

### SECTION 3: CHINA'S HUMAN ESPIONAGE ACTIVITIES THAT TARGET THE UNITED STATES, AND THE RESULTING IMPACTS ON U.S. NATIONAL SECURITY

“The Commission shall investigate and report exclusively on—

...

“REGIONAL ECONOMIC AND SECURITY IMPACTS—The triangular economic and security relationship among the United States, Taipei and the People’s Republic of China (including the military modernization and force deployments of the People’s Republic of China aimed at Taipei), the national budget of the People’s Republic of China, and the fiscal strength of the People’s Republic of China in relation to internal instability in the People’s Republic of China and the likelihood of the externalization of problems arising from such internal instability. ...”

#### Introduction

In recent years, the Department of Justice has filed an increasing number of cases concerning espionage or illegal technology acquisition involving the People’s Republic of China (PRC). While these filings include some colorful spy cases that grab media headlines, the majority of them involve violations of export control laws or instances of industrial espionage. These cases attract far less public attention but are no less significant to U.S. economic and national security.

David Szady, a former assistant director of the Federal Bureau of Investigation’s (FBI) counterintelligence division, has referred to China as “the biggest [espionage] threat to the U.S. today.”<sup>249</sup> FBI Director Robert Mueller has warned that “China is stealing our secrets in an effort to leap ahead in terms of its military technology, but also the economic capability of China. It is a substantial threat.”<sup>250</sup> Joel Brenner, a former senior counterintelligence official in the office of the Director of National Intelligence, has characterized China’s intelligence services as the most aggressive out of 140 such entities trying to penetrate U.S. targets.<sup>251</sup>

Other statements from government counterintelligence officials suggest a Chinese intelligence collection effort that is growing in scale, intensity, and sophistication. “The Counterintelligence Community considers the People’s Republic of China to be one of the most aggressive countries targeting U.S. military, political, and economic secrets as well as sensitive U.S. trade secrets and technologies,” according to a May 2009 statement from the Office of the

Director of National Intelligence. “For a number of reasons, we believe China poses a significantly greater foreign intelligence threat today than it did during most of the cold war era.”<sup>252</sup>

Most of the law enforcement cases that have China at the nexus involve the illegal acquisition of U.S. controlled technologies. While some of these cases have ties to China’s intelligence services, the vast majority are linked to other state organizations, particularly the factories and research institutes of China’s military-industrial complex. Data released by the U.S. Department of Justice have indicated that, in cases resulting in federal prosecutions during fiscal years 2007 and 2008, China was ranked second only to Iran as the leading destination for illegal exports of restricted U.S. technology. The specific technologies illegally exported to China in these cases included rocket launch data, space shuttle technology, missile technology, naval warship data, unmanned aerial vehicle technology, thermal imaging systems, and military night vision systems.<sup>253</sup>

This year the Commission examined the extent of Chinese espionage directed against the United States as well as the impacts of such espionage on both U.S. national security and future U.S. economic competitiveness. Multiple Chinese state entities are engaged in an active effort to acquire restricted U.S. technologies; the Chinese government also encourages and rewards the actions of private individuals to obtain technology on its behalf. Agents of the Chinese government are also displaying an increasing willingness to offer financial inducements to U.S. government officials in order to encourage them to compromise classified information. Finally, Chinese government officials are engaged in the surveillance and harassment of Chinese dissident organizations within the United States.

Additional analysis will be included in the classified annex of the Commission’s 2009 Report to Congress. China’s extensive and growing cyber espionage activities will be addressed in chapter 2, section 4, of this Report, “China’s Cyber Activities that Target the United States, and the Resulting Impacts on U.S. National Security.”

### **China’s Traditional Intelligence Methodologies**

Traditional Chinese approaches to espionage differ significantly from those of the “classical” approach to espionage that has been encountered by the United States in the past.<sup>254</sup> Generally, where foreign sources are concerned, China has not “normally [paid] an agent for information, request[ed] that the person provide classified documents, [or] use[d] intelligence officers to elicit information from the agent or engage[d] in clandestine activity like ‘dead drops.’ . . . China prefers to obtain its information a little bit at a time.”<sup>255</sup> The means used to accomplish this have included inviting foreign scientific experts to conferences in China; flattering them; subjecting them to grueling schedules intended to wear them down mentally; and peppering them with incessant, coordinated elicitation intended to produce indiscreet disclosures rather than conscious espionage.<sup>256</sup>

Unlike Russian intelligence officers looking to exploit ego, greed, or other personal weaknesses, Chinese intelligence personnel are more inclined to make use of sympathetic people willing to act as a “friend of China.”<sup>257</sup> While this most clearly has been seen in

PRC-targeted recruitment of Chinese-Americans, PRC agents also have used as sources U.S. citizens of other ethnic backgrounds.

### ***A Shift in Traditional Practices of Source Recruitment***

Many historical cases of PRC-directed espionage against the United States have involved U.S. citizens of Chinese ethnic heritage. The issue is not that Chinese-Americans are less trustworthy than U.S. citizens of other ethnic backgrounds; instead, as former FBI analyst Paul Moore once noted, “the reason that it is always ethnic Chinese who seem to be involved in Chinese intelligence matters is that they typically are the only ones China asks for assistance.”<sup>258</sup>

One U.S. government handbook on counterintelligence has explained that

*the selling point in a normal PRC recruitment operation is not an appeal to ethnicity per se, but to whatever feelings of obligation the targeted individual may have towards China, family members in China, old friends in China, etc. The crux of the PRC approach is not to try to exploit a perceived vulnerability but to appeal to an individual's desire to help China out in some way ... ethnic targeting to arouse feelings of obligation is the single most distinctive feature of PRC intelligence operations.*<sup>259</sup>

However, in a shift from these historical practices, the Commission has noted that at least two prominent cases of Chinese-affiliated espionage within the United States over the past year have displayed an increased willingness by Chinese intelligence to reach beyond the confines of the Chinese-American community to seek sources as well as a greater willingness to offer financial inducements in exchange for information. (See “The Bergersen and Fondren Cases” later in this section.)

## **China's Intelligence and Technology Collectors**

### ***The Ministry of State Security***

The Ministry of State Security is China's leading civilian intelligence agency, with responsibility for both foreign intelligence and domestic security operations.<sup>260</sup> Similar to the intelligence services of other Communist states, China's Ministry of State Security is best understood as an arm of the ruling Chinese Communist Party (CCP), entrusted with a primary mission of preserving the CCP in power.<sup>261</sup> The Ministry of State Security collects foreign intelligence but also has a leading role in counterintelligence, broadly defined in political terms—i.e., to include the surveillance and suppression of groups viewed as oppositional to the CCP, such as political dissidents and ethnic separatists.<sup>262</sup> This role of acting against internal “opposition elements” has also been directed abroad. Li Fengzhi, a reported former Ministry of State Security officer who has since resettled in the United States, stated in early 2009 that a major emphasis of Ministry of State Security activities abroad is targeting Chinese dissident and prodemocracy groups.<sup>263</sup>

The foreign intelligence operations of the Ministry of State Security are centered in its Second Bureau, which operates agents

abroad under a range of covers, including both official diplomatic covers and unofficial covers such as students and businessmen. The Ministry of State Security also makes extensive use of news media covers, sending agents abroad as correspondents for the state news agency Xinhua and as reporters for newspapers such as the *People's Daily* and *China Youth Daily*.<sup>264</sup>

The Ministry of State Security also maintains a public face in the form of its affiliated think tank, the China Institutes for Contemporary International Relations (CICIR), located in northwestern Beijing. Aside from its public role, CICIR is fully incorporated as the Eighth Bureau of the Ministry of State Security and provides research and analysis for the Chinese leadership.<sup>265</sup> CICIR also publishes its own journal, "*Xiandai Guoji Guanxi*" (Contemporary International Relations) and frequently hosts U.S. visitors to China.<sup>266</sup> Members of this Commission have met on multiple occasions with representatives of CICIR during annual Commission fact-finding trips to China. (For further discussion of CICIR and the relationships between Chinese think tanks and U.S. institutions, see chap. 4, sec. 2, of this Report, "China's External Propaganda and Influence Operations, and the Resulting Impacts on U.S. National Security.")

#### ***The Military Intelligence Department of the People's Liberation Army (PLA)***

China's military intelligence agency is the Second Department of the People's Liberation Army General Staff Department, also known as the Military Intelligence Department. As a military organization, the Military Intelligence Department primarily collects intelligence on foreign military orders of battle, military doctrine, and weapons systems.<sup>267</sup> The Military Intelligence Department conducts overt collection of information through its military attachés in Chinese embassies but also has run covert collection operations through agents operating under cover.<sup>268</sup>

According to sources dating from the 1990s, the Military Intelligence Department has been the most active of China's intelligence services in acquiring foreign technology, particularly technology with potential military applications.<sup>269</sup> The Military Intelligence Department has operated multiple front companies in Hong Kong to facilitate technology transfers and other intelligence operations.<sup>270</sup>

Like the Ministry of State Security, the Military Intelligence Department also maintains affiliated think tank institutions. The foreign policy and national security affairs think tank of the Military Intelligence Department is the China Institute of International Strategic Studies, or CIISS.<sup>271</sup> Although CIISS does not publicly acknowledge its ties to the Military Intelligence Department, most of its researchers are current or former PLA officers, and the active-duty military officers assigned there divide work responsibilities between the institute and the Military Intelligence Department.<sup>272</sup> The current chairman of the institute is General (Ret.) Xiong Guangkai, a former director of the Military Intelligence Department.<sup>273</sup> Members of this Commission have held discussions with representatives of the China Institute of International Strategic Studies in the course of fact-finding visits to China. The Military Intelligence Department is also directly affiliated with the

PLA Institute of International Relations in Nanjing, which functions as a training center for officers of the Military Intelligence Department.<sup>274</sup>

<b>PRC Security, Foreign Intelligence &amp; Technology Collection Agencies</b>	<b>Institutional Subordination</b>	<b>Primary Missions</b>
<b><i>Civilian Entities</i></b>		
Ministry of State Security	PRC State Council/CCP Politburo Politics and Law Committee <sup>275</sup>	<ul style="list-style-type: none"> <li>• Foreign intelligence collection</li> <li>• Intelligence analysis</li> <li>• Counterintelligence</li> <li>• Suppression of dissident groups</li> </ul>
Ministry of Public Security	PRC State Council/CCP Politburo Politics and Law Committee <sup>276</sup>	<ul style="list-style-type: none"> <li>• Domestic security operations/law enforcement</li> <li>• Counterintelligence</li> </ul>
CCP International Liaison Department	CCP Central Committee <sup>277</sup>	<ul style="list-style-type: none"> <li>• Liaison with foreign political parties</li> <li>• Influence operations</li> <li>• Intelligence collection</li> </ul>
CCP United Front Work Department	CCP Central Committee <sup>278</sup>	<ul style="list-style-type: none"> <li>• Liaison with non-Communist Chinese groups</li> <li>• Influence operations</li> <li>• Intelligence collection</li> </ul>
Various Civilian Scientific Research & Development Institutions	Chinese Academy of Sciences (primary) <sup>279</sup>	<ul style="list-style-type: none"> <li>• Technology acquisition</li> </ul>
<b><i>Military Entities</i></b>		
Second Department, PLA General Staff Department (Military Intelligence)	PLA General Staff Department	<ul style="list-style-type: none"> <li>• Foreign intelligence collection (especially military data)</li> <li>• Intelligence analysis</li> <li>• Technology acquisition</li> </ul>
Third Department, PLA General Staff Department (Signals intelligence)	PLA General Staff Department	<ul style="list-style-type: none"> <li>• Signals intelligence collection and analysis</li> <li>• Cyber intelligence collection and analysis</li> </ul>
Fourth Department, PLA General Staff Department (Electronic Warfare)	PLA General Staff Department	<ul style="list-style-type: none"> <li>• Electronic warfare (jamming, etc.)</li> <li>• Computer network attacks</li> </ul>
International Liaison Department, PLA General Political Department	PLA General Political Department	<ul style="list-style-type: none"> <li>• Foreign intelligence collection</li> <li>• Political/psychological warfare</li> </ul>
Various Defense Industrial Firms	11 different state-owned defense enterprise group companies <sup>280</sup>	<ul style="list-style-type: none"> <li>• Technology acquisition</li> </ul>

This chart, although not comprehensive, shows some of the most prominent PRC agencies involved in security, and counterintelligence and the collection of foreign intelligence and/or restricted technology, along with their primary areas of responsibility.

Source: Compiled by Commission staff from multiple sources.

### ***Other Intelligence Entities***

The Chinese government also has a number of other institutional entities involved in foreign intelligence collection operations. The Third Department of the People's Liberation Army General Staff Department is China's leading signals intelligence agency and is also reportedly the largest of all of China's intelligence services, although no authoritative open-source figure is available for its total number of personnel.<sup>281</sup> The Third Department may also have a complementary relationship with the Fourth Department of the People's Liberation Army General Staff Department, which is responsible for electronic warfare.<sup>282</sup> (Further discussion of the activities of the Third and Fourth Departments may be found in chap. 2, sec. 4, of this Report.)

Alongside the Ministry of State Security and the Military Intelligence Department, the International Liaison Department of the PLA General Political Department has been identified by a U.S. government counterintelligence handbook as one of three Chinese agencies that conduct covert intelligence collection against the United States.<sup>283</sup> Bearing responsibility for propaganda and psychological warfare, the International Liaison Department has in past years been active in targeting Taiwan military officers.<sup>284</sup> Although the organization has been described as both smaller and less effective than either the Ministry of State Security or the Military Intelligence Department in its U.S. operations,<sup>285</sup> there is little publicly available information about the agency's operations within the United States.<sup>286</sup> However, a statement from the U.S. Office of the Director of National Intelligence in May 2009 listed the International Liaison Department as an active collector against U.S. interests.<sup>287</sup>

Other entities of the Chinese party-state also maintain a role in gathering foreign intelligence and spreading propaganda on behalf of the government. These include the United Front Work Department of the CCP and the Foreign Liaison Department of the CCP.<sup>288</sup> China's official Xinhua state news agency also serves some of the functions of an intelligence agency, gathering information and producing classified reports for the Chinese leadership on both domestic and international events.<sup>289</sup>

### **Chinese Intelligence and Technology Collection within the United States**

Information from recent criminal indictments indicates that Chinese intelligence and technology collection operations within the United States are more varied and complex than previously understood. A wide range of actors are at work collecting information and technology on behalf of the Chinese government, ranging from agents of the professional intelligence services described above to individuals seeking out technology and data that they might be able to sell to Chinese agencies. These efforts fall into four broad categories: 1) "actuarial" intelligence cobbled together from multiple sources; 2) "professional" intelligence-gathering conducted or directly sponsored by PRC intelligence agents; 3) "enterprise-directed" acquisition of controlled technology driven by entities within the Chinese state scientific research and development and mili-

tary-industrial sectors; and 4) “entrepreneurial” industrial espionage and illegal technology exports carried out by private actors seeking rewards from the Chinese government.

### **“Actuarial Intelligence”**

One distinctive element of Chinese espionage is the “grains of sand” or “actuarial” approach to intelligence-gathering. Rather than going after a narrowly targeted set of restricted information, Chinese intelligence efforts often focus on gathering immense quantities of raw information—most of which may not be classified or otherwise restricted, and much of which could be completely extraneous—and seeking to combine the vast number of puzzle pieces into a revealing “mosaic.”<sup>290</sup> As former FBI special agent I.C. Smith told the Commission, this traditional approach has been one of “just get the information to us, and we will sort it out later.”<sup>291</sup>

PRC intelligence operatives have also displayed a past preference for gathering information from many agents or sources rather than from any one, well-placed source: “The entire process is sometimes referred to as ‘actuarial intelligence,’ because its basis is not unlike the principles that insurance company actuaries apply to determine the profitability of insuring large groups of people.”<sup>292</sup> This approach allows cross-checking of information from multiple sources while also increasing deniability in any particular instance and reducing the risk to any single source of exposure.

This traditional Chinese intelligence collection methodology is less likely than the “classical” model<sup>293</sup> to produce unambiguous evidence of espionage that can be prosecuted in a U.S. courtroom. As characterized in a Central Intelligence Agency (CIA) and FBI report to Congress, Chinese spying activities “are usually low-key and singular in nature, thus creating a significant counterintelligence dilemma for the FBI.”<sup>294</sup> And while this Chinese approach may appear unwieldy, it can produce significant results over time; in the memorable phrase of a U.S. government counterintelligence handbook, the traditional Chinese approach to espionage is “inefficient but not ineffective.”<sup>295</sup>

A declassified joint CIA and FBI report from 2000 indicated that the widespread collection of “grains of sand” could be explained in part by China’s relatively low level of technological development compared to western countries:

*Because the Chinese consider themselves to be in a developmental ‘catch-up’ situation, their collection program tends to have a comparatively broad scope. Chinese collectors target information and technology on anything of value to China, which leads them to seek to collect open-source information as well as restricted/proprietary and classified information.*<sup>296</sup>

However, the rapid and dramatic advancement of science and technology in China in recent years is likely to produce gradually diminishing returns on such a scattershot method of collection. As China’s scientific research and development and industrial sectors become more advanced, their identified areas of shortfall—and therefore their collection requirements—are likely to become more

focused and specific. Many of the recent cases of Chinese state- or enterprise-directed information and technology acquisition that are cited in the examples to follow show signs of a more specific collection focus than that observed in the “actuarial” practices of past years.

### ***“Professional” Chinese Government-directed Espionage***

In contrast to the looser “actuarial” method of collection described above, agents working for the PRC’s professional intelligence services also seek out technological and intelligence information of a more specific nature. Three prominent cases of PRC-affiliated espionage that came into public view in recent years displayed this pattern, in which collectors operating on behalf of the Chinese government pursued specific technologies or information requirements tasked to them by higher authority.

#### *The Chi Mak Case*

Chi Mak was the central figure in an espionage investigation that culminated with his arrest in October 2005 and his sentencing in March 2008 to 24 years in prison. Born in China’s Guangzhou Province, Mr. Mak emigrated to southern California in the early 1980s and was naturalized as a U.S. citizen in 1985. By 1996, he was employed as an engineer with Power Paragon in Anaheim, California, a subsidiary of L-3/SPD Technologies/Power Systems Group, and had been granted a “Secret” level security clearance. At the time of his arrest, Mr. Mak was working as the lead project engineer on the “Quiet Electric Propulsion” project meant for future U.S. Navy warships.<sup>297</sup>

Mr. Mak took information about the Quiet Electric Propulsion project, as well as other Power Paragon projects, back to his residence and copied the information to compact discs that he then gave to his brother, Tai Mak, for encryption. Tai Mak operated as a courier for Chi Mak, relaying material to an unidentified PRC official in Guangzhou, China. Tai Mak intended to deliver a set of discs containing data on the Quiet Electric Propulsion project and other projects to this individual in Guangzhou at the end of October 2005 but was arrested while en route by FBI agents at Los Angeles International Airport.<sup>298</sup>

Prior to the arrests of Chi Mak and Tai Mak, FBI agents had retrieved shredded documents from the trash of Chi Mak’s residence that provided instructions and collections tasking to Chi Mak from his handler in China. These included instructions to Chi Mak to perform more networking through professional associations and conferences. The documents also laid out an extensive and specific list of 17 different categories of naval and space-based military technology on which Chi Mak was to seek out further information.

In May 2007, Chi Mak was convicted in the U.S. Court for the Central District of California on charges of conspiracy, two counts of attempted violation of export control laws, failing to register as an agent of a foreign government, and making false statements to federal investigators. In March 2008, he was sentenced to 24 years in prison. Statements from federal officials indicated that Chi Mak

had admitted to moving to the United States more than two decades earlier with the intention of gradually working his way into the U.S. defense industrial complex to steal military technology on behalf of the Chinese government.<sup>299</sup>

The Chi Mak case clearly reveals strong interest on the part of China's military research and development sector in gaining surreptitious access to specific U.S. military technologies under development. The information compromised by Chi Mak may prove to be of significant benefit to the PRC's naval systems modernization programs and may also improve the ability of PRC engineers to identify vulnerabilities in U.S. systems currently under development. (For more on China's naval modernization and increasing naval capabilities, see chap. 2, sec. 2, of this Report, "China's Naval Modernization and Strategy.")

#### *The Bergersen and Fondren Cases*

Two linked Chinese espionage cases in 2008–2009 displayed a hybrid amateur-professional espionage model, in which an apparently amateur agent or asset took directions from a Chinese government official to seek out classified and restricted distribution information from U.S. government officials. The first of these cases emerged into public view in February 2008 with a trio of arrests—that of Tai Shen Kuo, a naturalized U.S. citizen born in Taiwan; Yu Xin Kang ("Katie"), a PRC citizen and legal resident alien of the United States, who worked as an assistant to Kuo; and Gregg William Bergersen, a weapon systems policy analyst with the Defense Security Cooperation Agency, a Department of Defense (DoD) agency that implements foreign military sales.<sup>300</sup>

Tai Shen Kuo operated a furniture business in New Orleans and also maintained, through family connections, high-level contacts with defense officials in Taiwan.\* By an undisclosed series of events, he became affiliated with a PRC official in Guangzhou, China, who is not identified by name in the affidavit. This individual both provided funding for Mr. Kuo and assigned specific items of information that Mr. Kuo was to obtain from his contacts within the U.S. government.

Mr. Kuo deceived Mr. Bergersen by making him believe that he (Kuo) was using his contacts in Taiwan to lay the foundation for lucrative future defense contracting deals and that he was seeking information related to Taiwan military systems and future weapons sales in order to facilitate his business arrangements. Plying Mr. Bergersen with cash and gifts, and stringing him along with the hope of becoming a business partner for the expected future military contracting deals, Mr. Kuo was able to obtain from Mr. Bergersen information on the "*Po Sheng*" (Broad Victory) project,<sup>301</sup> a command-and-control upgrade program for the Taiwanese armed forces developed with U.S. assistance; publications on the "Global Information Grid" communications network of the DoD; and data from the "Javits Report" (classified "Secret"), a 2007

\*Tai Shen Kuo is a son-in-law of Hsueh Yeh, a former Republic of China Navy admiral who served the Guomindang during World War II and the Chinese Civil War of 1945–1949. See Peter Enav, "Taiwan Reviews Impact of New US Spy Charges," *Taipei Times*, February 14, 2008. <http://www.taipetimes.com/News/taiwan/archives/2008/02/14/2003401185>.

Defense Security Cooperation Agency spreadsheet on the planned U.S. sales of military equipment to foreign nations for the next five years.

In at least some instances—such as the information on the Global Information Grid and on future military sales to Taiwan—Mr. Bergersen was responding to specific requests from Mr. Kuo, who was in turn relaying taskings from the unnamed PRC official in Guangzhou. Throughout the time that he was handling over documents and information to Mr. Kuo, Mr. Bergersen apparently believed that this information was bound for officials in Taiwan and not the PRC. He was therefore deceived in a classic “false flag” operation, in which a source is misinformed regarding the identity of the end-user of the information.<sup>302</sup>

The other source exploited by Tai Shen Kuo was James Fondren, a retired U.S. Air Force lieutenant colonel who served from August 2001 through February 2008 as the deputy director of the United States Pacific Command Washington Liaison Office, located inside the Pentagon. Ties between the two men dated back to at least 1998, when Mr. Kuo allegedly became the sole client for a consulting service, “Strategy, Incorporated” that Mr. Fondren operated from his home. Mr. Kuo was in fact staying as a guest in Mr. Fondren’s home at the time of Mr. Kuo’s arrest in February 2008.<sup>303</sup>

Through Mr. Fondren’s consulting service, Mr. Kuo requested from Mr. Fondren “opinion papers” on topics related to military-to-military ties between the United States and China. The subjects of these papers included a description of the visit to the United States of a senior PRC military official, an overview of defense talks between DoD and PLA officials, and an assessment of a U.S. Navy-PLA Navy joint exercise. A review of Mr. Fondren’s “opinion papers” by investigators alleged that Mr. Fondren incorporated information from documents classified “Confidential” and “Secret,” including some passages copied nearly verbatim.

The affidavit in the Fondren case also indicates that Mr. Kuo’s PRC handler provided topics of interest that Mr. Kuo was to pass to Mr. Fondren and also suggested to Mr. Kuo that Mr. Fondren be misled into believing that his “opinion papers” were bound for senior military officials in Taiwan. If true, then Mr. Fondren, like Mr. Bergersen, was also duped by Mr. Kuo under a “false flag.” Mr. Fondren had also maintained some direct contacts with Mr. Kuo’s handler, reportedly exchanging 40 e-mail messages with him in 1999 and 2000.<sup>304</sup>

The actions of Gregg Bergersen and James Fondren could indicate a significant shift in the traditional character of Chinese state-supported espionage against the United States. There are significant differences between these cases and the traditional Chinese model: both men were U.S. government officials with access to classified information; neither man is Chinese-American; both were given specific taskings of documentation and information to hand over; and both were paid for their services. This indicates a set of practices verging closer to a more “classical” model of espionage<sup>305</sup> and shows a growing willingness on the part of PRC intelligence operatives to seek out individuals in the United States who have access to specific, required information.

Gregg Bergersen pled guilty on March 31, 2008, in the U.S. Court for the Eastern District of Virginia to a single count of conspiracy to disclose national defense secrets and was sentenced on July 11, 2008, to 57 months in prison.<sup>306</sup> Tai Shen Kuo pled guilty on May 13, 2008, in the U.S. Court for the Eastern District of Virginia to a one-count criminal charge of conspiracy to deliver national defense information to a foreign government and was sentenced on August 8, 2008, to 188 months in prison and a fine of \$40,000.<sup>307</sup> On September 25, 2009, James Fondren was convicted by a federal jury on one count of unlawfully communicating classified information to an agent of a foreign government and two counts of making false statements to the FBI. He is scheduled for sentencing on January 22, 2010.<sup>308</sup>

***“Enterprise-directed” Espionage Conducted by Chinese State-controlled Research Institutes and Commercial Entities***

While a significant part of Chinese espionage against the United States may be conducted at the behest of professional PRC intelligence agents, much of it—particularly in terms of economic and industrial espionage—is driven by the state-owned research institutes and factories of China’s military-industrial complex and/or by subsidiary companies spun off from these state institutions. As described by the CIA and FBI, “China’s commercial entities play a significant role in the pursuit of proprietary/trade secret U.S. technology. The vast majority of Chinese commercial entities in the United States are legitimate companies; however, some are a platform for intelligence collection activities.”<sup>309</sup> While many individual instances of collection may be conducted piecemeal, there is a central, national-level PRC program for technological acquisition and modernization dating back to the 1980s—the “863 Program”—that underlies this broader effort to obtain advanced technology.<sup>310</sup>

“Enterprise-directed” espionage may also be growing in importance and taking on a less random and more targeted form. The 2008 unclassified report of the Defense Security Service cited a rise in efforts undertaken by commercial entities to target restricted technologies, speculating that this likely represents “a purposeful attempt to make the contacts seem more innocuous by using non-governmental entities as surrogate collectors for interested government or government-affiliated entities.”<sup>311</sup> Although it does not provide specific country breakdowns, the same report also asserts that the East Asia and Pacific region is the origin of the most active efforts illegally to acquire U.S. defense technologies.<sup>312</sup>

However, if there is an increasingly organized and coordinated effort to target specific technologies by state-affiliated commercial and research entities, the collection prioritization and tasking process by which this is handled has not heretofore been well documented or understood. James Mulvenon, director of the Center for Intelligence Research and Analysis, Defense Group, Inc., described to the Commission a complex process that is by turns both state directed and driven by private initiative:

*I think it’s both bottom up and top down . . . we know from open sources that there is a high-level state coordination on [science & technology] procurement that goes on at the Bei-*

*jing level, whether it's in the Ministry of Science and Technology, whether it's ... under the Ministry of Industry and Information, whether it is derivative of the 863 Program, which itself was the result of high-level state coordination to identify key future technology gaps that China needed to push. ... At the same time, there is innovation going on at the bottom level where people are for their own materialist interests trying to acquire things that they know would be valuable and then going to find customers for it ... and so I think both of those processes are working at the same time.*<sup>313</sup>

Expanding on the matter of “enterprise-driven” collection, Dr. Mulvenon described a prominent role in technology acquisition undertaken by profit-driven commercial companies spun off from Chinese government-controlled defense industrial research institutes in the course of defense reforms in the late 1990s. He also described a decentralized, free-market system for the pursuit of technology acquisitions:

*[it's] often as mundane as simply receiving a fax saying, 'Here is the shopping list of things that we're interested in,' with no clear direction as to where they're going to find them, and then relying on the natural entrepreneurship and aggressiveness of the people that they've contacted ... often they're not the only people within the network that are being given this similar tasking ... this is a distributed network in which there is redundant multiple tasking, and often it's [a question of who gets there first].*<sup>314</sup>

#### *The Dongfan “Greg” Chung Case*

An example of “enterprise-directed” industrial espionage that was recently made public is the case of Dongfan “Greg” Chung, a naturalized U.S. citizen of Chinese heritage. Mr. Chung worked in the U.S. aviation industry from 1973 to 2006, holding positions with both the Boeing Company and Rockwell International. He held a “Secret” level clearance and worked as an engineer on various aerospace projects, including doing stress test analysis on space shuttle fuselages and developing a phased-array antenna for space shuttle communications.<sup>315</sup>

Mr. Chung was arrested in February 2008, in Orange, California. According to the indictment in his case, sometime around 1979 he established contact with a professor at the Harbin Institute of Technology and offered his services to “contribute to the [scientific modernizations] of China.” In succeeding years, Mr. Chung further communicated with officials at the China National Aero Technology Import and Export Corporation, the Nan Chang Aircraft Company, and the China Aviation Industry Corporation, receiving very specific questions regarding aircraft development and specific taskings for technical information. In response, Mr. Chung took multiple unreported trips to the PRC to deliver lectures. He also handed over—either via mail delivery or by passing them to an individual at the PRC consulate in San Francisco—a large number of proprietary Boeing and Rockwell technical manuals. These materials in-

cluded, among many other items, a shipment in 1985 that contained 27 manuals related to airframe stress analysis and 24 manuals related to the B-1 bomber program.

On July 16, 2009, Mr. Chung was convicted in the U.S. Court for the Central District of California of conspiracy to commit economic espionage; six counts of economic espionage to benefit a foreign country; one count of acting as an agent of the People's Republic of China; and one count of making false statements to the FBI. Mr. Chung is scheduled for sentencing on November 9, 2009.<sup>316</sup>

### ***“Entrepreneurial Espionage” on Behalf of China***

Another distinctive feature of Chinese intelligence collection—and one that is highly significant in terms of U.S. security—is the extent to which spying is also practiced by private individuals acting either independently or on behalf of the Chinese government. The Office of the Director of National Intelligence has reported the following:

*Nonprofessional intelligence collectors—including government and commercial researchers, students, academics, scientists, business people, delegations, and visitors—also provide China with a significant amount of sensitive U.S. technologies and trade secrets. Some members of this group knowingly or unknowingly collect on behalf of [PRC intelligence agencies] or Chinese defense industries, presenting a significant intelligence threat. But in many cases, the collection efforts of these private-sector players are driven entirely by the opportunity for commercial or professional gain and have no affiliation with [PRC intelligence].<sup>317</sup>*

Such reliance on amateur efforts to collect science and technology has led to a vast amount of “entrepreneurial” economic and industrial espionage conducted by Chinese students, trade delegations, businessmen, and educational and research institutions. The range of motivations for such espionage on private initiative can be varied and complex. Former FBI special agent I.C. Smith testified that the Ministry of State Security sometimes places pressure on Chinese citizens going abroad for educational or business purposes and may make pursuit of foreign technology a quid pro quo for permission to travel abroad.<sup>318</sup> However, this phenomenon of “entrepreneurial espionage” appears to be particularly common among businessmen who have direct commercial ties with Chinese companies and who seek to skirt U.S. export control and economic espionage laws in order to export controlled technologies to the PRC. In such instances, profit appears to be a primary motive, although the desire to “help China” can intersect in many cases with the expectation of personal financial gain.

The nature of such privately organized and implemented espionage efforts raises a number of thorny issues for U.S. counterintelligence and law enforcement officials. As special agent Smith asked, “Is it truly an intelligence operation in the absence of the presence of an intelligence service?”<sup>319</sup> Even in instances where there is no direct state involvement, however, the Chinese govern-

ment has been a major beneficiary of technology acquired through industrial espionage.<sup>320</sup>

“Espionage entrepreneurs” are not focused solely on obtaining state-of-the-art, high-tech data and equipment. Dr. Mulvenon testified to the Commission that many older technologies are still of considerable value to China’s military modernization:

*I would also submit to you that our export control system is overly focused on the state of the art and doesn’t apply a means-ends test to why the Chinese are requiring a specific piece of technology. There are pieces of technology . . . that the Chinese are trying to acquire that are 20, 25 years old, [and] that are mainstays of existing U.S. defense systems but come nowhere close to being considered state-of-the-art, and yet a means-ends test would correctly identify those as critical gaps in the Chinese system.*<sup>321</sup>

Expanding on this point, Dr. Mulvenon described to the Commission the existence of numerous entrepreneurial “mom-and-pop” companies—many of them nothing more than a titular business registered at a residential address—that legally purchase older military technology from U.S. manufacturers or through a secondary market of defense industrial equipment auctions, or even from the Internet, and then look for customer institutions back in China.<sup>322</sup>

#### *Two Cases of Industrial Espionage to Benefit China’s Space Industry*

Two illustrative cases of industrial espionage occurred within the United States during the Commission’s 2009 reporting period, both of which involved the intended illegal export to China of U.S. controlled technology and materials that would benefit China’s rapidly developing space industry. This is far from an exhaustive list—even within the narrow field of aerospace-related technologies other examples could be cited from 2009.

The first case is that of Quan-Sheng Shu, the owner of the firm AMAC International Inc., in Newport News, Virginia. Born in Shanghai in 1940, Dr. Shu was naturalized as a U.S. citizen in 1998.<sup>323</sup> He holds a PhD in physics and is the author of six books and more than 100 papers on the subjects of cryogenics and superconductivity.<sup>324</sup> Dr. Shu and his firm had worked on several research and development contracts on behalf of the U.S. Department of Energy and the National Aeronautics and Space Administration.<sup>325</sup>

In November 2008, Dr. Shu pled guilty in the U.S. Court for the Eastern District of Virginia to two violations of the Arms Export Control Act and one count of bribing Chinese officials in violation of the Foreign Corrupt Practices Act. Dr. Shu was sentenced to 51 months in prison and a fine of \$386,740.<sup>326</sup> As of summer 2009, AMAC International had divested itself of many of its past projects and proprietary technologies and had shut down its office in Beijing.<sup>327</sup>

The export control law violations pertained to Dr. Shu’s export to the PRC of a cryogenic fueling system for space launch vehicles

and technical data for a liquid hydrogen tank and cryogenic equipment. The items exported by Dr. Shu were intended to assist in the design and development of a cryogenic fueling system for space launch vehicles to be used at a heavy payload launch facility located on the southern island province of Hainan, PRC. According to the U.S. Department of Justice, the space launch facility at Hainan is affiliated with the PLA and the China Academy of Launch Vehicle Technology and is expected to be a launch site for space stations and satellites, manned space flights, and future lunar missions.<sup>328</sup>

A second case of alleged export violation in support of China's space program was revealed on October 28, 2008, when a grand jury in the U.S. District Court for Minnesota indicted Jian Wei Ding and Kok Tong Lim, both officials of FirmSpace Limited, an import/export company in Singapore; and Ping Cheng, a New York resident and reportedly the sole shareholder of FirmSpace. The three men were allegedly involved in a plan to sell carbon fiber material, with applications in aircraft, rockets, spacecraft, and uranium enrichment, to the China Academy of Space Technology.<sup>329</sup> Mr. Ding and Mr. Lim allegedly purchased the carbon fiber materials from an undisclosed firm in Minnesota via remote wire transfer, with the materials shipped to Mr. Cheng's address in New York. Mr. Cheng was allegedly then to inspect and store them and prepare them for shipment onwards to the China Academy of Space Technology.<sup>330</sup> Two other individuals, FirmSpace company directors, Hou Xinlu and Gao Xiang, are mentioned in conjunction with the case but have not been charged. Both men are believed to reside in China.<sup>331</sup>

Local media in Singapore have remarked that FirmSpace Limited seemed to have little else in the way of business activity. Despite the lack of the company's observable business, one local news outlet noted that the firm had not laid off any employees and had continued to pay them regularly. The firm's receptionist was quoted as saying, "I found it quite strange but I never thought of asking the bosses, as long as I still got my salary."<sup>332</sup>

### **How Well Is This Information Processed?**

With such a large intake of data and material, there remains a question as to how effective the Chinese system might actually be in separating the wheat of useful information from the mass quantities of chaff. The nature of the Chinese government bureaucracy, in which officials may be inclined to exaggerate successes to their superiors for purposes of career advancement, may facilitate waste within the system. For example, retired FBI agent I.C. Smith has described interviewing a former Ministry of State Security officer about that individual's responsibilities to obtain military technology inside the United States and being told of time wasted gathering useless U.S. military surplus items simply for the sake of bureaucratic appearances.<sup>333</sup>

However, amid the vast quantities of equipment and information collected by the Chinese system there emerge nuggets of genuinely useful material. One report from the late 1990s indicated that PLA-affiliated enterprises were actively involved in buying surplus

and cast-off equipment from U.S. military bases and may have been able in this way to acquire models of U.S. military systems for reverse engineering, possibly including the radar digital guidance system for the Pershing II intermediate-range ballistic missile system.<sup>334</sup>

### **Targeting Chinese Dissident Groups Abroad**

Another highly significant aspect of Chinese intelligence activities within the United States—and one with disturbing implications for many citizens and foreign residents of the United States—is the intensive effort put forward by Chinese government operatives to monitor, harass, and disrupt the activities of Chinese dissident groups operating abroad. There is ample evidence of such activity by Chinese officials within the United States, extending back for many years. In testimony presented before the House Foreign Affairs Committee in June 1990, Lin Xu, a former PRC consular official who had sought asylum within the United States, testified that Ministry of State Security officials had visited the Chinese embassy in Washington, DC, in the wake of the Tiananmen Square massacre to consult with educational services consular officials. These officials were subsequently assigned to monitor and harass Chinese students within the United States who were perceived to have reformist or prodemocracy sympathies.<sup>335</sup>

There have also been very similar and even more detailed accounts by PRC defectors in recent years. Chen Yonglin, a former PRC first secretary and consul in Sydney, Australia, defected in May 2005 and sought asylum in Australia. Mr. Chen provided a detailed account of efforts by Chinese government officials to monitor, harass, and disrupt the activities of “hostile elements.” Mr. Chen stated that the same model of PRC intelligence activities applies in both Australia and the United States.<sup>336</sup>

Mr. Chen produced an internal PRC government document that referred to the “Five Poisonous Groups” of Falun Gong members, Tibetan separatists, Uighur separatists, Taiwan proindependence activists, and prodemocracy activists. The document further described the “Consulate’s main counter-strategy in the battle” against such groups, with consular officials directed to “strengthen monitoring” of the activists on a list of names; to “conduct propaganda work through multiple channels,” with a particular focus on local Chinese language media; and to “try to work on local government officials.”<sup>337</sup> In regard to the latter effort, Mr. Chen described specific efforts to levy quid pro quo economic pressure on Australian officials and lobbying pressure placed on Sydney-area education officials to deny public funding to a school whose principal was a Falun Gong member. In such efforts driven by PRC government officials, a central point of emphasis is “mobilizing the force of the [local] Chinese community” to act on behalf of PRC interests.<sup>338</sup>

Falun Gong activists in the United States have alleged activities by PRC consular officials of a similar nature to those described by Chen Yonglin. A Falun Gong-affiliated newspaper, *Epoch Times*, has alleged that officials from the PRC’s New York consulate orga-

nized a series of assaults in 2008 against Falun Gong demonstrators in the New York neighborhood of Flushing, Queens.<sup>339</sup>

Two expert witnesses who spoke before the Commission this year, neither of whom has any affiliation with Falun Gong, both testified that PRC embassy and consular officials take an active role in organizing and mobilizing Chinese-American civic groups to act on behalf of the Chinese government.<sup>340</sup>

Other recent examples of PRC consular officials mobilizing ethnic Chinese groups were observed during the worldwide running of the Olympic Torch in spring 2008. As the torch relay made its way toward Beijing, scuffles took place in a number of cities between protesters made up of pro-Tibetan, pro-human rights, and other activists critical of the Chinese government, and counterdemonstrators made up of Chinese students or local ethnic Chinese residents. In some of these locations, particularly in Paris and Seoul, these confrontations turned violent.

One such example within the United States occurred on April 8, 2008, at a protest and large counterprotest on the campus of Duke University in Durham, North Carolina. This incident attracted significant media attention after a Chinese student attempting to mediate between the two opposing groups was vilified on the Internet by nationalist activists and the home of her parents in China subsequently vandalized.<sup>341</sup> In the incident at Duke, a group of approximately 15 students from a campus human rights group organized a pro-Tibet rally timed to coincide with the date of the torch relay, only to find themselves surrounded and drowned out by a crowd of approximately 400 counterdemonstrators. As described in an account provided to the Commission by a Duke student who witnessed the event,

*[t]he most striking characteristic of the gathering was the organization of the China supporters. In addition to gathering hundreds of supporters, which is no small feat on such a relatively small campus, most had large, pre-designed posters, printed leaflets, full-size Chinese flags, large U.S. flags, and were chanting and singing in unison. The Chinese supporters were not gathered in pell-mell like you'd expect from a gathering of 400 people. The organization and size of the pro-China crowd could be attributed to the fact that a large portion of those gathered . . . were not even Duke students.<sup>342</sup>*

In many such instances, the groups of ethnic Chinese counterprotesters showed clear signs of being encouraged and organized by officials from PRC embassies or consulates. As stated in a report issued by the analytical firm Strategic Forecasting, Inc., about the April 9, 2008, passage of the torch relay through San Francisco,

*[b]y 8 a.m. April 9, the pro-China demonstrators were taking up positions along the planned torch relay route, pulling in groups carrying Chinese, U.S. and Olympic flags, and equipped with cases of food and water. However, these were not spontaneous gatherings of overseas Chinese supporting the motherland, as Beijing media have portrayed them. Rather, there was a coordinated effort between local Chinese business and social associations and the consulate*

*to attract, equip, deploy and coordinate the large pro-China turnout. . . . By some estimates, as many as 50 busloads of Chinese from other parts of California were brought to San Francisco.*

This account also alleges the use of prank calls, text messages, and even low-level, localized jamming against the cell phones of the anti-PRC demonstrators—demonstrating, if true, prior knowledge of the phone numbers of the activists organizing the protests. Also described are possible efforts to incite confrontations in such a way as to make the anti-PRC demonstrators appear violent:

*On numerous occasions, individuals or small groups carrying cameras would seek to incite the anti-China demonstrators to acts of confrontation or violence, frequently by parading through the middle of a group of Free Tibet or Save Darfur demonstrators with a large Chinese flag, walking back and forth through the group. In some cases, small scuffles broke out—and pictures were snapped—though the anti-China demonstrators soon deployed individuals to try to keep the two opposing sides separated. The same day, Chinese media ran photos of pro-Tibet demonstrators shoving pro-China demonstrators, ‘proving’ their point that the Tibet supporters are violent.<sup>343</sup>*

Such activities directed at, by turns, either mobilizing or monitoring Chinese-Americans may be explained in part by a pervasive attitude among PRC officials that ethnic Chinese everywhere naturally owe loyalty to Beijing.<sup>344</sup>

Such examples also paint the Chinese government as highly fearful of dissident or ethnic minority activity organized abroad and willing to devote considerable attention and resources to thwarting activist groups backing these causes. They also reinforce Chen Yonglin’s description of PRC government officials seeking to hide their hand by coopting and mobilizing local ethnic Chinese business and community groups to undertake work on their behalf. This pattern of activity is best understood within the context of the CCP’s political imperative to present its domestic audience with a narrative of Chinese people around the world united in support of the Chinese government. It also fits in with a long-standing CCP pattern of “united front” activity intended to subvert and turn non-Communist Chinese groups into tools for advancing the goals of the CCP.

## Conclusions

- The intelligence services of the Chinese government are actively involved in operations directed against the United States and against U.S. interests. China is the most aggressive country conducting espionage against the United States, focusing on obtaining U.S. information and technologies beneficial to China’s military modernization and economic development.
- Some of the espionage carried out on behalf of China is conducted by nonprofessional collectors. These nonprofessional collectors may be motivated by profit, patriotism, feelings of ethnic

kinship, or coercion. Even in many cases where there is no obvious direct state involvement in the theft or illegal export of controlled technology, the Chinese government encourages such efforts and has benefited from them.

- Recent cases of espionage involving China show evidence of more focused efforts at information collection employing sources outside of the Chinese-American community.
- Chinese operatives and consular officials are actively engaged in the surveillance and harassment of Chinese dissident groups on U.S. soil.