were affected by Chinese state actors, but did not report the intrusions out of fear for their reputation.

In 2013, Edward Snowden revealed the US mass internet surveillance program and shed light on the US cyberespionage campaigns against China. It showed that the US had spied on Chinese information technology firms, banks, and leaders of the Communist Party of China. The lack of data makes it difficult to evaluate the economic losses caused by US cyberespionage in China and to assess whether the US still conducts such campaigns.

The disagreement between the two powers over cyberespionage mainly related to the nature of the campaigns. US authorities make a distinction between cyberespionage for national security concerns and cyberespionage for economic purposes. The former is internationally tolerated, but the latter is not. Intelligence for national security, as opposed to economic reasons, is judged as being part of a state's responsibility to protect its population and territory from foreign threats. The US authorities claimed that its cyberespionage campaigns were only about national security and did not serve any economic purposes. On the other hand, the Chinese government denied perpetrating any cyberespionage. This disagreement increased mistrust between the two powers and the risk of misinterpreting activities in cyberspace as acts of war.

The 2015 Agreement

1. Respond to requests for information and assistance for malicious cyber activities.
2. Investigate cybercrime emanating from the signatories' respective territories.
3. Exchange information on the status of the aforementioned investigations.
4. Refrain from conducting or supporting cyberespionage for economic purposes and theft of intellectual property.
5. Make efforts to identify and promote international norms of state behavior in cyberspace.
6. Create a high-level joint dialog mechanism on fighting cybercrime and related issues.
7. Create a hotline to discuss issues related to cyber activities.

At the same time, groups affiliated with the Chinese People's Liberation Army (PLA) perpetrated a large number of cyberespionage campaigns. The theft of intellectual property enabled the PLA to develop technologies without having to invest in research, but it seems that the PLA had difficulties to transform the stolen information into competitive advantages. This was explained by the organizational structure of the PLA, which supposedly prevented the Chinese military from converting the stolen information. The PLA was overloaded with intellectual property information coming from cyberespionage campaigns, which could not be used efficiently because of a strongly compartmentalized bureaucracy. The fact that technology was constantly becoming more complex also made it more difficult for the PLA to perfectly imitate and replicate it.

The 2015 Agreement

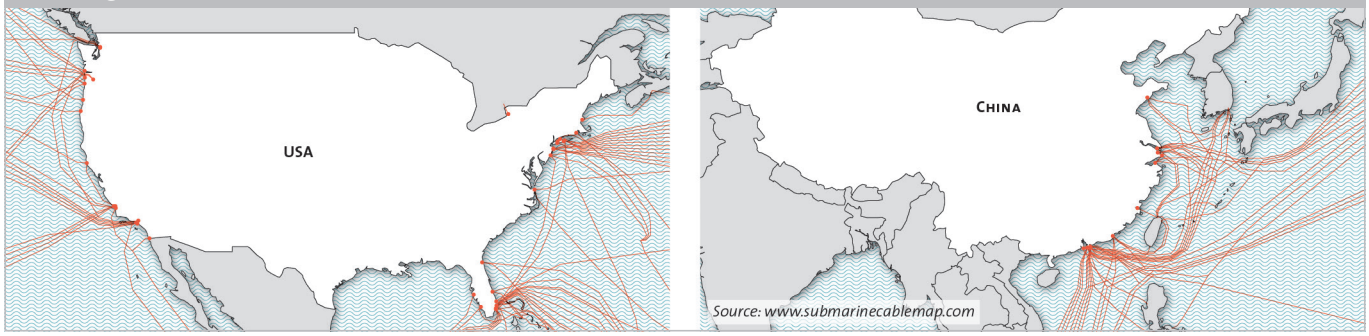
The US tried to take a tougher stance against Chinese cyberespionage campaigns. In May 2014, the US indicted five members of the PLA to show that it would not let cyberattacks against its firms go unpunished. This was mostly a symbolic move, as the five officers stayed in China and were thus never jailed. After the US Office of Personnel Management had been hacked, the US also warned Chinese authorities that it was considering retaliation through economic sanctions and diplomatic measures. However, after the revelations of Edward Snowden in 2013, the credibility and legitimacy of US actions in cyberspace were severely diminished among both its allies and its competitors. The disclosures added tensions to the relationship between China and the US, but mostly created an opportunity to settle the issue of cybersecurity by exposing both states' practices.

The solution to decrease this pressure was found in the development of a bilateral agreement to initiate confidence-building measures in cyberspace. In the 2015 Agreement, both states agreed to not commit or support economic cyberespionage. The accord also included regular meetings between representatives of both states' security agencies to exchange information on cybercrime, and the creation of a hotline to communicate directly on cybersecurity issues (see list). The agreement was considered a good step towards the development of cooperation between the US and China over cybersecurity issues. It was hoped that more cooperation on these issues would reduce the risks of misperceptions (perceiving a cyberattack as an act of war) and escalation (tensions boiling over into a conventional war) in cyberspace. The agreement was seen as a victory for the US, which persuaded the Chinese government to agree to the distinction between economic and national security cyberespionage. The Chinese authorities also perceived the agreement positively as they had asked for more cooperation on cybercrime for years. Chinese individuals and firms were regularly targeted by cybercriminals, and Chinese authorities complained that Western countries were reluctant to collaborate in investigations.

After the Agreement

Since the 2015 agreement, US cybersecurity experts have noticed that the number of cyberattacks originating from Chinese state actors against US economic targets has significantly decreased. However, they also observed that attacks from other countries increased. They advance four hypotheses to explain this shift. First, they thought that the 2015 agreement might have forced Chinese hackers to use proxies in other countries to target victims in the US. Second, US experts argued that the agreement could have pushed Chinese state actors to become more sophisticated and more dif-

Landing Stations of Submarine Cables in the US and China



ficult to detect in cyberspace. Third, the agreement might have pushed Chinese hackers to redirect their cyberattacks towards easier targets outside the US. Finally, Chinese authorities conducted a vast anti-corruption campaign in the government and the PLA shortly after signing the 2015 agreement. This campaign might have discouraged some employees who had previously carried out cyberattacks to supplement their salary.

The discourse is moving away from a Cyber Pearl Harbor to a more practical approach to cybersecurity.

However, the agreement was not meant to stop all cyberespionage, only the economically motivated campaigns. Traditional national security cyberespionage continued. Chinese hacker groups with links to the Chinese government have been caught targeting US dual-use technology firms working with the US government and maritime industries connected to the South China Sea. Such targets are not covered by the agreement, and could also be considered national security targets.

Even though the 2015 agreement seemed to succeed in diminishing the number of cyberattacks from China, the accord presents some limits. Its implementation is difficult to evaluate, as it is laborious to estimate the number of cyberattacks. Indeed, not all victims declare that they have been attacked, and cyberespionage campaigns often take time to be discovered. Furthermore, neither the US government nor the Chinese authorities can control every individual on their territory. They would not be able to prevent citizens from conducting cyberattacks that could be interpreted by the other state as an act perpetrated or supported by state's authorities. In addition, the 2015 agreement on cybersecurity does not have enforcement measures. In case China or the US were to support or conduct economic cyberespionage against the other, the accord would not foresee any punitive measures. Finally, it is difficult to distinguish economic cyberespionage from national security cyberespionage. A state could argue that it conducted a cyberespionage campaign against a business for reasons of national security, but such a practice would be difficult to justify. This is particularly true for the US, as Chinese firms are often state-owned, which complicates the distinction between national security and economic purposes of cyberespionage.

At the international level, the 2015 agreement on cybersecurity was perceived as a positive sign. It showed that diplomatic solutions can be used for cybersecurity issues. This accord could be considered a first step towards an internationalization of such norms on cybersecurity, if enough states were to sign similar pacts. Since 2015, the UK and Australia have signed comparable agreements on cybersecurity with China.

In October 2017, the US and China jointly announced that they would continue to uphold the 2015 agreement. The Trump administration thus does not deny the decrease in economic cyberespionage campaigns, and does not see any reason to stop the cooperation. A further step in cooperation between both states in cyberspace could be the development of another bilateral agreement to regulate the use of cyberspace in wartime.

The Internet Governance Issue

However, two other issues on cybersecurity continue to be subjects of tensions. A first disagreement is about the international governance of the internet. Historically, the US as the developer of the internet has imposed its approach of governance on the international community. The internet is currently managed by the Internet Corporation for Assigned Names and Numbers (ICANN), a not-for-profit organization based in Los Angeles. ICANN is directed by representatives of the main stakeholders (information technology industries and technicians) and users of the internet. This bottom-up structure leaves little space for states' inputs. Some of ICANN's functions are to regulate technical aspects of the structure of the internet like the allocation of internet addresses, the management of root servers, and the development of internet protocols. In October 2016, the US Department of Commerce did not extend the contract that regulated its supervision over ICANN's activities.

This transition did not change anything in the way the internet works, but it ensured that ICANN was truly independent in its decisionmaking processes. However, China, Russia, and other states have criticized this multi-stakeholder and bottom-up approach of governance and claimed that it continues to serve US intelligence and interests. They would prefer a governance model giving more weight to the states, as is the case in the International Telecommunications Union, for example. These states are worried about the US interfering in their domestic management of the internet. The Chinese government has strictly controlled the content of the internet on its territory through its "Great Firewall" since 1996. This tool functions as a filter that prevents people on Chinese territory to access specific websites. The Chinese govern-

ment is concerned that unlimited access to foreign information would destabilize the Chinese social and political order. The Chinese authorities regularly accuse the US of trying to influence and Westernize its population with soft power through the internet. Since March 2015, the Chinese government has used its "Great Cannon", an offensive cybertool, to censor certain websites. This tool redirects internet traffic toward a specific website and causes it to crash by distributed denial of service attack (DDoS). This type of attack consists of overwhelming a website with a high amount of internet traffic. The 2015 agreement does not cover the issue of internet governance, but such issue cannot be dealt with in a bilateral agreement and would need to be addressed internationally.

In theory, A2/AD could also be applied to cyberspace.

Anti-Access/Areal Denial Zones

A second disagreement relates to the establishment of Anti Access/Area Denial (A2/AD) zones by China in the South and East China Seas. A2/AD zones are an asymmetric defense approach using all the military domains to prevent or deter an adversary to enter a particular zone. China is aware that it cannot hope to overcome the US in a full-scale conventional war, so to ensure its freedom of movement at sea, China developed these zones to reduce US projection of force in these regions. To secure these areas, China not only modernized its arsenal of military hardware, it also improved its cyber capabilities to control the information space in the event of a conflict. The aim is to disrupt an adversary's ability to communicate with and to control its troops by interrupting GPS localization and/or communications. China has already shown that it is capable of disrupting satellites with conventional and cyber means. It shot down one of its own defunct satellite in 2007, and hacked a US weather satellite in 2014.

As predicted, the US, which has allies and partners in the region, viewed the development of A2/AD zones in the South and East China Seas with concern. In response to Chinese A2/AD efforts, the US created the Joint Operational Access Concept and the AirSea Battle Operational Concept. These two concepts stipulate the deployment of a large amount of submarines with long-range missiles used in coordination with cyber operations to destroy Chinese command-and-control centers and against Chinese missile systems.

In theory, A2/AD could also be applied to cyberspace. The concept, also called cyber blockade, foresees denying of access to the internet or disrupting the information flow to adversaries. That could be achieved by launching cyberattacks on the internet exchange points (facility interconnecting internet networks) to disable them or by physically tampering with physical internet infrastructures (e.g., cables, servers, and exchange points).

In the event of an escalation between China and the US, one state could try to deny internet access to the other to slow down or cut the information flow to and from military command and control centers. It would do so by tampering with submarine or terrestrial cables, or communication satellites. However, it will not be an easy task for the US to disconnect China's internet. As China has more than a dozen landing stations (stations where submarine cables are connected to the terrestrial network), the US would have to cut them all simultaneously to be efficient (See map 1). In the reverse situation, it would be just as difficult for China to act on landing stations in the US (see map 2). If states only act on a small number of cables, access to the internet could be slowed down, but the impact would mostly be insignificant. Though states could still attack communication satellites, such measures would not have enough impact to deny internet access to an adversary either.

The development of such zones and the inclusion of cyberspace as a military domain marks a shift in the military discourse. The discourse is moving away from the "Cyber Pearl Harbor" scenario (which anticipates a highly devastating cyberattack) to a more practical and doctrinal approach to cybersecurity.

Marie Baezner is a researcher in the Cyber Defense Team of the Center for Security Studies (CSS) at ETH Zurich. She has co-authored several "CSS Cyber Defense Hot Spot Analyses" on cyber-incidents and cyber aspects in current conflicts.

CSS Analyses is edited by the Center for Security Studies (CSS) at ETH Zurich. Each month, two analyses are published in German, French, and English. The CSS is a center of competence for Swiss and international security policy.

Editors: Christian Nünlist, Matthias Bieri, Fabien Merz, Benno Zogg
Layout and graphics: Miriam Dahinden-Ganzoni
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000254684

Feedback and comments: analysen@sipo.gess.ethz.ch
More issues and free online subscription:
www.css.ethz.ch/en/publications/css-analyses-in-security-policy