EAST-WEST CENTER
COLLABORATION • EXPERTISE • LEADERSHIP
SINCE 1960

Asia Pacific Bulletin

Number 135 | November 1, 2011

China and the United States: Hacking Away at Cyber Warfare

BY TING XU

Ting Xu, Senior Project Manager at the Washington, D.C.-based Bertelsmann Foundation, explains why "Adding cyber warfare to an already long list of irritants between Washington and Beijing will not make the dialogue between them any easier. But the increasing links between cyber warfare and traditional warfare ensure that the two countries cannot avoid the subject."

Rising cyber attacks against Western governments and companies along with speculation that critical infrastructure has been infiltrated has put China under suspicion as the world's leader in cyber espionage. Beijing is increasingly assumed to be behind any high-profile cyber assault, while the US government is faulted for an inability to protect its national interests from such attacks. The situation has led to more mutual Sino-American recriminations, an alarming development between two nations whose relationship is already fraught with mistrust.

Ominous tones are emerging from Washington as a result. The Pentagon has concluded that a cyber attack that causes substantial infrastructural damage may be deemed an act of war, and Defense Secretary Leon Panetta recently warned that such an attack could be America's next "Pearl Harbor." Given the already significant wariness with which China and the United States eye one another, the stakes for safely managing cyber space are high. Unfortunately, accomplishing this goal is complicated since attributing an attack to a specific actor is not always possible. In addition, the internet's fluid nature and structure prevent computer systems from being completely resilient to external infiltration.

The US public and private sectors have begun working to better protect their online infrastructure from attack, but solving the problem of cyber attack attribution is a thornier matter because it is a two-step process. First, collecting the necessary data is difficult due to the large number of cyber assaults, the rapidly changing tactics behind them, and the tendency for companies to conceal cyber losses. Second, to determine if a foreign government is behind the attack a motive or intention to attack must exist, regardless of the ability to trace it to a government agency. In 2007, for example, data on a cyber attack against the Estonian government and private cyber infrastructure showed it originated in 178 countries. But since Russia was seen as having the most to gain from initiating such an action, it was accused, correctly or incorrectly, of initiating the illicit activity. Two years later, a Russian youth group claimed responsibility for the attack and denied that the Kremlin had any role in it.

Were data related to a cyber attack against the United States to show origination in China, or vice versa, the error-prone, intention-based judgment that both countries use could lead to the conclusion that the other was behind the attack. That miscalculation, however, could have devastating military consequences if initial damage was severe or if the cyber attack were seen as a precursor of an attack by traditional means. This would be an especially tragic outcome considering that a non-state terrorist entity could have infiltrated one country's system and launched the attack against the other. Such a tragedy need not occur. It is important to remember that 80 percent of reported global cyber incidents are profit-driven economic crimes; only a small proportion are politically or militarily motivated. Distinguishing between the two is vital.

Asia Pacific Bulletin | November 1, 2011

Cyber crimes are illegal and often profit driven. Primary examples of such activities include online bank information theft, identity theft and online predatory crimes. They involve simple tactics such as phishing, and building security-system resilience is cost-effective and relatively straightforward. Cyber attacks, however, would likely be coordinated by large organizations or governments. They can cause serious political and economic damage by collecting intelligence or compromising critical infrastructure and military capability, and are more difficult to defend against. It would be hard to argue that a major government, including China's, would be behind cyber crimes. On the contrary, Beijing has every incentive to prevent such crimes initiated by or targeting Chinese entities.

"There can be little doubt that global militaries are developing cyber warfare strategies and that any future conflict will have a cyber component. The necessity for China and the United States to cooperate on setting the rules for cyber activities, thereby reducing the risk of miscalculation, is clear. Fortunately, the opportunity to do so exists."

However, intelligence gathering is another matter. Governments have long spied on one another, and cyberspace opens another avenue for this tradecraft. There can be little doubt that global militaries are developing cyber warfare strategies and that any future conflict will have a cyber component. The necessity for China and the United States to cooperate on setting the rules for cyber activities, thereby reducing the risk of miscalculation, is clear. Fortunately, the opportunity to do so exists.

To begin, both countries can lead the process of establishing an international framework for the commercial use of cyber space and for a system of policing cross-border cyber crimes. This framework could include a common definition of cyber crimes and cyber attacks, developing public-private partnerships so that governments are informed of efforts to infiltrate systems, and establishing international procedures for attribution and prosecution of cross-border illicit activity.

Since cyber crimes are a relatively new phenomenon, this required international framework could be negotiated and established with a new international order that is based on the current distribution of global power. China's cooperation is vital to repress rogue activity. Putting China at the forefront of efforts to combat such crimes would avoid isolating Beijing and prevent criticism that "Western values," as Beijing so often claims, dictate the international norm-setting process. Such a procedure to govern commercial cyber space would also set a valuable precedent for future governance structures to address emerging global security challenges.

Regarding cyber warfare, some experts view "state-sponsored" cyber attacks as one-time actions followed, with near certainty, by traditional attacks. If this view is accurate, legitimate risks of escalation to traditional warfare exist. In addition, the challenge of precisely attributing an attack also opens a door for well-organized terrorist groups to manipulate the Sino-American relationship by launching an attack that appears instead to originate in Washington or Beijing.

China and the United States need to make cyber warfare a prominent part of their ongoing, bilateral strategic dialogue to ensure that mistrust does not lead to hostilities. As part of this dialogue, which now focuses on weapons of mass destruction, they can clarify the types of cyber attacks that would constitute a declaration of war. Also, bilateral consultations could address the types of cyber attack that could trigger nuclear retaliation and clarify to what extent cyber attacks against US allies would drag Washington into a conventional war. Finally, the Sino-US strategic dialogue could find ways to ensure that lines of communication remain open in event of emergencies caused by cyber attacks, such as damaged critical infrastructure, even in cases in which attribution is strongly suspected but unproven.

Adding cyber warfare to an already long list of irritants between Washington and Beijing will not make the dialogue between them any easier. But the increasing links between cyber warfare and traditional warfare ensure that the two countries cannot avoid the subject.

Ting Xu is Senior Project Manager at the Washington, D.C.-based Bertelsmann Foundation. The views expressed here are solely those of the author and not of any organization with which she is affiliated. She can be contacted via email at ting.xu@bertelsmann-foundation.org.