Should State-Sponsored Cyber Operations Target the Private Sector? American and Chinese Assessments

***Dr. Joseph Fitsanakis**, Coordinator, Security and Intelligence Studies program, King University; Director, King Institute for Security and Intelligence Studies.*

June 5, 2014. Article n°III.13

In May 2014, the government of the United States indicted five officers of the Chinese People's Liberation Army (PLA) with conspiracy to commit computer fraud, economic espionage, and theft of trade secrets, among other charges (Indictment Memorandum 2014). In a press conference held to announce the indictments against the five officers, the US Department of Justice accused them of expropriating trade secrets belonging to American companies through a variety of illegal computer hacking techniques (Finkle, Menn and Viswanatha 2014). At the same press conference, US government officials suggested that the PLA officers were members of Unit 61398, one of several groups of computer hackers operating within the command structure of the Chinese Armed Forces (Riley and Lawrence 2012). These groups are suspected of having participated in computer hacking attacks against at least 1,000 private companies or public agencies since 2001 (Schmidt and Sanger 2014). It was also suggested at the press conference that Chinese state-owned corporations —which were not named— had essentially hired the PLA hackers "to provide information technology [and] corporate intelligence" services (Finkle, Menn and Viswanatha 2014).

In the days following the indictments, Western media observers noted that the move to charge the five PLA officers was highly symbolic and would have little practical impact on the admittedly adversarial relations between the two countries in the field of cybersecurity (Schmidt and Sanger 2014). Indeed, the Chinese Ministry of Foreign Affairs almost immediately dismissed the charges as "ludicrous" and "made up", and indicated that there was "virtually no chance" that the five PLA officers would be extradited in the US to face cyberespionage charges (ibid.). Beijing went further, reminding the world's media of "large amounts of publicly disclosed information, [which] show that relevant US institutions have been conducting cyber intrusion, wiretapping and surveillance activities against Chinese government departments, institutions, companies, universities and individuals" in recent years (Taylor 2014). The Chinese government's statement refers almost certainly to the Office of Tailored Access Operations of the US National Security Agency (NSA), which, according to American intelligence researcher Mathew M. Aid, who disclosed its existence in 2013, has been targeting Chinese computer networks since at least 1999 (Aid 2013).

Defending Against Foreign State-Sponsored Cyberespionage

None of this seems especially novel. Beijing's protestations that it does not engage in cyberespionage sound as improbable as Washington's repeated assurances that its cybersecurity posture is purely defensive (Fitsanakis 2012). However, the indictments against the PLA officers are notable in that they represent the first-ever computer hacking charges pressed by the US Department of Justice against named officials of a foreign government. Many observers, including Jan Weedon of the American cybersecurity firm Mandiant, which produced the first publicly available report about Unit 61398 (Sanger 2014), described Washington's move as "a paradigm shift with regards to [...] ways countries try to hold each other accountable" in the field of cybersecurity (Finkle, Menn and Viswanatha 2014). Moreover, the charges against the PLA officers can be said to signal a highly visible turn in the policy of American government agencies *vis-à-vis* the protection of the country's private sector from cyberespionage and cybersabotage. American corporations have for years tried to defend themselves against cyberattacks allegedly perpetrated by foreign national entities, usually by hiring private investigators and consultancy firms (Riley and Lawrence 2012). But the indictments against the PLA officers, which are said to represent the culmination of a two-year-long probe by the Department of Justice, signal the determination of the American government to defend the country's private sector from foreign cyberattacks.

Economic Versus National-Security Cyberespionage

It is important to note, however, that, in indicting the five PLA officers, the US Department of Justice went to great pains to ensure that it did not accuse the suspects of engaging in cyberespionage in defense of China's national security. As observers put it at the time, there was an implicit acceptance in the language of the indictment that "large countries routinely spy on each other for national security purposes" (Schmidt and Sanger 2014). What sparked the indictments was that the accused PLA hackers employed intelligence resources belonging to the Chinese state in order to give a competitive advantage to Chinese companies vying for international contracts against American firms. Put differently, the US implicitly admits that it too conducts cyberespionage in defense of its national security. But it considers it "pernicious to use the intelligence instruments of the state for a business advantage" (Sanger 2014). In the words of US Attorney General Eric Holder, the operational difference between American and Chinese cyberespionage is that "we do not collect intelligence to provide a competitive advantage to US companies, or US commercial sectors", whereas China engages in the practice "for no reason other than to advantage state-owned companies and other interests in China, at the expense of businesses here in the United States" (qtd ibid.). The US Attorney General's comments appeared to garner enthusiastic support by the US Intelligence Community. One notable commentator was former NSA and Central Intelligence Agency (CIA) Director General Michael Hayden, who welcomed the indictment against the PLA officers "because it has our government rejecting the false equivalence between us and the Chinese" (ibid.).

But do the Chinese share Washington's strict distinction between state-sponsored cyberespionage activities conducted in the service of national security and operations aimed at advancing corporate interests? Evidence suggests that they do not. For Beijing, the line separating national security from business supremacy appears to be far less solid than for Washington. Chinese cultural conceptions of business practices are not based on the traditional American delineation between public and private spheres of activity. Moreover, the PLA's information warfare doctrine does not distinguish between military agility and economic strength (Cheng 2013). As some observers succinctly put it, for the Chinese Armed Forces, "economic security and national security are one" (Schmidt and Sanger 2014). Consequently, Chinese military doctrine does not see cyberespionage attacks against foreign companies as a criminal breach of intellectual property rights. Rather it views it as one thread in a broad fabric of methods that enable China to compete globally with the United States and other adversaries. In the words of China watcher Bonnie Glasser, of the Center for Strategic and International Studies, the PLA sees both state and corporate cyberespionage targets as "fair game and an essential means to accelerate China's reemergence as a great power" (qtd in Taylor 2014). This doctrinal perspective is reflected in the pattern of China's recent cyberespionage activities in the American private-sector realm. Beijing's targets have included oil companies, patent law firms, nuclear power facilities, market analysis units of global investment banks, and

unions that lobby against the increasing availability of Chinese-manufactured products in the domestic American market (Riley and Lawrence 2012).

A False Dichotomy Between Public and Private Sectors?

For the Chinese, Washington's intelligence dichotomy between the state and private sector a false "American artifact devised for commercial advantage" (Sanger 2014). Beijing essentially sees the demarcation between state and private activity as a conceptual model deliberately devised by the US to disadvantage China's intelligence-collection ability. Although China's private sector accounts for the vast majority of its gross domestic product, the country's economic life remains structured around approximately 200 large state-owned companies, which dominate areas such as the utility sector and heavy industry, including weapons-design and production (Medeiros *et al.* 2005). By contrast, the American utility sector is almost wholly privatized, while the defense industry is comprised of commercial entities that are simultaneously part of the national defense apparatus. These entities —firms such as the Raytheon Company or the Northrop Grumman Corporation— usually have a single primary customer, namely the US Department of Defense. The macroeconomic reasons for this peculiar arrangement are plain enough: it prevents significant state interference in the manufacturing sector while facilitating the production of unique large-scale military systems, without transforming the economy into a state-operated enterprise. But it does not change the fact that America's national-defense infrastructure is manufactured and maintained by private enterprise operating in the service of national security. This arrangement is crucial in highlighting the inconsistencies of Washington's cybersecurity doctrine.

In May 2014, while announcing the indictments against the PLA officers, Attorney General Holder reproached Beijing for deploying "military or intelligence resources and tools against [...] American executive[s] or corporation[s] to obtain trade secrets or sensitive business information for the benefit of its state-owned companies" (qtd in Finkle, Menn and Viswanatha 2014). But this distinction appears nonsensical when applied within the real-life context of the Chinese and American defense industries. If observed, Attorney General Holden's quasi-legal distinction between state-owned and private-sector cyberespionage targets would forbid China from spying on American defense contractors, since they are technically privately owned, as well as from sharing its intelligence product with its state-owned defense manufacturers. But it would not forbid American intelligence agencies from spying on Chinese state-owned defense manufacturers for the benefit of the US core defense industry. In light of this obvious disparity, several observers noted that Washington's criminal indictment against the PLA officers "did not touch on Chinese attacks aimed at [...] major [American] defense contractors", thus implicitly recognizing the "often blurry" lines separating state from private sectors in the US defense realm (Sanger 2014; Schmidt and Sanger 2014).

The Reality of Cyberespionage

In reality, the demarcating line between state agencies and the private sector is theoretical at best when it comes to core functions of the contemporary nation-state, such as defense, energy or telecommunications. Consequently, intelligence planners often find it difficult to resist excluding the private sector from their list of targets, especially in the field of cyberespionage, which carries with it the promise of easier access to corporate proprietary information. American intelligence policy is not immune to such pressures. Seasoned intelligence observers will recall the transatlantic tensions caused by the 1999 release of *Interception Capabilities 2000*, a report produced by the Office of the Director General for Research of the European Parliament. The report, which sparked an investigation by the European Union, listed repeated cases of alleged economic espionage conducted by the NSA in support of American companies competing against European firms for international contracts during the 1990s (Campbell 1999).

More recently, internal US government documents leaked by American defector Edward Snowden revealed an NSA cyberespionage technique called "supply-chain interdiction", in which the American signals intelligence (SIGINT) agency physically intercepts American-made network routers destined for foreign

buyers. The agency then allegedly implants the intercepted routers with communications beacons before repackaging them and shipping them to their intended consumers (Greenwald 2014). This unconfirmed revelation was viewed by observers as "underscoring the vulnerability of multinationals" who often act as unwilling facilitators of state-sponsored cyberespionage (Finkle, Menn and Viswanatha 2014). But, if true, the exposé also points to deliberate private-sector targeting by the NSA, and would seem to weaken Washington's protestations over China's alleged cyberespionage against American firms.

Further documents supplied by Snowden seem to suggest that the NSA spied on Huawei Technologies, a private Chinese telecommunications systems manufacturer, in an effort to compromise the security of the hardware it sells to its international customers. In fact, the leaked documents indicate that the American SIGINT agency appeared conscious of the fact that it was targeting a private entity, which, in accordance with Washington's official cyberintelligence doctrine, should be out of bounds for state intelligence agencies. In one internal memorandum, the NSA noted that "the [US] Intelligence Community structures are not suited for handling issues that combine economic, counterintelligence, military influence and telecommunications infrastructure from one entity" (Anon. 2014). Nor is the NSA the only American agency that appears to be pursuing intelligence targets rooted firmly in the private sector. The year before the Huawei revelations, the National Council of the Swiss Federal Assembly refused to consider national legislation designed to help Washington identify tax evaders employing Swiss banking services, after it emerged that the CIA had resorted to blackmail techniques in order to recruit a senior official of a Swiss bank as an agent (Bart 2013).

Is Financial Intelligence (FININT) a Legitimate Cyberespionage Target?

It would appear that America is not the only Western country to be actively incorporating private-sector companies on its list of cyberespionage targets. In 2014, *The New York Times* exposed a complex 2003 operation by the Australian Signals Directorate (ASD) against a law firm that represented the Indonesian state in a series of sensitive international trade negotiations (Risen and Poitras 2014). What is more, it appears that the intelligence gathered by the ASD was distributed to its American SIGINT partner, the NSA, at a period when Indonesia was engaged in trade negotiations with the US. According to a leaked ASD memorandum, the information shared with the NSA gave "highly useful intelligence for interested US customers" (ibid.). Australia, a trusted American intelligence partner, is also believed to have engaged in both human intelligence and cyberespionage operations against the government of East Timor in 2003, in an effort to acquire inside information about a crucial energy deal under the Certain Maritime Arrangements in the Timor Sea (CMATS) treaty (Fitsanakis 2013).

Were these legitimate cyberespionage targets? According to the view of the US Department of Justice, it would appear that they were not. And yet Western intelligence planners are repeatedly compelled to incorporate FININT in their operations in the service of protecting national security. In 2010, the government of Spain tasked the country's National Intelligence Center (CNI) to investigate alleged efforts by foreign financial speculators to destabilize the Spanish economy. According to media reports, the CNI was asked to probe supposed links between speculative moves in global financial markets and a series of damaging editorials "in the Anglo-Saxon media" about the state of the Spanish economy (Perez 2010). Later that year, the National Intelligence Service of Greece was reported to be collaborating with Spanish, Irish and Portuguese intelligence services in investigating a series of coordinated speculative attacks on money markets, most of which were alleged to have originated from London and Washington (Georgiopoulos 2010).

There is evidence that, along with European intelligence agencies, the US Intelligence Community is aggressively pursuing FININT targets of its own. In the midst of the global financial crisis of 2009, the then US Director of National Intelligence, Dennis Blair, warned that the financial crisis was the US Intelligence Community's "primary near-term security concern" (Mazzetti 2009), while his Office issued a public warning to China that Washington would consider any attempts to sell US Treasury bonds an act of "financial warfare" (Fitsanakis 2009). Soon afterwards, the CIA's Directorate of Intelligence launched a recruitment program aimed at hiring investment bankers as part of "a national strategy […] to deal with [...] financial issues" (Ryssdal 2009). Two years later, the Intelligence Advanced Research Projects Activity, the US Intelligence

Community's research arm, began developing tools to help intelligence analysts "quickly and accurately assess petabytes of complex anonymized financial data". These tools would reportedly be able to "spot indicators of market behavior, find relationships between seemingly unrelated transactions across hundreds of global markets, and provide insight into specific events and general financial trends" (Groeger 2011).

Conclusion: Blurred Targeting in Cyber Operations

American conceptions of intelligence-targeting in cyber operations are arguably influenced by the country's cultural practices, which tend to vividly distinguish between state and private economic activity. In contrast, Chinese macroeconomic attitudes can be said to favor the supremacy of state authority and national security over the requirements of private industry. It is in that context that Beijing's dismissive attitude against Washington's private-public intelligence distinction must be examined. Moreover, American protestations of Chinese cyberespionage against US firms are considerably weakened by recent revelations of NSA cyber operations targeting foreign economic interests. It can be argued that there are clear conceptual and operational differences between, on the one hand, state-sponsored cyber operations aimed at protecting national security and, on the other hand, cyber operations seeking to further narrow business interests. Those of us who favor the observation of legal standards in international relations cannot but admire Washington's vocal efforts to place clear distinctions between the two. But before American intelligence planners can claim the moral high ground in that discussion, Washington must first ensure that it observes its own standards, not only in the realm of counterintelligence, but also in offensive cyberespionage activities.

Bibliography

Aid, M.M. (2013) "Inside the NSA's Ultra-Secret China Hacking Group", *Foreign Policy*, 10 June.

Anonymous (2014) "NSA Spionierte Chinas Staatsführung und Konzerne aus", *Der Spiegel*, 22 March.

Bart, K. (2013) "Swiss parliament stalls progress of US tax deal", Reuters, 18 June.

Campbell, D. (1999) "Interception Capabilities 2000", Directorate for Research, European Parliament, Brussels, Belgium, April.

Cheng, D. (2013) "Information Dominance: PLA Views of Information Warfare and Cyberwarfare", Chaire de Cyberdéfense et Cybersécurité, July.

Finkle, J., Menn, J., and **Viswanatha, A.** (2014) "US accuses China of cyber spying on American companies", Reuters, 19 May.

Fitsanakis, J. (2009) "US Issues Financial Warfare Warning", intelNews, 20 February.

Fitsanakis, J. (2012) "US cybersecurity posture is not purely defensive", intelNews, 28 May.

Fitsanakis, J. (2013) "Australia tries to stop ex-spy from testifying in international court", intelNews, 05 December.

Georgiopoulos, G. (2010) "Greek intelligence probes bond speculators", Reuters, 19 February.

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, Metropolitan Books, New York, NY.

Groeger, L. (2011) "US Spies Totally Confused by Wall Street, Too", Wired, 22 August.

Indictment Memorandum (2014) *United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui*, United States District Court for the Western District of Pennsylvania, May 1.

Mazzetti, M. (2009) "Global Economy Top Threat to US, Spy Chief Says", *The New York Times*, 12 February.

Medeiros, E.S., **Cliff, R.**, **Crane, K.**, and **Mulvenon, J.C.** (2005) *New Direction for China's Defense Industry*, RAND Corporation, Santa Monica, CA.

Perez, C. (2010) "El CNI investiga las presiones especulativas sobre España", *El País*, 14 February.

Riley, M., and **Lawrence, D.** (2012) "Hackers Linked to China's Army Seen From EU to DC", Bloomberg, 26 July.

Risen, J., and Poitras, L. (2014) "Spying by NSA Ally Entangled US Law Firm", *The New York Times*, 15

February.
Ryssdal, K. (2009) "Investment bankers: CIA wants you" National Public Radio, 28 May.
Sanger, D.E. (2014) "With Spy Charges, US Draws a Line That Few Others Recognize", *The New York Times*, 19 May.
Schmidt, M.S., and **Sanger, D.E.** (2014) "5 in China Army Face US Charges of Cyberattacks", *The New York Times*, 19 May.
Taylor, A. (2014) "Edward Snowden makes it easier for China to dismiss new spying charges", *The Washington Post*, 19 May.