# Testimony before the U.S.-China Economic and Security Review Commission: Chinese Human Intelligence Operations against the United States

*Peter Mattis*
*Fellow, The Jamestown Foundation*
*June 9, 2016*

China's intelligence services are among the world's most active against the United States, but the Chinese approach to human intelligence (HUMINT) remains misunderstood. Observers have conflated the operations of the intelligence services with the amateur clandestine collectors (but professional scientists/engineers/businesspeople) who collect foreign science and technology. The Chinese intelligence services have a long professional history, dating nearly to the dawn of the Chinese Communist Party, and intelligence has long been the province of professionals. The intelligence services were not immune to the political purges and the red vs. expert debates, and the Cultural Revolution destroyed much of the expertise in clandestine agent operations.[1] As China's interests abroad have grown and the blind spots created by the country's domestic-based intelligence posture have become more acute, the Chinese intelligence services are evolving operationally and becoming more aggressive in pursuit of higher-quality intelligence.

* * *

The principal intelligence services conducting HUMINT operations, both clandestine and overt, against the United States are the Ministry of State Security (MSS) and Joint Staff Department's Intelligence Bureau (JSD/IB) in the People's Liberation Army (PLA). Prior to the military reforms announced in November 2015, the latter was known as the General Staff Department's Second Department (commonly abbreviated 2PLA). Because the full ramifications of the PLA's reform effort have unclear implications for intelligence, the testimony below will reflect what was known about 2PLA rather than the JSD/IB, unless specifically noted.

The MSS consists of the central ministry, provincial state security departments, and municipal/county state security bureaus. At least the central ministry and the provincial departments conduct clandestine agent operations, though only a few provincial departments are routinely active in collecting on the United States. The others exploit targets of opportunities passing through their jurisdictions and occasionally pursue them outside of their ostensible turf.

The 2PLA conducted both clandestine and overt HUMINT operations through case officers operating under traditional covers and defense attaché offices, respectively. The clandestine collectors operate from liaison offices in China, official missions overseas, and non-official cover platforms abroad. It is believed that there are five liaison offices in Beijing, Shanghai, Shenyang, Guangzhou, and Tianjin, which as the principal stations for 2PLA's clandestine agent operations.[2]

---

[1] David Ian Chambers, "Edging in from the Cold: The Past and Present State of Chinese Intelligence Historiography," *Studies in Intelligence*, Vol. 56, No. 3 (September 2012), pp. 31–46.

[2] Kan Zhongguo, "Intelligence Agencies Exist in Great Numbers, Spies Are Present Everywhere; China's Major Intelligence Departments Fully Exposed." *Chien Shao* (Hong Kong), January 1, 2006.

Chinese HUMINT operations use case officers as well as other collectors operating under a wide variety of covers and different operational modes to collect intelligence both overtly and clandestinely. Here are five well-documented ways in which Chinese intelligence, both civilian and military, collect intelligence:[3]

- Diplomats, defense attachés, and journalists form the cadre of embassy-based case officers under official cover. Mostly these collectors pursue internal security targets (which may not be scrutinized by local counterintelligence/security services), interviews commensurate with their cover, and other open source information. Only recently have these officers appeared to engage in clandestine agent operations.
- Seeding operations involve recruiting an individual and then trying to direct them into positions where they can collect valuable intelligence. These kind of operations originated in the Chinese Revolution and have remained a staple approach with a very mixed record of success.[4]
- Academics and scholars have been familiar feature of China's public face for intelligence, through such august organizations as the MSS bureau known as the China Institutes of Contemporary International Relations. For the most part these organizations do nothing more nefarious than open source collection and elicitation through interviews. Occasionally, however, case officers covered as academics have run clandestine agent operations.
- Domestically, local government offices, such as numbered but otherwise anonymous municipal offices (e.g. the Shanghai Municipal Government Office No. 7), are frequently used to create a fig leaf between intelligence officers and those with whom they are in contact.
- Business people at home and abroad also are used as case officers, collaborators, and principal agents who develop spy networks themselves.

Other Chinese bureaucracies are involved in covert action, such as political influence, and intelligence, such as monitoring ethnic Chinese and minorities; however, their role in targeting the U.S. Government directly is limited. These include the Ministry of Public Security, Liaison Department of the PLA's Political Work Department, the party's United Front Work Department, and the Overseas Chinese Affairs Office. Though these organizations and others do represent a threat to U.S. interests, their activities are beyond the scope of this testimony and require a different kind of discussion.

Similarly, the largest portion of China's efforts to acquire foreign scientific and technological information is not run from the intelligence services, but a specialized bureaucracy for cataloguing and disseminating technical information.

Ultimately, the activities of the intelligence services are governed by the Politburo Standing Committee and the Central Military Commission. Beneath these two bodies, the Political-Legal Affairs Commission system and the Joint Staff Department have direct responsibilities for the intelligence services. The Minister of State Security and the JSD deputy chief with responsibility for intelligence and foreign affairs both sit on the relevant leading small groups, including, at least, foreign affairs, Hong Kong & Macao affairs, Taiwan affairs, countering evil cults, and preserving stability. While the intelligence services may only provide information to these groups, presumably they receive guidance

[3] For a lengthier treatment, see, Peter Mattis, "Five Ways China Spies," *The National Interest*, March 6, 2014.

[4] "Shriver Case Highlights Traditional Chinese Espionage," *Jamestown Foundation China Brief*, Vol. 10, No. 22, November 5, 2010

about important intelligence requirements when these bodies deliberate. The State Security Committee (sometimes referred to as China's National Security Council) also may oversee intelligence operations; however, the membership and functioning remains mostly unknown and its focus may be more on protecting the party-state than guiding foreign and national security policy.[5]

**What Do the Chinese Mean by Intelligence?**

Most writing about Chinese intelligence suggests the Chinese conduct intelligence in a completely different way while avoiding traditional methods of clandestine agent operations. Variously called the "grains of sand," "mosaic," or "vacuum-cleaner" approach to intelligence, the conventional perspective holds that Chinese intelligence relies on amateur collectors with little clandestine tradecraft, does not exploit negative vulnerabilities like venality, and collect little bits of information that can be assembled later in China. This view fails in the face of Chinese intelligence history, concepts, and practices beginning from the beginning of CCP intelligence in 1927.[6]

One of basic mistakes foreign analysts have made about the Chinese is to say that the Chinese make no meaningful distinction between intelligence and information, leading to broad-based collection of information almost irrespective of specific intelligence requirements. Former FBI Special Agent I.C. Smith and intelligence historian Nigel West wrote "In the Chinese language, there is no real distinction between 'intelligence' and 'information' in common usage, and there is no specific term for 'intelligence-gathering.' *Qingbaosou* refers to 'information-gathering,' an essential ingredient of the mammoth intelligence gathering effort directed at Western countries."[7] From a purely academic perspective, two British intelligence scholars stated "traditionally, the Chinese vocabulary has not distinguished between 'intelligence' and 'information.' Accordingly, China's agencies operate different than other espionage organizations by collecting large quantities of open information."[8]

At least since the early 20th Century, the Chinese have defined intelligence in ways recognizable in Western terms. The common element is information serving a specific purpose and in support of decisionmaking. One of the most commonly used Chinese definitions of intelligence comes from the U.S.-trained rocket scientist Qian Xuesen, who also played an important role in systematizing the collection of foreign scientific knowledge. Dr. Qian stated "Intelligence is the knowledge necessary to solve a specific [decision-making] problem. This view embodies two concepts. One is that [intelligence] is knowledge, not false, nor random. And the other? It is for a specific requirement and also for a specific question, so timeliness and relevance are very important …"[9] Numerous PLA publications

---

[5] David M. Lampton, "Xi Jinping and the National Security Commission: Policy Coordination and Political Power," *Journal of Contemporary China*, Vol. 24, No. 95 (2015), 759–777; Samantha Hoffman and Peter Mattis, "Inside China's New Security Council," *The National Interest*, November 21, 2013.

[6] For a full accounting of these problems, see, William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge, 2013), 186–216; Peter Mattis, "Assessing Western Perspectives on Chinese Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 25, No. 4 (Fall 2012), 678–699.

[7] I.C. Smith and Nigel West, *Historical Dictionary of Chinese Intelligence* (Lanham, MD: The Scarecrow Press, 2012), 220.

[8] Richard J. Aldrich and John Kasuku, "Escaping from American Intelligence: Culture, Ethnocentrism, and the Anglosphere," *International Affairs*, Vol. 88, No. 5 (September 2012), 1020.

[9] Chen Jiugeng, "Guanyu qingbao he xinxi [Regarding Intelligence and Information]," *Qingbao zazhi* (Journal of Information) 19, No. 1 (January 2000), 4–6.

and intelligence histories reinforce the view that intelligence is specially-collected, -processed, -analyzed, and -disseminated information for policymakers and other decision makers.

Intelligence also is a form of clandestine or covert power. The inclusion of intelligence warfare as one of the four components of information warfare—the other three are network warfare, electromagnetic warfare, and political/psychological warfare—is rooted in China's strategic tradition dating back to the *Sunzi Bingfa*.[10]

**China's Evolving Approach to HUMINT**

The best word to describe China's changing approach to intelligence collection in the last fifteen years is aggressiveness. Elements of this aggressiveness have risen and then faded, such as the very direct use of sexual entrapment and blackmail.[11] Other parts of this aggressiveness remain. As China's intelligence services have demonstrated greater willingness to pay human agents, they have become impatient for results. Most analyses of Chinese tradecraft suggested they used long development phases and may never have reached the stage for formal recruitment. Based on this analyst's interviews with individuals and foreign intelligence services, the Chinese are perfectly willing to pitch a potential source within one to three meetings including an initial spot payment and promise of future remuneration.

Perhaps the most notable specific development has been the recruitment of clandestine agents abroad by case officers posted outside China. The first example is Taiwan army general Lo Hsien-che, who the Taiwanese authorities arrested in early 2011. Chinese intelligence, probably 2PLA, recruited Lo sometime during his posting as a military attaché in Bangkok in the early 2000s. There is nothing in the public record to suggest General Lo was ever handled at meetings taking place inside China, and his primary case officer (though not the necessarily the one who recruited him) was covered as a Thailand-based businesswoman with legitimate Australian citizenship.[12] The second example is Baibur Maihesuti, a Uighur living in Sweden and who the Swedish authorities arrested in 2009 for spying on fellow Uighurs living outside China. Chinese intelligence, most likely the MSS, used two case officers: one covered as a journalist for an official Chinese paper and that other covered as a diplomat in the embassy.[13]

It is possible, if not probable, that Chinese intelligence recruited agents in ethnic Chinese overseas communities, Chinese ethnic minorities, and Taiwanese, but U.S. and other local counterintelligence services did not focus on such activities. In democracies, such activities may not even necessarily break the law. China's intelligence services first and foremost have a responsibility for the protecting the

---

[10] Ralph Sawyer, "Subversive Information: The Historical Thrust of Chinese Intelligence", in Philip H.J. Davies and Kristian Gustafson, eds., *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (Washington, DC: Georgetown University Press, 2012), 29–48.

[11] This culminated in the suicide in 2006 of a Japanese code clerk posted at the Shanghai Consulate. See, Justin McCurry, "Japan Says Diplomat's Suicide Followed Blackmail by China," *The Guardian*, December 20, 2005; Reiji Yoshida, "China Slammed Over Diplomat's Suicide," *Japan Times Online*, December 29, 2005.

[12] Peter Mattis, "Taiwan Espionage Cases Highlight Changes in Chinese Intelligence Operations," *Jamestown Foundation China Brief*, Vol. 11, No. 12, July 1, 2011.

[13] Paul O'Mahony, "Pensioner Indicted over China Spy Scandal," *The Local* (Sweden), December 15, 2009; "Refugee Spy Remanded into Custody," *The Local* (Sweden), 6 June 2009; Paul O'Mahony, "Security Police Arrest 'Refugee Spy'" *The Local* (Sweden), June 4, 2009; "Sweden Jails Uighur Chinese Man for Spying," *Reuters*, March 8, 2010.

party-state and this is why what some analysts have called "ethnic targeting" occurred. But as China's global interests beyond state security have expanded, Chinese intelligence must shift its operational footing to protect sources who receive a higher degree of scrutiny and accept a greater risk to their careers and livelihoods. A government official, contractor, or interlocutor often needs clandestine tradecraft as reassurance that a foreign intelligence service for whom they spy can take care of them. The pressure to support decisionmakers should be moving Chinese intelligence, both 2PLA and MSS, toward more sophisticated clandestine tradecraft, including such techniques as covert communications, overseas surveillance teams, using agents to enable access to closed networks or provide other technical collection, etc.

The publicly-available data on military intelligence and MSS operations is insufficient to judge the distinctions, if any, between the two sets of intelligence services. Both seem to use more than one intelligence officer whenever handling a source, and both rely heavily on operations conducted inside China. The domestic base for operations often means that what counterintelligence officials see are principle agents, not professional intelligence officers, trying to operate and find sources overseas. It can look amateurish because it is, and the truly professional relationship often remains hidden from view unless a principle agent decides to cooperate after his arrest.

The distinctions between the U.S. and Chinese approaches to HUMINT probably are questions of specific techniques and comfort operating overseas. There is no recorded example of the Chinese using a dead drop, i.e. leaving messages, money, or other items in specific place to pass between case officer and agent. However, the Chinese have used live drops, i.e. a signal is sent to trigger a meeting where items are passed between officer and agent. The number of examples of the Chinese identifying and recruiting an agent outside China are few and relatively recent, suggesting that conducting clandestine argent operations abroad remains tightly controlled.[14]

**Chinese HUMINT in Three Cases**

The U.S. espionage cases centered around Larry Wu-Tai Chin, Kuo Tai-Shen, and Glenn Duffie Shriver offer a window into the conduct of Chinese clandestine agent operations. They demonstrate China's capability and highlight the Chinese use of the traditional tools of espionage that are shared among most of the world's intelligence services involved in the HUMINT business.

Larry Wu-Tai Chin was recruited by Chinese intelligence while he was working for the U.S. mission in Nanjing prior to the formation of the PRC in 1949. Chin continued to report to Chinese intelligence for almost forty years until his arrest in 1985. For most of this time, he worked as a translator in various capacities, such as for the U.S. Army in Korea helping with prisoner interrogation and later at the Foreign Broadcast Information Service. Chinese intelligence may have paid him over a $1 million. Throughout the operation, Chin made several surreptitious trips into China for meetings and to be recognized for his reporting. When Chin was ready to pass documents onward, he would mail a letter to an accommodation address in Hong Kong and that would signal a follow on meeting at a preset time in Canada, where he would pass the documents to a courier.[15]

---

[14] Peter Mattis, "The New Normal: China's Risky Intelligence Operations," *The National Interest*, July 6, 2015.

[15] Ronald Ostrow, "Accused Spy Chin Faces New Charges," *Los Angeles Times*, January 3, 1986; Chitra Ragavan, "A Spy Who Changed History," *U.S. News and World Report*, November 20, 2003; Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994), 32–34; Bill Gertz, "Former FBI Agent Cites Penetration of CIA by China," *Washington Times*, December 15, 2004.

Kuo Tai-Shen was a naturalized U.S. citizen and Louisana-based furniture salesman who was recruited in the 1990s during one of his frequent business trips to mainland China. Although Kuo had access to some political circles in Taiwan through his marriage, he had no direct access to U.S. Government information. His handlers in 2PLA encouraged to develop contacts in the U.S. Department of Defense, and he successfully recruited James Fondren and Gregg Bergersen to spy for China. Fondren was a retired military officer who returned to work for the U.S. Pacific Command office in Washington, DC, after working as a consultant whose primary client was Kuo for whom he wrote assessments of U.S. policy. Bergersen worked for the Defense Security Cooperation Agency, and he provided classified information to Kuo on U.S. arms sales to Taiwan thinking that Kuo worked for Taipei. Kuo persuaded Bergersen that they should set up an arms export business once he retired to sell military-related components to Taiwan. 2PLA met Kuo exclusively inside China, but did provide him with courier and tried to teach him how to communicate discreetly via email.[16]

Glenn Duffie Shriver was a recent university graduate in China when he was spotted by Chinese intelligence, probably the MSS, through an essay contest on U.S.-China relations. The contest was a gimmick intended to draw out individuals who might have long-term intelligence value to Chinese intelligence. Shriver met several times with a younger case officer and at least one or two others. He was arrested in Summer 2010 on his third attempt to join the U.S. national security establishment, this time at the Central Intelligence Agency. He had applied twice previously to the U.S. Department of State, but failed to pass the foreign service examination with sufficiently high marks. For his attempts to join, Shriver was $70,000. Shriver never met Chinese intelligence officers outside of China, and he used only email rather than any special equipment for communication.[17]

These cases highlight a few points of Chinese tradecraft that are worth noting. First, the agents recruited by Chinese intelligence spent substantial amounts of time in China. Second, Chinese intelligence demonstrated operational tradecraft and exploited traditional motives like greed. Third, potential Chinese agents do not need to have direct access to sensitive or desired materials, just a willingness to make attempts to acquire them.[18] Fourth, Chinese intelligence handled all of these agents from within China.

**Chinese Effectiveness in Human Intelligence Collection**

Without the benefit of inside information from the Chinese intelligence services, judging Chinese effectiveness and success involves speculating off the basis of a small percentage of Chinese espionage cases. These cases also may not represent the most sophisticated operations, and China's intelligence

---

[16] "Defense Department Official Charged with Espionage Conspiracy," Department of Justice Press Release, May 13, 2009; Jerry Markon and Carrie Johnson, "Former Pentagon Official Pleads Guilty to Espionage," *Washington Post*, April 1, 2008; and *United States v. Tai Shen Kuo, Gregg William Bergersen, and Yu Xin Kang*, Affidavit before the US District Court for the Eastern District of Virginia (2008).

[17] David Ashenfelter and Lori Higgins, "Former Grand Rapids Man Pleads Guilty to Spying for China," *Detroit Free Press*, 22 October 2010; "Michigan Man Pleads Guilty to Attempting to Spy for the People's Republic of China," Department of Justice Press Release, October 22, 2010.

[18] This particular feature is seen frequently in Taiwan's espionage cases, where a retired official, businessperson, or traveler is recruited to cultivate his friends, family, and former classmates/colleagues to collect intelligence. See, Peter Mattis, "China's Espionage Against Taiwan (Part I): Analysis of Recent Operations," *Jamestown Foundation China Brief*, Vol. 14, No. 21, November 7, 2014.

services have demonstrated the ability to handle a clandestine source for more than a decade. With these caveats aside,

The Chinese intelligence services benefit enormously from the resources available domestically to surveil targets, access their possessions, and exploit their personal electronics. Instead of days past where physical surveillance was required to evaluate visitors to China, the services can bring to bear advanced technical resources to follow individuals and find out who they are through their electronics without the manpower requirements of physical surveillance.

Perhaps the strongest part of China's HUMINT operations are the efforts to collect open source intelligence. The think tanks run by Chinese intelligence, such as the China Institutes of Contemporary International Relations (CICIR) and the China Institute for International and Strategic Studies (CIISS), host a steady stream of foreign visitors, regularly send delegations abroad, and even post their analysts abroad on visiting fellowships. The Internet may have made gathering reports and publications much easier, but these direct person-to-person interactions offer another avenue for open source collection that often is not considered in the U.S. context. Foreign interlocutors can provide the gossip of their home country's policy community (useful for targeting), background information that never makes newspapers or reports, and occasionally more direct intelligence reporting.

The shortcomings to how China conducts clandestine HUMINT operations are threefold: the domestic base creates blind spots; the legacy of the Cultural Revolution damaged Chinese clandestine tradecraft; and wide variations in the training of Chinese case officers.

The domestic base for Chinese operations probably creates blind spots in the intelligence support available to Chinese decisionmakers. The kinds of sources that China can recruit easily are best positioned to report on their country's China-related affairs. Foreign specialists on China and, to a lesser extent, Asia travel to China, but those focused on other geographical areas do not necessarily go to China with the frequency or duration that would make a recruitment possible.

To date, China's clandestine tradecraft probably does not rate among the world's most sophisticated at least with any consistency across a large number of intelligence officers. The Cultural Revolution and previous political movements purged (or killed) many of the Chinese case officers with professional knowledge, experience, and training in assessing, developing, recruiting, and handling clandestine sources, especially foreigners. The close compartmentation of sources restricted knowledge of HUMINT operations and left case officers vulnerable to charges of espionage for their contacts with foreigners.[19] Such tradecraft is important for handling sensitive sources who place their lives in the hands of their case officer. For some time now, the Chinese intelligence threat could best be described as based on the scope, scale, and potential impact of these operations, not operational skill.

Although military intelligence is more centralized, the MSS is a far-flung, sprawling operation with a central headquarters, provincial departments, and municipal/county bureaus. At least the center and provincial departments run operations against foreign targets. Each is responsible for inducting new officers, mirroring the rest of the government. Local universities vary substantially in their quality and presumably this creates unevenness across the ministry's personnel. With little indication of

[19] Chambers, "Edging in from the Cold."

centralized training program for new MSS officers from the ministry headquarters to the state security bureaus, the MSS appears to lack a way to ensure operations are conducted with a minimum level of competence.

This helps explain why so many China's intelligence successes have involved ethnic Chinese living overseas. Case officers with little foreign exposure, living inside China, cannot be expected to routinely approach potential foreign sources in the appropriate way. As former British Secret Intelligence Service director-general Richard Dearlove observed, human agents can only be recruited when "asked in the right way, by the right person, at the right time."[20]

**Challenges and Recommendations for Countering Chinese Human Intelligence Operations**

No one outside the U.S. Government, especially the Central Intelligence Agency, Federal Bureau of Investigation, and National Security Agency, can answer whether U.S. counterintelligence is up to the task of countering Chinese human intelligence operations. The biggest complaint by former U.S. counterintelligence officials is that the amount of effort the United States expends against the Chinese pales in comparison to the effort Beijing expends to collect intelligence on the United States.[21]

One of the biggest U.S. vulnerabilities is young people in or recently graduated from university who go to China for extended stretches of time for study, research, or work. China's intelligence services have demonstrated repeatedly over the last three decades the willingness to recruit students and others inside China who might be directed to join the U.S. Government in the hopes of future access. Americans generally lack basic security awareness and have little reason to gain it as they grow up. Appeals to an optimistic future of U.S.-China relations, being a friend of China, and mutual understanding are easy pathways to engage the unwary and naïve. Programs, like the National Security Education Program scholarships, also highlight U.S. students who will pursue a career in the national security and foreign policy establishment, saving Chinese intelligence the effort of identifying them.

The loss of Office of Personnel Management (OPM) files on millions of Americans with a security clearance and their associate foreign national contact data offers China something that it has not possessed previously on the U.S. national security establishment: a database of who's who. This data allows China's intelligence services, or at least the MSS, to validate the bona fides of potential U.S. sources, plan operational approaches through friends and acquaintances, and systematically approach Americans who hold or previously held security clearances. Having such a vast database of names and relationships is one of the ways in which Chinese intelligence has been able to sustain a high tempo of operations against Taiwan. Knowing who is potentially valuable allows them to exploit the constant stream of visitors from across the strait. The OPM data makes it possible to identify persons of interest as soon as they apply for a visa or enter the country[22]

---

[20] Sir Richard Dearlove, "The Plot Thickens," *Financial Times*, September 2, 2007.

[21] For example, Jeffrey Bliss, "China's Spying Overwhelms U.S. Counterintelligence," Bloomberg, April 2, 2007. Former National Counterintelligence Executive Michelle Van Cleave observed "The Chinese are the biggest problem we have with respect to the level of effort that they're devoting against us versus the level of attention we are giving to them," see, "Caught on Tape: Selling America's Secrets," CBS 60 Minutes, February 25, 2010.

[22] Peter Mattis, "China's New Intelligence War against the United States," *War on the Rocks*, July 22, 2015.

Retirees from government and military service also provide an avenue that the Chinese intelligence services have exploited in the United States and elsewhere. As retired officials, they are not subject to further background checks and or the other security measures that countries often put in place monitor officials with sensitive access. Although these officials no longer have direct access to policy deliberations and documents, they are in a position to provide assessments of policy developments informed by how the policy process and bureaucracy work as well as to identify and assess former colleagues. Chinese intelligence often asks for such reports rather than piles of documents.

Another area of U.S. vulnerability is losses through third-country partners, such as Japan, South Korea, Taiwan, Thailand, and many others. The U.S. alliance system, whatever its other national security benefits, creates vulnerabilities and access points to sensitive U.S. technology and information. For years, some of these countries had serious problems in trying to protect even their own information and systematic weaknesses in their ability to investigation problems. These vulnerabilities cannot be addressed unilaterally and require more routine cooperation with foreign counterintelligence authorities, like the effort that led to the arrest of Taiwanese General Lo Hsien-che in 2011.[23]

One of the outstanding issues in how the United States confronts Chinese intelligence is how the U.S. Department of Justice declines to prosecute espionage-related cases. The most notable recent example is the case of Helen Xiaoming Gao, who worked as a contract translator for the U.S. Department of State and other foreign policy-related organizations around Washington, DC. On the basis of unsealed court documents, it is not clear why someone who admitted taking money from persons she believed to be Chinese intelligence to report on U.S. Government employees would not be prosecuted.[24] There are legitimate reasons why prosecutors may choose not to pursue prosecution and why a case may not be as substantial as it appears.[25] However, because FBI operations are centered around cases, the inability to make a case can have far-reaching implications if the Justice Department's declinations to prosecute are viewed as repeatedly unjustified and politically motivated as the incentives to pursue Chinese intelligence-related cases disappear. As part of Congress's oversight role, requesting the Department of Justice to explain specific decisions not to prosecute going back over the last two decades would go a long way toward addressing concerns at the operational level about whether Chinese counterintelligence is a worthwhile pursuit.

---

[23] "AIT Confirms U.S. Role in Major Spy Investigation," *Taipei Times*, February 18, 2011.

[24] "Catherine Herridge, "State Dept. Contractor Allegedly Paid by Chinese Agent to Spy on Americans – Yet No Charges Filed," Fox News, April 22, 2015; *United States v. Helen Xiaoming Gao*, Affidavit before the U.S. District Court for the District of Maryland (2014).

[25] Several recent economic espionage cases, such as Sherry Chen and Xi Xiaoxing, have fallen apart on further scrutiny after sloppy investigative work, but serious problems go back to the Wen Ho Lee investigation and the leaks of nuclear secrets in the 1980s and 1990s as well as Katrina Leung investigation. See, Nicole Perlroth, "Accused of Spying for China, Until She Wasn't," *New York Times*, May 9, 2015; Devlin Barrett and John R. Emshwiller, "U.S. Drops Charges That Temple University Professor Sought to Give Tech Secrets to China," *Wall Street Journal*, September 11, 2015.