DIRECTED OR DIFFUSE?
CHINESE HUMAN INTELLIGENCE TARGETING OF US DEFENSE TECHNOLOGY

A Thesis
submitted to the Faculty of the
Edmund A. Walsh School of Foreign Service
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Security Studies

By

Amy Elizabeth Brown, B.A.

Washington, DC
April 17, 2009
# Table of Contents

**Introduction** ..........................................................1

**A Foundation for Analysis: Scope and Methodology** .................6

  Characterizing the Chinese intelligence threat ........................12

**The Chinese Technology Collection Mission** ........................18

  China’s S&T Collection Mandate ........................................18

  China’s intelligence apparatus ........................................19

**Chinese Technology Theft Cases: Analysis** ..........................26

  China’s use of non-traditional methods in technology collection ....26

  China’s use of traditional methods in technology collection .......32

**Implications for US Counterintelligence** ............................41

**Works Cited** ..................................................................46

**Appendix A: Pertinent Statues** .......................................49

**Appendix B: Cases assessed** ..........................................51
Introduction

In October, 2005, the Federal Bureau of Investigation (FBI) broke up a spy ring in California. Chi Mak, a US defense contractor of Chinese origin, along with his extended family, were arrested on charges of conspiring to transfer sensitive defense technology to Chinese government officials. The case filing revealed evidence that Mak and his family had moved to the United States some 20 years prior with the expressed purpose of assisting their motherland in obtaining valuable information. As a so-called “sleeper” agent, Mak obtained US citizenship and a job as a contractor working on US defense technologies. He lived and worked quietly as a legal American immigrant for years before receiving taskings from his handlers in China to obtain highly sensitive information for the Chinese government.¹

Consider also the case of Qing Li, a Chinese woman living in Connecticut who sought to buy military equipment commonly used to gauge the power of nuclear explosions and export it to China.² Li apparently offered to help a friend in China acquire the export-restricted technology by taking advantage of her US residency to purchase the technology from a willing seller. The situations surrounding the case suggest that Li did not have any training in collecting intelligence information and did not participate in any prior technology collection operations.

These are just two cases in a barrage of Chinese attempts to steal US defense technologies, but they are revealing of the breadth of China’s technology collection activities. The Mak case demonstrates a high degree of planning and implemented

sophisticated covert methods for communicating with agents in China, including the use of couriers to transmit information clandestinely, and the use of “cutouts,” or mediating agents, to deliver taskings and receive information from the cooptees. Indeed, in many ways, the level of sophistication exhibited by the Chi Mak cases is reminiscent of the old, familiar spy game the United States played with the USSR, in which an agent travels to the United States with the expressed mission of gathering sensitive information, and transmits this data covertly back to the agent’s home country. This stands in contrast to the view of Chinese intelligence operations that is often portrayed by media and US government officials, which depict China’s technology operations as largely opportunistic, collecting information passively by interviewing students and delegations to Western countries and attempting to boldly purchase restricted technology from willing sellers.³ The Qing Li case represents this type of operations.

Media, government and academic sources have characterized cases such as the Mak and Li cases of technology theft as symptoms of the same epidemic.⁴ Many assert that both long-term, clandestine operations and opportunistic [shorter-term] instances of technology transfer are emblematic of China’s diffuse style of intelligence collection. For example, one Washington Post article likened the methodology employed to collect sensitive technical information in the Mak case to the case of Wave Lab⁵, in which export-restricted technology was transferred to China through illegal export, an operation which was boldly overt. Even prominent

³ For its part, the Chinese government claims that all allegations of espionage on its behalf are groundless, and would never harm the interests of another government.
⁴ See Warrick and Johnson
⁵ See appendix B for more details on the Wave Lab case.
scholars of Chinese espionage have broadly characterized China’s collection
techniques as distinctly open and diffuse. For example, Nicolas Eftimiades, a former
DOD intelligence official and China scholar, speaking at a hearing before the US
Joint Economic Committee, drew a distinction between the “traditional” intelligence
activities used by Russia and the type of activities China typically engages in. He
noted that “senior US counterintelligence officials compare China’s methods to
classical Russian espionage techniques, which used fewer people but gathered more
information per person.”6

A closer look at China’s illegal technology acquisition activities, however,
reveals a sophisticated, multipronged approach, which is at times opportunistic and
at times direct in its collection methods. But under what circumstances does China
employ long-term, covert operations to obtain information from well-placed sources,
and in what situations does it use less coordinated, one-off operations, or other, more
overt collection methods? The answer to this question would not only improve the
United States ability to affect Chinese intelligence operations against its interests,
but could also deeply impact how the United States government allocates its
counterintelligence resources against China in a resource-constrained environment.
Moreover, a better understanding of China’s technology collection methods is
critical in the defense of the United States’ technological advantage. This
technological advantage is critical to the United States’ ability to deter, and if
necessary win, future wars.

---

6 Statement by Nicholas Eftimiades, Author, "Chinese Intelligence Operations” before the Joint
Economic Committee United States Congress. Wednesday, May 20, 1998 (testimony of Nicolas
Eftimiades).
This paper examines China’s use of traditional and non-traditional information gathering efforts, and seeks to delineate trends in its use of each. It asks two primary questions: First, under what circumstances does China employ traditional espionage methods to collect United States technologies and intelligence pertaining to those technologies? Second, under what circumstances does China employ non-traditional, diffuse methods for collecting United States technologies and intelligence pertaining to those technologies? I assess that China’s intelligence apparatus employs the activities that it deems most appropriate, given the sensitivity and accessibility of the desired technology. I hypothesize that China’s intelligence services implement more “traditional” intelligence operations in order to obtain more sensitive, to include classified, US government information, and use a more opportunistic, “non-traditional” approach for transfer of export restricted and other less sensitive types of information.

I define traditional and non-traditional intelligence collection methodology in the following manner:

- “Traditional” methods employ activities that are clandestine in nature, meaning direction to conduct the illegal activities by a Chinese government entity was detected. Usually there is evidence that trained intelligence professionals conducted the activity in question;

- “Non-traditional” methods are employed in instances in which no specific clandestine activities occur. Usually, these activities appear to be executed by

---

7 United States technologies are defined as technologies that are produced by either the United States government, or by companies which were established in the United States. As such, these technologies are protected from theft under US Law.

8 Clandestine activities are defined as activities in which the actor seeks to evade detection.
non-professionals with little or no training in intelligence collection methods.9

If my hypothesis is correct, I would expect to find evidence of the Chinese government’s direction in intelligence operations targeting highly sensitive and classified information. In these cases, the nature of the information sought would require a well-placed individual to obtain the information. For cases that involve less sensitive information, in which restricted technologies are transferred to China, I expect that more opportunistic or criminal behaviors will be observed. However, if my hypothesis is incorrect, I would expect not to find evidence that China uses clandestine methods to collect sensitive information, or find that there is no apparent correlation between the sensitivity of the information and the methods used to collect information and technologies.

This report is divided into the following sections: First, I will set out the scope and methodology for this paper. I will then discuss several standing hypotheses held by Western governments and analysts regarding China’s overall technology collection methods. Then I will lay out China’s science and technology (S&T) collection mandate and introduce the different government agencies that comprise China’s intelligence collection apparatus. This paper’s primary contribution to the topic of Chinese technology espionage is that it focuses on the distinction between China’s traditional and non-traditional methods of technology

---

9 I use the terms “Traditional” and Non-Traditional” to distinguish between commonly held perceptions about espionage methods, and less recognized methods for acquiring information. I use this generalization for the purposes of this paper only, and do not seek to compare China’s intelligence activities with the activities of other nations. It is important to note that every intelligence service has its own traditions and particular methods, so these terms should be viewed only in light of the cases represented in this report.
collection, and highlights the ways in its uses both. Additionally, academic studies on China’s intelligence activities are rare, so this thesis aims to contribute to the academic discussion on China’s methods, and the impact its intelligence operations have on governments.

A Foundation for Analysis: Scope and Methodology

It is necessary at the outset to define the terms used throughout this study. First, this paper identifies two general types of information which are sought by the Chinese government: 1) sensitive US government information, and 2) restricted technologies. Sensitive US government information is defined as information that is protected from transmittal to unapproved foreign entities through US federal regulations, such as classification. Information about these technologies would only be available US government employees and contractors with need-to-know. In other words, persons who have access to this information are pre-approved by the United States government. One example of the type of information that is restricted through classification would be the technical details of a technology that would give the United States a significant advantage in wartime. Information regarding the US military’s specific capabilities would also be classified. On the other hand, “restricted technology” is technology that is commercially available, but not approved for export to certain foreign countries.\(^\text{10}\) Though these technologies are not widely available to the public, they are not protected by classification or other regulations which require prior US government approval for access. For example,

most night vision technologies are not classified—numerous companies make certain types of night vision technologies can be sold commercially within the United States. However, some restrictions are placed on their availability to foreign entities. There are numerous types of trade restrictions, depending on the sensitivity of the technology involved, and the type of technology it represents. The United States Department of State and the US Department of Commerce regulate which types of technologies are approved for export and to which countries. In sum, the difference between restricted technology and classified US government information is the way by which a person can gain access to the technology.

Sometimes the transfer of restricted technologies can constitute economic espionage. However, it is important to distinguish cases relating to sensitive and restricted US technologies, and cases indicating simple economic espionage. The Economic Espionage act of 1996 makes illegal the theft of any proprietary information, including trade secrets, and also criminalizes conspiring to give proprietary information to persons not authorized to have it, including foreign governments. This applies to all proprietary technologies and ideas, from sophisticated defense technologies to, for example, the recipe for Coca-Cola products. As part of its efforts to improve its industrial base, China has been known to target technologies that do not have a direct defense application, such as commercial communications technologies. While these technologies can greatly assist China in rapidly developing its infrastructure, they are not owned or controlled

---

11 For more information on US export laws, please see Appendix A.
12 Economic Espionage Act of 1996, See appendix.
by the United States government, and therefore do not apply to this study. Although
economic espionage is a component of many of the cases in this study, any case that
involves the theft of trade secrets that do not pertain directly to national security is
excluded from consideration in this study.

In intelligence terminology, different terms are assigned to different types of
intelligence collectors. For the purposes of this paper, an “agent” refers to a person
who is an intelligence collection professional, and who is trained, by their home
service, to conduct intelligence operations. In China, these persons work for the
Ministry of State Security or the Second Department of the People’s Liberation
Army, for example. The people they recruit to conduct intelligence operations are
called “sources”, or “assets”, interchangeably. Persons who are termed “cooptees”
are sources who are witting participants in intelligence or technology collection
operations.¹⁴

In this paper, I distinguish between activities that reflect the traditional notion
of intelligence collection activities, in which hostile foreign intelligence services
target national defense information, and non-traditional collection activities, which
do not exhibit elements of government direction, but nonetheless have the potential
to positively impact China’s national security posture. Whereas traditional or
clandestine methods employ the use of agents, who receive specific collection
taskings and supply information to the Chinese government over a period of time,
non-traditional or opportunistic collection might be limited to a one-time criminal
activity, and does not reflect any specific and prolonged tasking by the Chinese

¹⁴ Not all intelligence sources must be witting of their involvement in espionage activities. Use of the
term “cooptee” helps to distinguish between witting and unwitting intelligence sources.
government. The line between these two activities is unfortunately indistinct. Good criminals seek to hide their activities in much the same way as spies. Likewise, spies have implemented certain methods, such as the use of front companies, because their usefulness has been borne out in other criminal activities. Because of this, I attempt to distinguish the level of direct Chinese government involvement in each case.

China’s intelligence collection against Western nations is multi-faceted, and open sources indicate that China is using human, cyber and other technical means of collecting intelligence information. Although China employs a numerous types of intelligence collection techniques, this paper focuses exclusively on human intelligence (HUMINT) collection methods. This is due to the relatively greater accessibility of information on such operations available to the researcher operating at the open source level. While HUMINT cases emerge into public view after arrests are made, cyber and other types of cases are harder attribution and therefore do not receive as much public attention as HUMINT.

Furthermore, this paper examines the Chinese government’s connection to intelligence activities broadly, and does not attempt to link the activities to a particular intelligence service or agency within the Chinese government. The reason for this is that the published affidavits used in this study do not indicate the particular intelligence service involved, and only link the activity to the government. The likely reason these affidavits do not indicate the intelligence service involved is that it would reveal too much of the United States government’s sources and
methods for obtaining information about the case. It is also possible that the service used in these cases is unknown, even to US government officials.

In order to examine China’s traditional and non-traditional uses of intelligence collection methodologies, I read and assessed 19 cases of espionage linked to China that were prosecuted in the United States from March 1999 to March 2009.\textsuperscript{15} I obtained information on these cases through Department of Justice affidavits; other official DOJ-issued correspondence, such as indictment proceedings and press releases; published interviews with government officials; media sources; and information contained in secondary source literature. I also draw on information provided in US government publications and Congressional reports, such as the Cox Commission Report. I found that most of the cases that went to prosecution during this time period were more “non-traditional” in nature. To assess China’s use of clandestine methods, I examine the cases for: the types of information or technologies sought; the methods employed; and connections to Chinese government entities.

This study seeks to illuminate patterns found throughout the 19 cases. I will highlight cases in this study which are illustrative of the overall findings. However, because access to information on these cases is highly variable, in addition to considering the applicability of the cases to my overall findings, it should also be noted that the highlighted cases were also chosen on the basis of availability of information.

The fundamental challenges that exist in studying espionage must also not go without acknowledgment. There are several deep epistemological concerns with

\textsuperscript{15} A list of the cases used as source material in this study is enclosed in Appendix A.
studying espionage and intelligence collection methods. First, the information available is imperfect and incomplete. Only cases that meet the public eye can be considered, and these cases likely represent only a sampling of the total cases, since presumably some espionage successfully goes undetected. For an espionage case to be brought trial, and thus into the public view, the burden of evidence is quite high. Trials expose information that was previously considered sensitive to the public eye, and unsuccessful trials can contribute to poor diplomatic relations between governments. Thus, there is strong incentive for the US government to ensure that those cases that do come to light are limited to only those strong cases that are likely to result in punitive action against the offender.

Furthermore, the clandestine aspects of intelligence operations are intrinsically designed to avoid detection. Thus, the cases which reach prosecution represent instances of espionage that “failed” on some level—even if sensitive technologies or information were successfully transferred in part or in whole out of the United States to China by the agent, the agent was nonetheless apprehended and the espionage efforts brought to light. Indeed, it is possible that in an unknown but larger number of instances China employs more effective tradecraft that goes undetected by counterintelligence officials, and therefore does not go to trial and into the public view. Or activities might be detected but for reasons of state is not prosecuted by the US in the court system. Additionally, before a case goes to trial, counterintelligence officials carefully screen the information that is released to the public to ensure that sensitive information does not come to light. Thus, the
information that comes into the public’s view is potentially only a portion of the total information that exists on the subject.

An additional limitation this study faces is that the data points are extremely limited. In this case, I am looking at a subset of espionage cases centered around illegal technology transfer. I further limited the case selection to focus on government-directed technology collection. That is, for those cases in which sensitive information is passed on to China, I examined only those that demonstrated government involvement, and did not use cases that suggest entrepreneurial or other self-interested motivations. Of course, motivation can be difficult to determine. An outside researcher is limited in her ability to collect information on this topic. Here, we must rely on the investigators who produce the information to disclose the government connection.

**Characterizing the Chinese intelligence threat**

American counterintelligence officials have noted that China has developed increasingly robust intelligence capabilities in recent years. Much has been written about China’s diffuse intelligence activities, and observed trends in China’s intelligence collection methodology have been well-documented, yet there remains much confusion amongst scholars and open source government publications regarding how and when China applies this capability.

---

In recent years, Western nations have sought to label China’s unique intelligence activities. Western governments, including the United States, often view China’s HUMINT methods in contrast with the familiar tactics developed in Russia, Europe and the United States. These methods, which have been loosely referred to as “traditional” intelligence methods by some in the United States government, might be characterized by the Cold War Russia v. US intelligence battles, in which trained agents of a government are employed to obtain information about a particular intelligence target. Agents are trained by the government intelligence apparatus in tradecraft methods and are always cognizant of the role they play in collecting intelligence information on its behalf. Conversely, in the Chinese model, more people participate in intelligence collection, and each person obtains quantitatively less information than in so-called “traditional model”. Furthermore, it is unclear if all participants in Chinese intelligence are aware they are participating in intelligence collection. According to the Cox Commission Report, China frequently utilizes persons from outside the intelligence apparatus to provide information to the Chinese government. This form of collection can take place by interviewing students with technical expertise, or inviting non-Chinese persons with the appropriate technical knowledge to travel to China and present information.

The diffuse and opportunistic use of non-service intelligence collectors often leads counterintelligence officials to describe China’s intelligence capabilities as

---

non-traditional or asymmetrical. For example David Szady, former head of the FBI’s Counterintelligence Division, has stated that China’s intelligence threat is:

…increasingly asymmetrical insofar as it seeks to exploit the areas where there is a perception of weakness within the US national security approach and organizations. Traditional notions of counterintelligence that focus on hostile foreign intelligence services targeting classified national defense information simply do not reflect the realities of today's complex international structure.\(^\text{18}\)

Szady has also publically termed this collection method as the “thousand grains of sand” method, in that China collects a large amount of information, and then sifts through the information to find those valuable “grains” of information, which constitute actionable intelligence information. Others, such as Nicolas Eftimiades, have termed this collection technique the “mosaic approach.”\(^\text{19}\)

According to FBI testimony before Congress, China’s diffuse, “thousand grains of sand” method allows it to collect a large body of information without breaking any laws, and thus without alerting law enforcement officials.

Chinese nationals working abroad lawfully gather most S&T and economic intelligence through open sources, such as US university libraries, research institutions, the Internet, and unclassified databases, providing the Chinese government with highly valued, yet unclassified information. PRC scientists, through mutually beneficial scientific exchange programs, gather S&T information through US national laboratories. Programs to enhance cooperation between the two countries have created an atmosphere of informational exchange, creating vulnerabilities in safeguarding US technical intelligence. These vulnerabilities emphasize the significant difficulty the United States encounters in detecting PRC espionage activity.\(^\text{20}\)

\(^{18}\) Changes the FBI is Making to the Counterintelligence Program, April 9 2002 (2002) (testimony of David Szady, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation).
\(^{19}\) Eftimiades, pg 66.
This “thousand grains of sand” collection method is especially useful in collecting US technologies, in part because of the nature of the scientific process. In scientific research, much of the basic research is conducted in an unclassified setting. If this basic research yields a technology that is particularly useful to furthering US national interests, the technology will be classified at the point of its inception. Thus, tomorrow’s most highly sensitive projects might start out as basic research at a university lab, staffed with various foreign students. Chinese intelligence collectors understand and exploit the open nature of US research labs. As indicated in the Cox Commission Report, “the PRC collects military-related science and technology information from openly available US and Western sources and military researchers.”^{21} Nicholas Eftimiades agrees, noting that China’s “most productive method of legally acquiring foreign technology is to send scientists overseas on scholarly exchange programs.”^{22, 23}

Another hypothesis posited by scholars and government officials is that China attempts to collect information through unclassified channels whenever possible, including collecting information that is perhaps not classified, but nevertheless has potential national security value, and seeks to take advantage of mistakes made through sloppy information security procedures. Perhaps the most indicative of this theory is a book which was published by Chinese military experts regarding the Chinese military’s intelligence collection methods and priorities. The manual, entitled, “Sources and Methods for Obtaining National Defense Science and

---

^{21} Cox Commission Report, pg 30
^{22} Eftimiades, pg 28.
^{23} “Western Intelligence Sources Fear China Aims Spy-Network at European Industry.” The Sunday Telegraph in English. (Open Source Center document, EUP20050703031014) 07/03/2005.
Technology Intelligence,” was published in 1991, and was the first comprehensive manual on China’s overseas military espionage activities to be revealed to the West. The manual focused predominantly on collection against US technology targets. The two authors of the book were Chinese military intelligence specialists. According to the book’s translators, the book’s dissemination was never restricted by the Chinese government, and contained surprising detail regarding the People’s Liberation Army’s intelligence collection methods. Additionally, the book provided insight into China’s perceptions regarding US culture and information weaknesses, for example displaying a general understanding of the open nature of US information, and advising its readers to take “fortuitous advantage” of opportunities to exploit loopholes in the American legal system and to uncover information leaks through media sources:

Public materials are still a major source of intelligence for national defense S&T workers. A common saying has it that there are no walls which completely block the wind, nor is absolute secrecy achievable, and invariably there will be numerous open situations in which things are revealed… By picking here and there among the vast amount of public materials and accumulating information a drop at a time, often it is possible to basically reveal the outline of some secret intelligence, and this is especially true of the Western countries.

The authors go on to elaborate the value of conducting open intelligence collection. The authors estimate that intelligence professionals can collect approximately 80 percent or more of the intelligence they need through open

---


25 Ironically, it appears that this training manual was released by mistake – a fact that gives Western intelligence services a glimmer of hope that China is perhaps also susceptible to the very sort of indiscretion that it exploits in western countries.

sources. The other 20 percent must be derived from special means, such as reconnaissance satellites, electronic eavesdropping, and HUMINT activity. To illustrate the point that highly valuable information can be collected through open means, the authors of the book detail the “hydrogen bomb leak incident,” in which classified information about the project was inappropriately declassified, compromising the project and eliminating an important technological advantage for the United States.  

If indeed 80 percent of information is collected through open means, how then, is the other 20 percent of intelligence information collected? Understanding how, when and why the Chinese government conducts these 20 percent of operations is a crucial, and often understudied, component of improving US counterintelligence operations against China. The next section will examine China’s technology collection mandate, and will review the available literature regarding Chinese government agencies responsible for collecting sensitive technology, as well as assessing the methods they employ, clandestine and otherwise.

---

27 Cox report, pg 21.
The Chinese Technology Collection Mission

China’s S&T Collection Mandate

The Chinese government seeks to encourage the transfer of Western technologies to China, by legal and non-legal means. Recognizing the need to bolster China’s technology position relative to more developed countries such as the United States, former Chinese paramount leader Deng Xiaoping instituted a plan called the 863 Program to foster the rapid development of technology needed to narrow the gap between China and the West in key science and technology sectors by the year 2000. China’s specific technology collection priorities were laid out in the 863 Program. According to the Cox report, the 863 Program was placed under the management of the Commission on Science and Technology in National Defense (COSTIND). The 863 Program budget is split between military and civilian projects, and focuses on both military and civilian aspects of science and technology. The program focused on the following military technology areas:

- Astronautics
- Information technology
- Laser technology
- Automation technology
- Energy technology
- New materials

In 1996, the PRC announced the “Super 863 Program” as a follow-on to the 863 Program for planning technology development through 2010. The “Super 863 Program” continues the research agenda of the 863 Program.

---

28 Cox Commission Report, pg. 11
In addition to the 863 Program, “the sixteen character policy” was created as China’s blueprint for overt and covert efforts to buy, steal or otherwise acquire sensitive military technology. As described by the Cox Committee, the slogan urges China’s science and technology planners to “combine the military and the civil; combine peace and war; give priority to military products; [and] let the civilian support the military.” 30

The type of rapid technology acquisition described by the 863 Program cannot be achieved through completely organic means: to accomplish China’s goals, outside assistance was sought, often through theft and replication of advanced technologies. The following section discusses the major intelligence services and other intelligence collectors which are responsible for executing China’s technology collection efforts, and will highlight some of the ways in which China conducts traditional and non-traditional intelligence activities.

China’s intelligence apparatus

Unlike in the United States, where the intelligence collection mission is assigned to specific government agencies, in China information collection is a responsibility of many, if not all, government bureaucracies. However, there are several government agencies that are particularly important for China’s foreign and domestic intelligence activities. This section describes some of the primary intelligence organs of the Chinese government and the extent to which they contribute to overseas technology collection.

30 Cox Commission Report pg. 14
Ministry of State Security (MSS)

The Ministry of State Security is China’s premier civilian intelligence agency, with responsibility for conducting intelligence operations at home and abroad. The MSS has developed the infrastructure and tradecraft required to conduct sophisticated intelligence operations. According to an article in a Chinese language newspaper, the Hong Kong Cheng Ming, the MSS is divided into several bureaus, each of which has a specific area of responsibility. Important to this discussion are the First Bureau (Domestic) and the Second Bureau (Foreign). The Domestic Bureau finds and recruits people with overseas connections to work for the MSS. If suitable persons are going abroad for study, business, pleasure, residence, inheritance or other purposes, agents from the First Bureau attempt to persuade or cajole them into doing intelligence work for the Bureau while abroad.\(^{31}\) It is also responsible for receiving Chinese intelligence agents from abroad when they come back to China.\(^{32}\)

The Foreign Bureau is responsible for the MSS’s operations abroad, and sends agents abroad using a variety of covers, including having them pose as employees of foreign trade companies, banks, insurance companies, and as journalists.\(^{33}\) The Foreign Bureau also posts agents to Chinese embassies and consulates, just as Russia and the United States do. It is responsible for recruiting agents abroad and giving orders to agents sent abroad. According to Hong Kong sources, the Second Bureau employs “sleeper” agents to be called upon when needed, and tasks intelligence collection to its agents and cooptees. It also receives, analyzes and reports to higher

\(^{31}\) Tan Po (3225 3124) “Spy Headquarters Behind the Shrubs—Supplement to Secrets About CPC Spies. OSC FTS19970311001137, 9/1/1996

\(^{32}\) ibid

\(^{33}\) ibid
levels of the Chinese government on information sent back by agents.\textsuperscript{34}

According to the Cox Commission Report, the MSS’s responsibilities include conducting foreign science and technology collection, and although military intelligence is not its primary responsibility, it will occasionally collect military information as well. The report states that MSS efforts to collect technology often support the goals of specific PRC technology acquisition programs, but the MSS will take advantage of any opportunity to acquire military technology that presents itself.\textsuperscript{35} According to Nicolas Eftimiades’s book \textit{Chinese Intelligence Operations}, there are three basic operational patterns with regard to technology-related espionage activities in the United States. First, cooptees are recruited in China and asked to acquire the targeted technology while they travel abroad. Second, American companies with access to desired technologies are purchased outright by Chinese state-run firms. And third, and most commonly, high technology equipment is purchased by recruited agents running front companies in Hong Kong.\textsuperscript{36}

The MSS has been observed to conduct both traditional and non-traditional espionage activities in support of its technology collection mission. In his book, Eftimiades highlights several cases in which the MSS recruited individuals to conduct espionage activities for China, and found evidence of both traditional and non-traditional espionage techniques. He examines two instances in which the MSS recruited individuals to work for China on a short-term basis.\textsuperscript{37} In both cases, he found that the individuals were required to sign an agreement to assist China in its

\textsuperscript{34} Ibid
\textsuperscript{35} Cox Commission Report, pg. 20
\textsuperscript{36} Eftimiades, pg 66
\textsuperscript{37} Eftimiades, pg 68.
intelligence collection activities. “No clandestine tradecraft training was offered to either agent; in both cases, they were told of their information requirements only in the most general terms.”38 The Cox Commission report lends further support to the use of non-traditional techniques by the MSS. It notes that in addition to its cadre of dedicated case officers and analysts, the MSS also relies on a network of non-professional individuals and organizations acting outside the direct control of the intelligence services, including scientific delegations and PRC nationals working abroad, to collect the vast majority of the information it seeks.39

Eftimiades’s work further highlights China’s ability to conduct traditional, clandestine operations, and to carefully observe operational security protocols. He notes one case in which the MSS recruited a student to do long-term espionage work for the Chinese government while living abroad.40 According to Eftimiades, the student was paid regularly and offered training to assist him in his intelligence collection activities. Moreover, the clandestine nature of the student’s relationship with the MSS was always stressed, demonstrating an attention to operational security.41 Richard Deacon, who has published several books on the subject of Chinese espionage, further discusses China’s attention to the security of the information it collects. He notes that China has a systematic approach for handling sensitive information, and is well versed in information security measures: “The whole apparatuses of internal security, espionage at home and abroad and counterespionage are all tightly interlocked and tightly controlled… There is a well-

38 ibid.
39 ibid.
40 Eftimiades, pg 66.
41 Operational security is the application of security procedures to any activity, (Eftimiades, pg 34.)
defined security system with comprehensive rules on how written materials and other information should be handled.”  

The case examples provided by Eftimiades and supporting evidence by other studies of Chinese intelligence indicate a two-pronged approach to collecting intelligence information. On the one hand, China recruits short-term agents to collect information along general lines. It also recruits individuals with specific skill sets to conduct long-term espionage activities, trains them, and provides compensation for their efforts.

The People’s Liberation Army (PLA) General Staff 2nd Department (Military Intelligence)

The Second Department of the PLA General Staff is responsible for military intelligence. Second Department HUMINT collection operations attempt to satisfy the information needs of a broad range of strategic-level forces and military industrial customers. According to Hong Kong’s Cheng Ming newspaper, “The Second Department of the PLA General Staff Headquarters is mainly responsible for collecting military information, which can be divided into three major parts: First, sending military attaches to Chinese embassies abroad; second, sending special agents to foreign countries to collect military information under the cover of various identities; and third, conducting military intelligence analysis based on information publicly published in foreign countries.”

---

42 Deacon, pg 313-314.
43 Eftimiades, pg 94.
44 Tan Po (3225 3124), Analysis of CPC Intelligence, Other Organs. Open Source Center FTS19960901000372
The Second Department’s mission requires that it maintain the capability to conduct both overt and clandestine operations. It employs military attachés to openly collect intelligence abroad, and also uses cover to conduct clandestine collection efforts. For example, Eftimiades cites a case in which the PLA most likely used the China’s permanent mission to the United Nations in New York as cover for PLA intelligence operations. Although it is known that the Second Department has the capability to conduct both traditional and non-traditional activities, the academic literature on this department’s actual activities is extremely limited. Eftimiades points to a more clandestine approach to collecting intelligence. Eftimiades look at exposed military intelligence operations that highlight the clandestine nature of PLA operations, and the sensitivity of the information sought. For example, in one case, a military attaché in the PRC’s Washington, DC embassy and an officer working under cover at the Chinese consulate in Chicago were caught trying to purchase what they believed to be classified NSA materials.

Non-professional intelligence collectors

In addition to and separate from these services, the PRC maintains a growing non-professional technology-collection effort led by other PRC government-controlled interests, such as research institutes and PRC military-industrial companies. Many of the most egregious losses of U.S. technology have resulted not from professional operations under the control or direction of the MSS or 2nd Intelligence Department, but as part of commercial, scientific, and academic

---

45 Eftimiades, pg 94.
46 Eftimiades, pg 93.
47 Cox Commission report, pg 19.
interactions between the United States and the PRC. According to the Cox Commission Report, those unfamiliar with the China’s intelligence practices often conclude that, because intelligence services conduct clandestine operations, all clandestine operations are directed by intelligence agencies. In the case of the PRC, this is not always the rule.\textsuperscript{48} Much of the China’s intelligence collection is independent of MSS direction. For example, a government scientific institute may work on its own to acquire information.

Important here is the Commission of Science, Technology and Industry for National Defense (COSTIND). According to Eftimiades, COSTIND has both overt and clandestine collection capabilities and functions. It is in charge of research and planning for military technologies and weapons systems and makes recommendations concerning these to the administrative office of the Central Military Commission.\textsuperscript{49} As part of its duties, COSTIND sends it scientists overseas as members of academic and scholarly exchanges to collect information and to identify needed foreign technologies or weapons systems. COSTIND’s intelligence collection methods include traveling to foreign countries as employees of a front company to buy and arrange for delivery of technologies not cleared for export, as well as inviting scholars and researchers to come to China, where they can be more easily prodded for information.\textsuperscript{50} Once the desired information is identified, the clandestine handling of the information is likely transferred to one of the intelligence services. Eftimiades states that once the material is identified, acquiring it becomes the job of either the MSS, the Second Department of the PLA, or COSTIND.

\textsuperscript{48} ibid
\textsuperscript{49} Eftimiades, pg 104.
\textsuperscript{50} Eftimiades, pg 104-105
depending on the availability of resources and access. As such, COSTIND is not an intelligence service *per se*, as its primary mission is not the collection of intelligence, but identification of needed technology.

As noted here, China’s intelligence apparatus has been observed implementing both diffuse, non-traditional intelligence collection methods, as well as more traditional, agent-driven collection techniques. The next section of this report will examine how the Chinese government has employed both methods to collect sensitive and restricted technologies from the United States.

**Chinese Technology Theft Cases: Analysis**

Chart 1: Chinese Technology Collection Cases, 1999-2009

<table>
<thead>
<tr>
<th>Traditional cases</th>
<th>Non-traditional Cases</th>
<th>Not enough data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chung Dongfan</td>
<td>Sheldon Meng</td>
<td>J. Reese Roth</td>
</tr>
<tr>
<td>Chi Mak et al</td>
<td>William Kovacs</td>
<td>Lee Wen Ho</td>
</tr>
<tr>
<td>Noshir Gowadia</td>
<td>Feng Yang</td>
<td></td>
</tr>
<tr>
<td>Bergersen/Kuo/Kang</td>
<td>Ding Zhengxing, Su Yang, Peter Zhu</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Joseph Piquet, Thomas Tam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wave Lab</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evan Zhong</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jian Wei Deng, Kok Tong Lim, and Ping Cheng</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ko-Suen Moo and Maurice Serge Voros</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hanson, Yaming, Nina Qi</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shu Quan-Sheng</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Qing Li</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ko-Suen Moo and Maurice Serge Voros</td>
<td></td>
</tr>
</tbody>
</table>

*China’s use of non-traditional methods in technology collection*

As indicated in the chart above, of the 19 cases examined for this paper, 13 appeared to use non-traditional collection methods. In each of these 13 cases, there was no evidence that trained intelligence professionals conducted the activities in

---

51 Eftimiades, pg 104.
question; rather, the activities appear to have been executed by non-professionals with little or no training in intelligence collection methodology. However, each of these cases sought highly-advanced technologies with potential military and other national defense applications. In all thirteen cases, the information sought was restricted through export controls, but did not carry a government classification and generally did not require any particular special access in order to acquire it.

One of the defining characteristics of China’s non-traditional techniques for obtaining technology, as observed in many of the cases noted here, is the lack of clandestine tradecraft, or even the most basic elements of operational security, involved in obtaining the information. Eftimiades notes that, “a unique characteristic of MSS technology transfer operations is that the recruited agent is often relatively honest with his American counterpart as to the final destination of the product.”52 In more traditional, “Western” HUMINT cases, great care is given to protecting the agent or cooptee from detection by the host government. It appears from this sampling that the Chinese agents are viewed to be “honest” because attention is not paid in these cases to operational security.

The most frequently observed method for acquiring technology is to simply purchase the technology from a willing seller, then simply ignore export restrictions and ship or hand-carry the items to China. Ten of the cases examined in this study appeared to use this methodology, with little or no additional observed tradecraft.53

---

52 Eftimiades, pg 31. While Eftimiades links these activities to the MSS, this paper found no correlation between these activities and the MSS, or any other particular intelligence service.
53 These cases were: Kovacs; Yang; Ding/Yang/Zhu; Piquet/Tam; Wave Lab; Zhong; Deng/Lim/Chung; Moo/Voros; Hanson; and Li.
In general, it appears that little or no care is used to ensure that the operation goes undetected.

This method is exemplified by the Xu Bing case. Xu was accused in 2007 of purchasing F-1600 night vision technology for resale to China. The F-1600 night vision technology Xu sought was categorized as a United States Munitions list item, and is explicitly restricted from export to China. According to the criminal complaint, employees of Xu’s company, Everbright Sci&Tech Company, contacted an undercover US Department of Homeland Security agent, who was posing as a willing seller,\(^{54}\) and expressed an interest in purchasing the night vision technology. In his dealings with the undercover agent, Xu openly acknowledged the wrongfulness of his activities, and made no attempt to conceal that the final destination of the night vision technology was China.\(^{55}\) In this case, only a basic level of tradecraft was observed. Although the company utilized an email address for its business dealings that was believed to be secure, the openness of Xu’s actions while dealing with the undercover agent suggest that he was not well-trained in covert collection activities.

In a separate case, Qing Li, a Chinese woman living in Connecticut, sought to buy and export to China a type of military equipment called an accelerometer.\(^{56}\) According to a DHS press release, these controlled military sensors are used in the development of missiles, artillery, and the calibration of large-scale nuclear and chemical explosions. Accelerometers are a designated defense article frequently used

---

\(^{54}\) Xu Bing Criminal Complaint. United States District Court District of New Jersey. 31 Oct. 2007. pg 2.

\(^{55}\) Xu Criminal Complaint, pg 3.

in missiles, ‘smart bombs’ and other major weapons systems, and are restricted from export unless written permission from the US State Department is granted. According to the press release, the end user for the products was a “special” scientific agency in China.\textsuperscript{57} Li’s activities were exposed because she attempted to purchase the sensors through an undercover US Immigrations and Customs Enforcement (ICE) agent. The press release noted that Li and her co-conspirator in China used e-mail messages and telephone calls to negotiate the illegal export transaction with the ICE agent. Li and her co-conspirator urged the ICE agent to deliver the accelerometers directly to China, advising that if the accelerometers tested properly, large orders would follow.

According to a website which claimed access to the indictment, Qing Li displayed her lack of understanding of operational security in an email she composed to the undercover contact in which she wrote:

I don’t need the products. I am just actually doing a favor for a friend in China to find the products. I have forwarded all the information to the friend and it’s up to them for the decision now. I have nothing to do with it. I have told the friend that I won’t be involved anymore due to the risk attached.\textsuperscript{58}

The openness of Li’s communication with the undercover agent suggests a lack of training in tradecraft. Furthermore, Li urged the undercover agent to deal directly with the Chinese agent, and send the sensors directly to the end user in China, shifting the majority of the risk associated with the operation to the seller. Human intelligence operations normally try to protect their sources from

detection by law enforcement entities, so as to maintain an open channel of
information. Li did not take measures to protect the supposed company she was
dealing with in the United States, thereby suggesting a lack of intelligence
training.

The lack of attention to operational security suggests a low level of Chinese
government involvement in the case. In other words, these operations, assuming
they are indeed conducted at the behest of the Chinese government, are most likely
not executed by intelligence professionals, and little or no training has been provided
to the cooptees.

Another underlying trend seen in the non-traditional cases is that China
collects information opportunistically. While this might seem intuitive, it appears
that China has a unique ability to take advantage of opportunities that present
themselves. The case of J. Reese Roth provides and example of how China might
obtain information through opportunistic means. Roth was accused of engaging in a
conspiracy to transmit export-controlled technical data related to a restricted United
States Air Force contract to develop plasma actuators59 for a munitions-type
Unmanned Aerial Vehicle (UAV) to a foreign national from China.60 Beginning
around 1989, Roth traveled on multiple occasions in his capacity as a university of
Tennessee faculty member to China to lecture regarding plasma science and
technology at certain PRC state-operated academic organizations and universities.
Roth was named an Honorary Professor at the University of Electronic Science and

59 According to the indictment, a plasma actuator is an electrical device for producing plasma and a
means by which such plasma can be applied to a surface, such as an aerodynamic surface like an
airfoil or a wing.
60 The United States of America vs. John Reese Roth and Atmospheric Glow Technologies,
indictment. United States District Court Eastern District of Tennessee.
Technology of China in 1992 and Tsinghua University in 2006. Xin Dai, a Chinese Ph.D. Student in Electrical Engineering was employed by Roth as a graduate assistant and was assigned by Roth to work on an Air Force Phase II Munitions Contract, titled “Augmented UAV Flight Performance Using Nonthermal Plasma Actuators,” which was subject to the rules, regulations and restrictions of the Arms Export Control Act. According to the indictment, Roth inappropriately gave Xin access to Air Force information, and furthermore exposed restricted US government information to Chinese officials through his visits to Chinese universities.\footnote{See Roth indictment.}

Although the indictment charges Roth with conspiracy to willfully export restricted information to China, it is unclear from the information provided in the affidavit whether Roth was anything other than negligent of his responsibilities to the Air Force contract. Roth did little to conceal his activities. In fact, he appeared to be rather flippant in his disregard for security regulations, suggesting that perhaps it was not his intention to harm US national security by supplying China with the technology information he handed over, but rather that he was instead willfully ignorant of security protocol. Given the sensitivity of the issues Roth worked on, it is reasonable to assume that his disregard for security protocols did not go unnoticed by the Chinese government, particularly when he presented information at universities in China. One would assume that the Chinese government was aware of the technical significance of the information brought to China by Roth, and took note of every detail.\footnote{I categorize this case as having not enough data to determine if it is traditional or non-traditional. This is primarily because the Roth indictment does not indicate the roll that the Chinese student played in exposing information to China, if at all. If the Chinese student had a clear role in managing
It is reasonable to assume that ultimately these non-traditional cases receive some high-level direction from the Chinese intelligence apparatus, and were not simply cases of persons wishing to sell the technologies on the black market, given that each of the technologies had significant military application and lesser commercial value. However, information surrounding each of the cases here suggest that the persons conducting the operation lacked extensive training in intelligence tradecraft. One might argue that perhaps these cases were detected because the persons indicated did not practice adequate operational security. However, it appears that theses cases demonstrate not just sloppy tradecraft, but a distinct lack of tradecraft. For example, Xu Bing’s forthrightness with the undercover agent demonstrated a level of carelessness not observed in any of the following clandestine cases.

*China’s use of traditional methods in technology collection*

While the cases discussed in the preceding section highlight the methods by which the Chinese government might obtain sensitive US defense technology, broadly speaking, all of the cases have one thing in common: though in each case, the potential benefit to China’s defense posture is clear, none of the cases exhibited direction by the PRC government. A review of the recently prosecuted cases, however, reveals that sometimes Chinese intelligence operations use methods which demonstrate active participation by a person or persons affiliated with the Chinese intelligence apparatus. The cases that will be discussed in this section demonstrate the information that Roth provided, then this case would be traditional. Without this understanding it is impossible to distinguish. However, the opportunistic characteristics of this case are emblematic of trends observed in Chinese non-traditional collection.
China’s clandestine effort to obtain US technology information. In this section, I analyze 4 cases in particular: Chi Mak and his family of co-conspirators, the Chung Dongfan case, the Greg Bergersen/Tai Shen Kuo/Yu Xin Kang case, and the Noshir Gowadia case. These cases, in general, exhibit direct taskings from the Chinese government to the agent in the United States.

According to Eftimiades, long-term agents are referred to in MSS slang as “fish at the bottom of the ocean (chen di yu).”\textsuperscript{63} These are individuals recruited as espionage agents who will not be activated until a later date.\textsuperscript{64} A notable element of this recruitment process is the degree of operational security practiced by MSS officers in cases when long-term assets are employed. In these relationships, the clandestine nature of the relationship with the source was always stressed.\textsuperscript{65} Both of these features were present in the case of Chi Mak, arguably the most damaging technology-related case to be successfully prosecuted in the United States over the last 10 years. Mak moved to the United States with his family in 1979 and became a naturalized US citizen in 1985. Mak was a skilled engineer, and obtained a US government issued Secret-level security clearance in 1996 as part of his position at Power Paragon, a subsidiary of L-3/SPD Technologies/Power Systems Group Power Paragon. Mak was the lead project engineer on a research project involving Quiet Electric Drive (“QED”) propulsion for use on US Navy warships. According to the affidavit filed in October 2005, QED is an extremely sensitive project. According to the Office of Naval Research, the technology developed in the QED program is considered by the Navy to be Significant Military Equipment and therefore banned

\textsuperscript{63} Eftimiades, pg 61.
\textsuperscript{64} Efimiades, pg 61.
\textsuperscript{65} Efimiades, pg 66.
from export to countries specifically denied by the US State Department, including China. The technology is covered by the security caveat “NOFORN, Distribution Schedule D”, a designation that restricts dissemination of material to foreign entities, agents, or interests, and the material can be released only to Department of Defense contractors and its employees.66

As part of the investigation, FBI agents found letters from Chinese agents instructing Mak to participate in more associations and seminars with special subject matters. One letter contained a directive to compile special conference materials on a disk.67 The letter also listed a number of military technologies that were sought, including information on space-based electromagnetic intercept systems, space-launched magnetic levitational platforms, electromagnetic artillery systems, submarine torpedoes, electromagnetic launch systems, and aircraft carrier electronic systems, among others. In response to several such directives, Mak allegedly copied information from his employer to disks, which were then encrypted by his brother Tai and hand carried to China via courier. The affidavit also reveals evidence that the Mak family used code words used to help conceal their activities. For example, Tai Mak referred to the information sought as his “assistant”.

The Chi Mak case reveals much about China’s technology collection operations in the United States.68 First, it indicates a level of patience in China’s technology collection techniques. Chi Mak lived in the United States for over 20

---

66 Chi Mak Affidavit, pg 7
67 Chi Mak Affidavit, pg 11
68 Though the Chi Mak case tells much about China’s covert intelligence operations in the United States, many questions remain. The degree to which the Chinese government was involved in Chi’s life in the United States is unclear from the affidavit. It cannot be determined if Chi was directed to move to the United States and obtain employment, or if he himself decided to move to the United States and was recruited to work for the Chinese government after his arrival on US soil.
years before he was in a position to collect classified technology information. According to media sources, Mak was sent to the United States as a “sleeper” agent. “Chi Mak acknowledged that he had been placed in the United States more than 20 years earlier, in order to burrow into the defense-industrial establishment to steal secrets,” said Joel Brenner, the head of counterintelligence for the Office of the Director of National Intelligence, in an interview with the Washington Post.69

Second, the Chi Mak case demonstrates a level of covert intelligence methodology and operational security planning not seen in the non-traditional cases. Mak received specific collection taskings from persons in the Chinese government, demonstrating the government’s direct involvement in the case. The use of couriers to transmit collected information to China demonstrates a recognition of the dangerous security environment for conducting such operations. Also, it can be inferred from the affidavit that Mak traveled to China to meet with his intelligence handlers, tradecraft which would help to ensure the safety of Mak and his fellow accomplices because the cooptees can move and exchange information freely, without concern for detection. Also, Mak’s use of code words in conducting espionage demonstrates an awareness of operational security.

Another case corroborates many of the lessons learned from the Chi Mak case. The case of Chung Dongfan also reveals an explicit effort on behalf of the Chinese government to send long term “sleeper agents” to collect intelligence information, and demonstrates clandestine communication methods. Chung worked for Rockwell Boeing from 1973 until 2002, and held a Secret clearance in accordance with his employment as a stress analyst on Boeing’s space shuttle

69 Warrick and Johnson
program. Chung was indicted in 2006 for passing information about the Shuttle program to China. According to the indictment, Chung received direction, in the form of letters, from persons in China instructing him to provide information on “[t]he entire process of the aircraft’s fatigue life and its major links; the static strength and principles of fatigue design when designing new aircraft; the formulation of a fatigue test plan; and the determination of a helicopters’ rotor wings, blades, and propeller hub’s load.”

Chung’s spy activities began by at least 1985, when he began receiving letters from a person, presumably connected to the Chinese government. Between 1985 and 2003, Chung made multiple trips to the PRC to deliver lectures on technology involving the Space Shuttle and other programs, and during those trips he met with officials and agents of the PRC government. Chung failed to report his foreign travel to Boeing as required, suggesting that he sought to conceal his activities in China. According to the indictment, Chung began collecting manuals from the North American Aviation division of Rockwell, which were used in the design of the F-100, X-15 and B-70 aircraft, among others. Possession of these manuals was restricted to the engineering personnel of Rockwell International Aerospace Divisions. Chung’s contacts in China asked him to provide further information and offered to pay him for his services.

Like the Mak case, the Chung case exhibited elements of Chinese government control. Chung received taskings from China, in the form of a laundry list of topics his Chinese handlers were interested in learning more about. Chung’s

---

handlers used similar communication methods as observed in the Mak case. He received his taskings by letter, as Mak did, and was directed to send his information via courier—his brother-in-law—to China as it was deemed by his Chinese handler to be “more convenient”. Furthermore, the contact in China arranged for the transfer of money through surreptitious means, and suggested codenames for his travel. Chung’s case therefore further exemplifies how cases with demonstrated government direction tend to exhibit increased operational security awareness.

Another case demonstrated a different set of tradecraft skills, but nonetheless a similar level of direction on behalf of the Chinese government. In the case against Kuo, Bergersen, and Kang, Greg Bergersen, an employee of the Defense Security Cooperation Agency of the US Department of Defense who maintained a US Top Secret/SCI clearance, relayed information to Chinese officials about the US Government sale of a Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system to Taiwan. Bergersen conveyed classified information in meetings with his handlers, who he apparently believed worked for the Taiwan government. Bergersen received money for his services. Wire taps between Bergersen and his contact, Tai Shen Kuo, indicate that Bergersen knew that the information he transmitted to his handler was classified. Throughout the course of the case, the Chinese handlers displayed a high degree of operational security awareness. Bergersen was given the codename, G, which his handlers used in referring to him.

---

71 Chung indictment, pg 13.
72 The United States of America vs. Tai Shen Kuo, Gregg William Bergersen and Yu Xin Kang, affidavit. United States District Court Eastern District of Virginia. Feb. 2008. pg 12
In this case, the Chinese government maintained control of the case from China, and an agent based in the United States, Kuo, contacted Bergersen. At times, Kuo contacted Bergersen through an intermediary (sometimes called a “cut-out”), Yu Xin Kang. Kuo communicated with the Chinese officials through several different email accounts. This cutout appeared to add an additional layer of security, as it further concealed the Chinese government’s role in the operation. Also interesting is the fact that Bergersen apparently thought he was working with the Taiwan government. On at least one occasion, Bergersen asked his handler to help him establish a meeting with officials from the Taiwan Ministry of National Defense, apparently believing that his handler would be able to make such a contact. Probably adding to this façade was the fact that Kuo was from Taiwan. (Passing the classified information to Taiwan would also have been illegal, but it is interesting that China was able to dupe its cooptee into believing that he was helping a friendly country, rather than a foe, which probably helped Bergersen justify his actions to himself.)

Thus, because of the sensitivity of the information sought by China, a high level of operational security was paid to this case. The Chinese government’s actions were so secretive, that even their operative, Bergersen did not know the source of the directions he was receiving.

Another case which exhibited elements of traditional espionage techniques is the case of Noshir Gowadia. Like in the Bergersen case, financial gain appeared to

---

73 Kuo/Bergersen/Kang affidavit, pg 7.
74 It should be noted that on May 13, 2009, another Pentagon official was arrested on charges of providing classified information to Tai Shen Kuo, and ultimately to China. According to early Associated Press reports, the FBI arrested retired Air Force Lieutenant Colonel James Wilbur Fondren, a deputy director of the US Pacific Command’s Washington Liaison Office. Fondren held a Top Secret clearance and like Bergerson, Fondren believed that he was providing information to Taiwan, and not to China.
be the primary motive driving Gowadia to assist China’s technology collection. Gowadia was a naturalized citizen of the United States who obtained employment at Northrop Corporation\(^7_5\) in about 1986. In about 1979, Gowadia was assigned to a then-classified Special Access Program which developed the B-2 Spirit bomber. Specifically, he assisted in the development of the unique propulsion system of the B-2 by utilizing classified design techniques for infrared, visual and radar signature reduction which contributed to the aircraft’s low observable capabilities.\(^7_6\) After he left Northrop, Gowadia started his own business. According to the indictment, Gowadia used this business to knowingly transfer documents containing information at the Secret and Top Secret levels to Chinese government representatives. In return for this information, Gowadia received at least US$110,000.

The indictment alleges that Gowadia initiated contact with Chinese officials in order to sell controlled defense technologies related to the reduction of the infrared heat signatures of aircraft and airborne weapons systems. Gowadia and his Chinese handlers established tradecraft in an attempt to communicate securely. They established a covert e-mail address to transmit classified US national defense information. He also traveled to China on at least six occasions to meet with Chinese government officials with the specific purpose of assisting China in reducing the heat signature for one of its cruise missiles.\(^7_7\) The indictment stated that Gowadia and his Chinese co-conspirators attempted to conceal Gowadia’s travel to China by failing to stamp, or making false and misleading stamps, in Gowadia’s

\(^{75}\) Northrup Corporation later became known as Northrop Grumman Corporation.
\(^{77}\) Gowadia superseding indictment, pg 11.
passport. Gowadia’s contacts in China also paid for all of his travel expenses, in an attempt to further conceal his travels. Gowadia also took steps to conceal the payments he received from Chinese officials. He maintained several off-shore bank accounts, and requested Chinese officials to deposit payments directly into these accounts.

The Gowadia case is different than the above mentioned cases in that there is specific evidence that Gowadia sought contacts in the PRC in order to advance his business of selling US defense information to foreign governments. In the other cases, the affidavits do not indicate whether or not the source was actively recruited. However, in the case of Gowadia, China was clearly taking advantage of a situation which presented itself. Once the contact between Gowadia and the Chinese government was established, however, Gowadia’s Chinese contacts took active measures to conceal the relationship.

In sum, by analyzing the affidavits from the cases where Chinese government control was exhibited in the execution of the technology collection operations, one finds several common characteristics. First, where there is evidence of government direction, the information sought was always restricted through the US government’s classification system. In other words, the information sought by the Chinese government required special access, and therefore the information could only be obtained through a well-placed cooptee. For example, in the Chi Mak case, the information transferred to China required access to information that was only granted to Navy contractors. In the Bergersen case, the information sought required access to information about the US weapons sales to Taiwan. The sensitive nature
of the information sought in these cases also requires special consideration for maintaining the cooptee’s safety. In each of the cases, Chinese officials took steps to communicate with their assets covertly, and to conceal their role in the operations.

As noted earlier, Eftimiades’s research has indicated that the MSS often forges long-term relationships with its sources, and sometimes it sends sleeper agents abroad with the intention of awakening these agents once they have procured citizenship and gained access to valuable information. In several of the traditional cases, there is substantial evidence to suggest that China uses sleeper agents. It can be difficult to prove, however, that any particular agent was tasked before their arrival in the United States with the explicit purpose of obtaining sensitive information. In the cases presented here, the US government does not provide evidence to demonstrate that China purposefully planted sleeper agents in the United States with the expressed purpose of “awakening” them at a later date. However, information does point to a long relationship with representatives from the Chinese government. Specifically, the Chi Mak Case and the Chung Dongfan case appeared to use long-term collection techniques to obtain classified information. Prosecutors in the Mak case called him a “sleeper” agent, who had been sent to the United States by the Chinese government with the expressed purpose of gaining access to sensitive information and transmitting it back to China.

**Implications for US Counterintelligence**

China’s intelligence method is unique because it implements a multipronged approach that allows its intelligence apparatus to make the most of its resources.
China reserves its sophisticated, traditional espionage activities for situations that call for specialized access to information, and especially classified information. It relies on persons with little or no operational training individuals to conduct routine technology transfer operations, which seek restricted, but not classified, technologies. China is able to conduct more operations in comparison to its Western counterparts in part because it does not use trained operatives for all, or even a majority, of its operations. The compromise with this approach is that more cooptees are at risk for exposure because they are not adequately disguised through rigorous operational security. And since China denies involvement in espionage activities abroad as a rule, those who risk their freedom to provide information to China are unlikely to get assistance from its government if they find themselves apprehended.

The number of arrests made in the United States in Chinese technology transfer cases suggests that this is a risk China is willing to take. Indeed, China’s methods appear to have paid off. According to a 2005 report to the US House of Representatives, “the technology that China is developing and producing is increasing in sophistication at an unexpectedly fast pace. China has been able to leapfrog in its technology development using technology and know-how obtained from foreign enterprises in ways other developing nations have not been able to replicate.”\(^7\)

Portions of the technologies “obtained from foreign enterprises” were almost certainly obtained through China’s non-traditional intelligence collection methods.

The Chinese approach poses many problems for U.S. law enforcement efforts, both because the frequency of China’s non-traditional collection efforts tax the US law enforcement system’s ability to keep pace with the activity, and because China’s long-term, traditional clandestine technology collection efforts are, by design, difficult to detect.

What can law enforcement do to assuage this upward trend in China’s intelligence collection? An understanding of Chinese intelligence priorities will help counterintelligence officials to apportion its resources appropriately.

In non-traditional cases, cooptees often only contribute small amounts of information, or only participate in a few operations. According to FBI counterintelligence chief Harry Godfrey III: “For prosecutive purposes, you are looking at an individual collecting one small part one time, and you don’t have the quality of case that our country will take to prosecute as far as espionage.”\(^{79}\) This makes prevention an especially important tactic. I would argue that it would be in the best interests of federal law enforcement agencies, such as the FBI, to take a proactive approach to deterring China’s non-traditional technology collection efforts. The United States government should take steps educate businesses and universities regarding the threat China poses to in attempt to proactively protect information. This approach will likely require fewer and less sophisticated resources than would combating the collection through traditional law enforcement mechanisms. The typical investigation requires not only case agents which specialized counterintelligence skills, but also linguists and analytical, and legal support staff to

\(^{79}\) Eftimiades testimony
successfully bring a case to the point of arrest and prosecution. A proactive approach would ask commercial entities to bear some of this burden.

The United States counterintelligence apparatus cannot focus solely on China’s non-traditional activities. Despite their daunting numbers, for US counterintelligence, non-traditional operations are often the “low hanging fruit” of China’s technology collection operations. In other words, it is relatively easy to detect and dismantle an operation that is so overt in its intentions. It is those operations for which the intentions are disguised through careful operational security and sophisticated tradecraft that pose a particular challenge to US counterintelligence. Substantial resources should be placed on countering China’s clandestine intelligence operations. While there is considerable evidence to suggest that a large part of China’s intelligence operations employ a diffuse approach to collecting information, I argue that to underestimate the importance of the clandestine tradecraft China employs to obtain sensitive information is to misunderstand the most damaging component of China’s intelligence strategy. The information lost in cases of Mak, Chung, Bergersen and Gowadia stand as testament to the damaging effects that China’s clandestine efforts can have on US national security.

In conclusion, China’s approach to collecting intelligence information is often characterized as diffuse, and focusing on relatively open information. This is, at least in part, true. However it should not be forgotten that China is also capable of employing sophisticated, clandestine technology collection operations, which are reminiscent of Western and Russian collection techniques. These operations seek
highly sensitive information, the loss of which can be severely detrimental to the national security of the United States. Understanding both of the methods China uses to collect defense science and technology intelligence is important to protecting US technology from theft, and therefore preserving the United States’ technological advantage.
Works Cited

“Changes the FBI is Making to the Counterintelligence Program,” April 9 2002 (2002) (testimony of David Szady, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation before Congress).


Times online:


"Qing Li Indictment Update." ExportLawBlog. Apr. 11 2009


Report to Congress on Chinese Espionage Activities Against the United States.


Tan Po (3225 3124) “Spy Headquarters Behind the Shrubs—Supplement to Secrets About CPC Spies. OSC FTS19970311001137, Sept 1 1996

Tan Po (3225 3124), “Analysis of CPC Intelligence, Other Organs.” Open Source Center FTS19960901000372


Warrick, Joby, and Carrie Warrick. "Chinese Spy 'Slept' In U.S. for 2 Decades."


Appendix A: Pertinent Statutes

The Arms Export Control Act:
The Arms Export Control Act (AECA), 22 U.S.C. 2778, regulates the export from and import into the United States of “defense articles”1 and “defense services.”2 The State Department, Directorate of Trade Controls (DDTC), promulgates regulations under the AECA, which are known as the International Traffic In Arms Regulations (ITAR). 22 C.F.R. §§ 120-130. The ITAR contains the Munitions List, which sets forth twenty-one categories of defense articles and services that are subject to export licensing controls. Id. at § 121.1. Unless an exemption applies, the ITAR requires a validated export license from the DDTC for the export of Munitions List articles and related technical data3 to all destinations. See 22 C.F.R. §§ 123-125.

The Munitions List:
The defense articles which are subject to such licensing requirements are designated on the United States Munitions List. Those designations are made by the State Department with the concurrence of the Defense Department, under 22 U.S.C. § 2778(a)(1), and 22 C.F.R. § 120.2. The Munitions List is a catalog of designated “defense articles” subject to export and certain import restrictions. Any person who intends to export, or import temporarily, defense articles on the Munitions List from or into the United States, is required to first obtain a license from the DDTC. In the application for an export license, the exporter is required to state, among other things, the nature of the defense articles to be exported, the end recipient of the defense articles and the purpose for which such articles are intended. These factors and others assist the DDTC in determining whether the export of the defense articles would further the security and foreign policy interests of the United States or would otherwise affect world peace. A foreign person, however, may not obtain a license to export an item on the United States Munitions List.

Illegal Exports:
There are three essential elements of an illegal export: (1) the defendant exported, or caused to be exported, from the United States an article listed on the Munitions List or a technology relating to an article on the Munitions List; (2) the defendant did not obtain a license or written approval for the export from the State Department; and (3) the defendant acted willfully. See United States v. Reyes, 270 F.3d 1158, 1169 (7th Cir. 2001).

The ITAR contains a specific definition of what constitutes the export of an item. The following, inter alia, constitute an exportation: (1) sending or taking a defense article out of the United States in any manner; or (2) disclosing (including oral or visual disclosure) or transferring “technical data” to a foreign person, whether in the United States or abroad (sometimes referred to as a “deemed export”). 22 C.F.R. § 120.17.

Economic Espionage Act of 1996:
Public Law 104-294 October 11, 1996 “(a) IN GENERAL.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign
instrumentality, or foreign agent, knowingly— ``(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; ``(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photo- copies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;``(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; ``(4) attempts to commit any offense described in any of paragraphs (1) through (3); or ``(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both. ``(b) ORGANIZATIONS.—Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

Title 18, U.S.C., Section 793(e)
Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.....Shall be fined under this title or imprisoned not more than ten years, or both.
Appendix B: Cases assessed

Chi Mak et al. – Arrested in October 2005. Worked at L3/SPD Technologies/Power systems Group in Anaheim CA, and was granted a US government Secret clearance in 1996. Through his work at Power systems group, Mak had access to classified Navy Technology, and led a project on Quiet Electric Drive (QED) propulsion for use in US Navy warships, which is a sensitive Navy program which was carried the caveat NOFORN, Schedule D, which strictly prohibited its transfer to foreign countries. The indictment alleges that Mak transferred information concerning the QED and other US Government projects from work to home. There, Mak copied information onto disks and delivered them to his brother, Tai, who transported them to China. Mak responded to requests by Chinese government officials.

Chung Dongfan, aka Greg Chung – Arrested February 2008. Chung worked for Rockwell and Boeing from 1973 to 2002. He held a secret clearance while employed by Rockwell Boeing. Chung was arrested Orange County, California in 2006 on charges of theft of trade secrets at Boeing, and conspiracy to give information to a foreign government (China). According to the affidavit, Chung was sent requests by officials and agents of the government of the PRC for information relating to the United States Space Shuttle and military and civilian aircraft, and helicopters. He also traveled to PRC to deliver lectures on technology involving the US Space Shuttle and other programs, and meet with officials and agents of the government of the PRC. He accepted payment for his services. He utilized family members and friends to carry information back to China and sent information through the Education Consul at the Chinese Consulate in San Francisco. His motivation is assessed as both monetary and a desire to help China.

Noshir Gowadia – Arrested in October 2005. In October 2007, Noshir Gowadia was charged in a second superseding indictment in the District of Hawaii with an additional count of transmitting classified national defense information to China and two additional counts of filing false tax returns. Gowadia was charged in a superseding indictment in November 2006 with performing substantial defense related services for China by agreeing to design, and later designing, a cruise missile exhaust system nozzle that renders the missile less susceptible to detection and interception. According to the second superseding indictment, Gowadia initiated contact with Chinese officials in order to sell controlled defense technologies related to the reduction of the infrared heat signatures of aircraft and airborne weapons systems. Gowadia obtained knowledge of these technologies through his former employment at Northrup Corporation.

Reconnaissance (C4ISR) system to Taiwan. Bergerson communicated information to Kuo, who acted as a “cutout” between Chinese intelligence officials in China and Bergersen. Kang also assisted in the transmittal of information to China. Bergersen apparently believed that he was giving information to Taiwan, not China, an act which would still have been illegal, since the information Bergersen relayed was not approved for release to Taiwan, either.

**Meng Xiaodong (Sheldon)** – Arrested December 2006. Meng was employed by Quantum3D, a company which produces high-end visual simulation systems and interactive, open architecture visual computing solutions, image generators and embedded graphics subsystems. Meng took several Quantum3D products with him on trips to China which were regulated by ITAR. Quantum produced products for military purposes, including military combat training in simulated real time conditions during the day and night and the use of Infrared and Electro-optical and Night Vision Goggle devices. Meng sought out clients in foreign countries for Quantum 3D products, in an effort to sell the products without the permission of the company.

**Shu Quan Sheng** – Arrested in September 2008. Shu, a PhD physicist, was charged of illegally exporting space launch technical data and services to China and offering bribes to Chinese government officials. Shu was the President, Secretary and Treasurer of AMAC International, a high-tech company located in Newport News, Va., and with an office in Beijing, China. According to the criminal complaint, around January 2003, Shu provided technical assistance and foreign technology acquisition expertise to several Chinese government entities involved in the design, development, engineering and manufacture of a space launch facility in the southern island province of Hainan, PRC. This facility will house liquid-propelled heavy payload launch vehicles designed to send space stations and satellites into orbit, as well as provide support for manned space flight and future lunar missions. Among those PRC government entities involved in the Hainan space launch facility the People's Liberation Army's General Armaments Department and the 101st Research Institute.

**John Reece Roth** – Arrested in May 2008. Worked at the University of Tennessee as a professor Emeritus and at Atmospheric Glow Technology Inc, a Knoxville-based technology company. The Indictment alleges that Roth conspired to disclose restricted US military data about Unmanned Aerial Vehicles to foreign national without first obtaining the required US government license or approval. Transmitted restricted US defense department data to a PRC student working for him, and did not disclose the student as required by law. Roth traveled to PRC to give talks at Chinese Universities. He also directed a wire transmission to an individual in China a document containing restricted technical data controlled by the ITAR.

**Yaming Nina Qi Hanson** – Arrested February 2009. Hanson was charged on a single count criminal complaint of supplying the PRC with controlled technology without the required license. In August 2008, Hanson knowingly and illegally
exported controlled items to China, consisting of miniature Unmanned Aerial Vehicle Autopilots in violation of the International Emergency Economic Powers Act. The export contained components manufactured in Canada and are the world's smallest UAV autopilots. The items were known as dual use technology and are controlled by the Department of Commerce for export to China.

Qing Li – In September 2008, Qing Li was charged with conspiracy to smuggle military-grade accelerometers from the United States to China. According to court papers, Li conspired with an individual in China to locate and procure as many as 30 Endevco 7270A-200K accelerometers for what her co-conspirator described as a "special" scientific agency in China. This accelerometer has military applications in "smart" bombs and missile development and in calibrating the g-forces of nuclear and chemical explosions.

Feng Yang – In August 2007, Feng Yang, the president of Excellence Engineering Electronics, Inc., pleaded guilty in the Northern District of California to a charge of illegally exporting controlled microwave integrated circuits to China without the required authorization from the Department of Commerce.

William Kovacs - In November 2003, Kovacs, the owner and president of Elatec Technology Corporation in Massachusetts, was charged with illegally exporting a hot press industrial furnace to a research institute in China affiliated with the government aerospace and missile programs.

Ding Zhengxing, Su Yang, Peter Zhu – Indicted in December 2007. Ding, Yang and Zhu were indicted in for Arms Export Control Act violations in connection with an alleged plot to purchase and illegally export to China amplifiers that are controlled for military purposes. The amplifiers are used in digital radios and wireless area networks. Ding and Yang were arrested in January 2008 after they traveled to Saipan to take possession of the amplifiers. Peter Zhu, of Shanghai Meuro Electronics Company Ltd., in China, remains at large.

Joseph Piquet, Thomas Tam – On June 5, 2008, Piquet and Tam were charged with violations of the Arms Export Control Act and the International Emergency Economic Powers Act in connection with a conspiracy to illegally export to China military amplifiers used in early warning radar and missile target acquisition systems. The defendants were also charged will illegally exporting controlled dual-use amplifiers that have military applications. Piquet is the owner and President of AlphaTronX, a company in Port St. Lucie, Florida, that produces electronic components. Tam is a director of Ontime Electronics, an electronics company in China.

Wave Lab - In June 2008, WaveLab, Inc. of Reston, Virginia, was charged with the unlawful export of hundreds of controlled power amplifiers to China. The exported items, which have potential military applications, are controlled and listed on the Commerce Control List for national security reasons. Wave Lab purchased these
items from a US company and assured the company that the products would not be exported from the United States, but would be sold domestically.

**You Wen Zhang, aka Evan Zhang** – Arrested in April 2008. Zhang served as the President and Chief Executive Officer of Zybron Optical Electronics, Inc., an Ohio company involved in the development of high tech commodities, including infrared thermal imaging devices. In February 2007, Zhang illegally exported infrared thermal imaging cameras to Zhi Yong Guo, the managing director of Beijing Shenzhoukaiye System Engineering Technology Research Center in Beijing, China. Zhang pleaded guilty to one count of exporting national security controlled items without obtaining the necessary license in violation of the International Emergency Economic Powers Act and the Export Administration Regulations.

**Jian Wei Deng, Kok Tong Lim, and Ping Cheng** – Indicted October 2008, Jian, Kok, and Ping were charged with conspiring to illegally export to China controlled carbon-fiber material with applications in aircraft, rockets, spacecraft, and uranium enrichment process. According to the indictment, the intended destination for some of the materials was the China Academy of Space Technology, which oversees research institutes working on spacecraft systems for the Chinese government. Jian Wei Ding and Kok Tong Lim are residents of Singapore and affiliated with a Singaporean import/export company known as FirmSpace, Pte Ltd. Ping Cheng is a resident of New York and the sole shareholder of Prime Technology Corporation.

**Ko-Suen Moo and Maurice Serge Voros** – Arrested May 2006. Ko-Suen Moo and Maurice Serge Voros were charged with various violations of the Arms Export Control Act involving the illegal brokering and attempted export of certain defense articles to China, including one F-16 aircraft engine, Blackhawk helicopter engines, cruise missiles and air to air missiles, in They are also charged with conspiracy to export defense articles to China without a license, and money laundering and conspiracy to commit money laundering, in violation Defendant Moo was additionally charged with being a covert agent of the government of China operating within the United States without prior notification to the Attorney General. Moo was an ex-employee of Lockheed-Martin, a major US defense contractor.

**Wen Ho Lee** – Arrested March 1999. Lee was a hydrodynamicist and mathematician who was formerly assigned to the X division of Los Alamos National Lab (LANL), which carried the highest level of security of any division at the lab. It is LANL’s research and development division responsible for the design of thermonuclear weapons. At LANL, he worked on five Lagrangian mathematical codes, also known as "source codes". Two of these codes are classified and were used in the development of various nuclear weapons, including a weapon known as the W-88. The evidence against Lee included a failed polygraph, the fact that he made unreported trips to Beijing, and suspiciously deleted files from his computer. He ultimately pleaded guilty to only one count of mishandling classified information and was released on time served.