Ramping Down Chinese Commercial Cyber Espionage

Emilio Iasiello

Despite criticism from skeptics, China is trying to honor its “no commercial hacking for profit” commitments as first promised in an accord with the United States, and later reaffirmed at the November 2015 G20 summit. Recent news reports cited that in a show of good faith, China had arrested hackers per the U.S. government’s request prior to meeting with President Obama in September. While detractors believe that commercial cyber espionage hasn’t really stopped, recent Chinese efforts show a government trying to get a handle on its large spying apparatus that could include hired and independent contractors acting autonomously in addition to its other resources. While complete cessation may never occur, significant timely reduction demonstrates Beijing’s willingness to work with the United States as a partner and not a pariah, and provides a foundation from which the two governments can move forward on other cyber security areas where incongruity persists.

Emilio Iasiello has been a cyber threat analyst for the past thirteen years working as a government contractor and a government civilian in the Department of State as well as the Department of Defense, as well as as well as private sector companies providing cyber intelligence to Fortune 100 clients. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in peer-reviewed journals.

Foreign Policy Journal, December 9, 2015
China’s Cyber Spying Apparatus – Too Large to Manage?

According to recent press reporting, cyber spying perpetrated by the Chinese military against U.S. commercial targets waned substantially after the Department of Justice indictment of five People’s Liberation Army (PLA) officers for cyber-enabled commercial espionage. While this represents significant progress toward curbing bad behavior by a state whose nefarious cyber theft was termed “pervasive” by the Director of National Intelligence, some believe that China’s foreign intelligence service is still engaged in these types of activities. According to one security vendor, as of mid-October 2015, hackers associated with the Chinese government have targeted seven U.S. companies (five technology, two pharmaceutical) since September.

Still, despite these proclamations, there are those U.S. officials taking a pragmatic approach to the cessation of China’s cyber spying for commercial gain, such as the deputy commander of U.S. Cyber Command, who believes the effort will take time. According to the same press report, led by its president, China began applying pressure on its military to cease its economic espionage refocusing it on operations that support ensuring the country’s national security interests. This is encouraging for a state that has perpetually denied any involvement in hacking.

China is suspected of having successfully infiltrated the networks of as many as 141 organizations from 15 nations and in nearly two-dozen critical industries including tech, financial services, government, and defense since 2006, an effort that would take considerable resources to perform. The Chinese military, which has approximately 15 units known as technical reconnaissance bureaus that have a signals/cyber collection mission, is only one part of equation. The PLA has a strong militia system as well, in which active reserves augment almost every area of military operations. Added to the mix are several civilian organizations that are believed to have a cyber mission such as the Ministry of Public Security (MPS), as well as the Ministry of State Security (MSS), which has been linked by some to the 2015 Anthem breach. Added to the mix are academic and research institutes that may also be pursuing their own cyber espionage efforts.
While this may seem monolithic in scope, and a surprise to some, for China watchers, Chinese interest in this area is not novel, although it has been evolving. Discussions on network warfare were included in China’s 2013 *Science of Military Strategy*, an authoritative study of Chinese strategic thinking. Identifying PLA, MSS/MPS, and “non-governmental” forces involved in these types of activities. Indeed, the need for these forces is reaffirmed in China’s 2015 military strategy in which it identified “information society” (cyber power) as the departure point of international security.\(^m\)

Of note, according to the same press report,\(^n\) some portion of the vast Chinese cyber espionage operations looks to have been conducted by military personnel independent of the government’s direction, and perhaps, knowledge. Like independent contractors looking for buyers for their merchandise, these individuals provided stolen information to companies, further blurring the lines of what constitutes state culpability in these types of activities, and further complicates controlling them. There has been steady reporting reflecting the continued convergence of the tactics, techniques, and procedures (TTPS) used by cyber criminal and cyber espionage actors, such as employing spear phishing and using the same malware, for example.\(^o\) Despite having a steadily increasing military budget, inflation has impacted any benefits, contributing to significant corruption among its ranks,\(^p\) which may help explain “moon-lighting” practices and this cross pollination of criminal and espionage TTPs.

Given the various state and non-state individuals potentially engaged in cyber collection, it should come as little surprise that the volume of theft cannot be turned off at a moment’s notice. Taking into account overlapping mission areas, competition to deliver, target deconfliction issues, operations currently underway, independent operations, priority and non-priority tasking, it is understandable why reduction of cyber theft may be more of a evolving process than previously anticipated. This may help to explain the various targets and various types of capabilities observed over the past few years. Further complicating matters, oversight of these groups likely varies depending on the level of state affiliation that exists.
The recent arrest of hackers suspected of conducting the breach against the Office of Personnel Management in 2015 revealed that the hackers in question were criminals and not state-sponsored, according to Chinese officials. While skeptics doubt that the “real” perpetrators will be the ones prosecuted, it does demonstrate China’s willingness to meet the conditions of its promises to the United States. It also sends the message that China is a contributing partner in the global fight against cyber crime—crime being the optimum word here—and may open up future discussions to determine what is a global consensus on espionage definitions and characteristics.

Conclusion

This gives hope for cautious optimism in Beijing reducing—not completely stopping—cyber-enabled commercial espionage. While detractors are quick to point out that the recent “no hack” pledges made by China with other governments, including the joint one made at the recent G20 meeting, are paper promises that have no hope of enduring over a long period of time, they are nevertheless a marked progression toward codifying acceptable—and more importantly, unacceptable—nation state behavior in cyberspace.

This is not to say the United States should grant China carte blanche to stopping cyber espionage activities on their timetable. Washington should further engage with Beijing on the identification of key deliverable milestones and how they will be measured that would demonstrate Beijing’s commitment to its pledge. Too much progress has been made to let a knee-jerk reaction derail the agreement. As cited by one former White House director for cyber security policy at the National Security Council, “The importance of China committing to answer our calls… is a massive, massive change.” Allow the carrot of diplomatic engagement to run its course as the stick of sanctions always looms near.
References


