

Tony Boyles

Chinese 375: China Overview

Dr. Yawei Liu

Sunday, August 5, 2007

Chinese Intelligence

Analysts in the West have long predicted that China would command greater and greater sway on the international stage. China is the only nation to merit annual reviews of military activity to the United States Congress. The United States, in particular, views China's trend of rapid economic and military growth as threatening to US hegemony, although Chinese officials regularly deny that China has hegemonic ambitions. Despite this great interest in China, the United States has largely neglected what could be one of the most important aspects of the Chinese ascent—intelligence. FBI Assistant Director for Counterintelligence, David Szady, has remarked that China represents “the biggest threat to the United States today.” (Solomon 2005) Thus, it is strange that very little information is available about the Chinese intelligence services, compared to the substantial body of knowledge surrounding last century's Soviet, Nazi, and Fascist intelligence services. Even so, there is enough information to construct a rudimentary picture of modern Chinese intelligence operations.

Human Intelligence Overseas

Chinese espionage is handled predominantly by two agencies: the Ministry of State Security (MSS) and the People's Liberation Army (PLA), specifically the PLA's Second Department of the General Staff Department. While espionage is a familiar difficulty to any intelligence analyst, the Chinese modus operandi of espionage provides some fresh practical difficulties for western counterintelligence efforts. Following the Soviet model, Chinese intelligence agencies employ fewer trained operatives who recruit a greater number of agents. The MSS or PLA rely predominantly on recruiting students planning to study abroad, businessmen abroad for short meetings, academics overseas for conferences, or other travelers planning to spend very little time outside of Chinese borders to collect their information. They may be asked to retrieve specific pieces of information (e.g. schematics of Apache helicopter rotors), or may just be directed to gather all available information in a body of relevant study (e.g. anything about Apache

helicopters). These agents usually have no intelligence training, no experience in clandestine activities, and so are relatively susceptible to surveillance and capture upon suspicion of espionage activity. However, many agents successfully return with very small pieces of information, some of which may be permitted for export anyway. (Eftimiades 1998)

The trouble for foreign counterintelligence agencies is charging the visiting Chinese aliens with espionage, when the amount of information is practically negligible compared to the body of more highly guarded information that could have been compromised. By having many hundreds of such agents popping in and out of foreign nations each year, the Chinese agencies can accurately piece together large bodies of information, and rely on scientists or analysts (depending on the variety of information) to fill in the blank spots. (Lilley 2003) A handful of moderate to high profile cases break this mold, though they are few and farther between than stories of catching Soviet spies.

The one known counterexample, a single agent collecting a massive amount of information, is the story of Katrina Leung. Leung, a Chinese native who moved to the United States while in high school, was recruited by the FBI during her Master's degree study. (Wikipedia Contributors) She worked as a double agent, penetrating deep into PRC diplomatic circles. However, she had had multiple long-standing affairs with multiple FBI agents, which she used to make copies of classified US government documents. The PRC began collecting information from Leung, which she claimed she had been coerced into giving, her secret status as a double-agent having been negotiated by a Chinese operative. She was indicted for "Unauthorized Copying of National Defense Information with Intent to Injure or Benefit a Foreign Nation." The charge was dismissed on the grounds of prosecutorial misconduct, and she was subsequently charged with filing an illegal tax return (which had turned up in the investigation), and sentenced three years probation, in addition to a monetary fine and community service. (WGBH 2004) It is estimated that her betrayal of the FBI, in particular the agents with whom she had been sexually involved, had rendered twenty years worth of intelligence on China (the entire since she had been recruited) useless. (Lilley 2003)

The Leung case reveals another important trait of Chinese intelligence practices. The Chinese favor the opportunity of recruiting persons of Chinese heritage whenever possible, with the expectation that they will have some allegiance to the PRC. (Eftimiades 1998) As though the task of convicting Chinese

agents wasn't difficult enough for the US Department of Justice, keeping track of probable targets of the Chinese government leads to charges of racism. (Wang 1999, Zia 1999) This was never more true than in the case of Wen Ho Lee, an American (born in Taiwan) computer scientist working for Los Alamos National Laboratories, who was falsely accused of espionage in 1999 and held without the presentation of adequate evidence for conviction. (Wang 1999) Despite having never been a Chinese citizen, he was suspected of spying for the PRC because of casual meetings he'd had with Chinese nuclear scientists. The investigation did reveal he had downloaded some 40 classified documents to a public computer terminal at UCLA, though his reason for doing so is unknown. His arrest caused a massive outcry in the Asian-American community. (Wang 1999, Wikipedia Contributors) The US government was (perhaps not entirely incorrectly) accused of overt racism against persons of oriental descent (Zia 1999).

Besides this conventional agent-recruiting model of intelligence collection, Nicholas Eftimiades described two other methods of acquisition in his 1998 address to the Joint Economic Committee of Congress. In the first, the Chinese government (via a state-run firm) simply purchases American companies with access to the desired information. While this does secure the required information (legitimately), it accomplishes the task of intelligence collection with all the finesse of a herd of stampeding three-legged elephants. It is a blatant revelation to the originating government what information the Chinese are after, and depending on the government's decision to permit the transaction, the value of the acquisition. In the second, more discreet method, the PRC recruits agents to set up puppet companies (which may perform legitimate business transactions), which, again, purchase American companies with access to the desired information. (Eftimiades 1998, Solomon 2005)

This last method was recognized by Former Ambassador to China, James Lilley (who was also previously a CIA operative working in China), as the means by which the Chinese worked to obtain nuclear secrets from the US. By setting up something as innocuous as a wire manufacturing firm, the Chinese built a front with which they placed bids to purchase other American companies with intellectual rights (or at least access) to useful information concerning nuclear weaponry and other US military technology. (Lilley 2003)

Eftimiades suggests that the most effective agents are recruited not in the provinces of the People's Republic of China (PRC), but in Hong Kong. While Hong Kong was under British rule, it was convenient for the PRC intelligence agencies to recruit agents there. Citizens of Hong Kong were effectively citizens of Her Majesty's Empire, and therefore if caught and prosecuted abroad for espionage activities, China could not be held responsible. The fact that little has changed in Hong Kong since its return to the PRC has allowed for the maintenance of this now defunct safeguard. Hong Kong also still provides a favorable domain for the aforementioned puppet companies to make purchase inquiries to American firms, because of its maintenance of a progressive government on good terms with the United States.

Chinese espionage maintains a fairly low profile on the global scale, because common targets for Chinese agents are perceived as low-threat by the originating country. Frequently pursued information includes intermediate military devices and commercial technology. This targeted information provides further difficulty for prosecution of spies, because such information is always prioritized after cutting-edge, high-tech equipment. (Lilley 2003)

Domestic Intelligence

Unlike their American equivalents (NSA, FBI, etc...), the Chinese security services still operate under an authoritarian regime. This provides the Chinese with advantages in domestic surveillance. Instead of constant congressional oversight, the Chinese spy agencies are given free reign to maintain comprehensive surveillance of the country. In spite of Western ideals of privacy and security, this quantity of information provides substantial advantages. While the FBI cannot legally keep "files" on every US citizen, the MSS both can and may very well do so (although this claim can be neither supported nor refuted). This means that the MSS may have instant access to information on almost anyone who is perceived as a threat, or even marginally related to a possible threat to national security, without having to do any substantial background research or real-time surveillance, both of which can be a time-consuming and bureaucratically frustrating process in the United States.

Most domestic operations have the same targets as foreign operations. Visiting academics, businesspeople and government officials are all routinely subject to recruitment attempts, requests to divulge information to the Chinese government or to use their status to obtain information with the intent of

doing so. Additionally, recruited agents may be asked to use influence overseas to sway events to favor the PRC's agenda. (Eftimiades 1998)

Electronic Intelligence

China's burgeoning commercial aerospace industry provides an ideal platform for expanding its already formidable Signals Intelligence (SIGINT) capabilities. China maintains the largest SIGINT operation in the Orient, with mobile coverage stemming from PLA Naval vessels listening specifically for American radio transmissions. (Eftimiades 1998) Additionally, new satellite fleets provide China with the opportunity for live photoreconnaissance all over the world. Whether the Chinese have taken the opportunity to make such use of the commercial satellites launched for extra-national clients, I cannot say with certainty or verification. However, for the Chinese not to do so would be squandering a great opportunity.

Conclusion

While China's growing power drives China's growing thirst for knowledge, America should maintain vigilance about protecting its secrets. It would be naïve to claim that there is a simple solution to plugging all the holes in America's classified community, but it would be even more naïve to suggest that the system is sufficient as it is. There will always be another leak, another gap. The intelligence and military agencies need to do everything possible to end such dangers as quickly as possible. In the case of specifically Chinese intelligence collection, this especially includes increasing counterintelligence efforts. Quietly feed the Chinese government incorrect information, and catch them when they act on it. This may not be so simple, and will always vary from case to case. However, if emerging threats are not met with due expediency, the United States is bureaucratically incapable of defending itself, and therefore has already lost its claim to hegemony. Whether the Chinese chose to step up to the title (and adjoining responsibilities) in America's wake is up to them, but their trend for development and enormous speed with which they achieve advances suggests they will.

References

Eftimiades, Nicholas. 1998. Statements before the Joint Economic Council of the United States Congress

Concerning Chinese Intelligence Collection Operations, May 20, in Washington D.C.

Lilley, James. [unaired] Interview. PBS Frontline: From China with Love. June 4, 2003.

<http://www.pbs.org/wgbh/pages/frontline/shows/spy/interviews/lilley.html>

Solomon, Jay. 2005. "FBI Sees Big Threat from Chinese Spies; Businesses Wonder". *Wall Street Journal*,

August 12, Online Edition, accessed through YaleGlobal Online.

<http://yaleglobal.yale.edu/article.print?id=6140>

Wang, Ling-chi. 1999. "Spy Hysteria". *AsianWeek* Volume 20, Number 30. March 25.

http://www.asianweek.com/032599/feature_commentary.html

WGBH. 2004. PBS Frontline: From China with Love.

<http://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/> (accessed July 29, 2007)

Wikipedia contributors, "Chinese intelligence activity in other countries," *Wikipedia, The Free*

Encyclopedia, <http://en.wikipedia.org/w/index.php?>

[title=Chinese_intelligence_activity_in_other_countries&oldid=115337334](http://en.wikipedia.org/w/index.php?title=Chinese_intelligence_activity_in_other_countries&oldid=115337334) (accessed August 1, 2007).

Wikipedia contributors, "Katrina Leung," *Wikipedia, The Free Encyclopedia*,

http://en.wikipedia.org/w/index.php?title=Katrina_Leung&oldid=145882464 (accessed August 2, 2007)

Zia, Helen. 1999. "I'm Not a Spy, Are You?" *AsianWeek* Volume 20, Number 41.

http://www.asianweek.com/061099/opinion_roundtable.html