STRATEGIC COUNTERINTELLIGENCE AND
APPLICATIONS FOR THE PEOPLE’S REPUBLIC OF CHINA

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

Jonathan Callard, B.A.

Washington, D.C.
November 19, 2010
Copyright 2010 by Jonathan Callard
All Rights Reserved.
TABLE OF CONTENTS

INTRODUCTION ........................................................................................................... 1

COUNTERINTELLIGENCE AND DECISION ADVANTAGE THEORY ......................... 4

STRATEGIC LANDSCAPE .............................................................................................. 9

CHINESE INTELLIGENCE ....................................................................................... 19

U.S. COUNTERINTELLIGENCE ........................................................................... 27

POLICY IMPLICATIONS ........................................................................................ 37

BIBLIOGRAPHY ........................................................................................................ 45
Collection on the United States is one of the top priorities for practically every foreign intelligence agency on the planet.¹ To defend against this vast intelligence threat, the United States has historically relied upon a disaggregated consortium of government entities to carry out counterintelligence. Five years ago, the United States published its first National Counterintelligence Strategy.² Now an annual publication, the Strategy provides “strategic direction and guidance for counterintelligence activities of the United States government.”³ In 2009, for the first time, “integrating counterintelligence” became a mission objective in the United States National Intelligence Strategy as set forth by the Office of the Director of National Intelligence (ODNI).⁴ These developments are congruent with a growing appreciation in the U.S. government of the threat posed by foreign intelligence entities and the need to improve U.S. counterintelligence capabilities.

Creating a more cohesive counterintelligence (CI) apparatus in the United States is a worthwhile endeavor considering the amount of foreign intelligence activity directed against the United States. Publishing the National Counterintelligence Strategy is an important first step, but it is not a strategic doctrine. Because the United

---

¹ The Commission on the Intelligence Abilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States (Washington, March 31, 2005) 486
States is subject to hostile intelligence operations from approximately 140 countries,\(^5\) no single strategy would be sufficient in dealing with the multitude of threats the nation faces. U.S. policy makers and intelligence professionals must prioritize their efforts and resources according to how they perceive these threats.

The focus of this project is to examine the stated goal of the United States to create and employ strategic counterintelligence, and to explore new ideas on how to apply counterintelligence towards the People’s Republic of China (PRC). China’s large and capable intelligence services are a vital component of its national power, and they are targeting the United States. The PRC is considered by most intelligence officials to be the greatest U.S intelligence threat.\(^6\) Former National Counterintelligence Executive (NCIX) Michelle Van Cleave claims that China “maintains some of the world’s most effective intelligence services.”\(^7\) The goal is not to improve counterintelligence for its own sake, but to leverage counterintelligence to give the United States increased strategic advantage.

The main question this project seeks to answer is: how can finite counterintelligence resources and capabilities be better prioritized and utilized to undermine Chinese positive intelligence\(^8\) in a way that is the most advantageous to the United States? This is a tough question because U.S. counterintelligence already seems


\(^8\) The term *positive intelligence* refers to intelligence collected on a foreign target, also known as *foreign intelligence*. Most espionage falls under this category.
to be overwhelmed by Chinese intelligence efforts. However, since this is not merely a law enforcement issue, the United States need not worry about neutralizing all Chinese intelligence operations conducted against her. Rather, a strategic counterintelligence effort could be employed to hinder, influence, or neutralize Chinese intelligence enough to give the United States an edge in the areas of greatest importance.

Due to the secretive nature of intelligence and counterintelligence issues, unclassified empirical data is admittedly scarce. China’s reticence and control of information further frustrate this endeavor. However, there is ample open source information available to assess the overall strategic environment in which U.S. and Chinese intelligence professionals and policy makers operate.

This paper is divided into five sections. First, the concepts of strategic intelligence and counterintelligence are defined within the context of decision advantage theory. Second, some of China’s core national interests are discussed and juxtaposed against conflicting U.S. interests to understand the strategic landscape. The third section explores Chinese intelligence collection activities and how those activities seek to advance Chinese national interests. Fourth, an overview of the U.S. counterintelligence apparatus is provided so that a capabilities comparison can be made. This paper concludes by raising some of the questions that must be considered, and ultimately answered, by policy makers if CI is to ever become truly strategic.
Counterintelligence and Decision Advantage Theory

What is Counterintelligence? As the name implies, the goal of counterintelligence is to undermine an adversary’s positive intelligence capabilities. Despite the several attempts of scholars to rewrite the definition, the original designation from the National Security Act of 1947 (as amended) still holds the most authority:

The term ‘counterintelligence’ means information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.\(^9\)

“Information gathered and activities conducted” means that counterintelligence by its very nature can be both proactive and reactive. Counterintelligence operations can be defensive or offensive; these categories can be again subdivided into passive or active endeavors.\(^10\) See the table below.\(^11\)

---

\(^10\) CI scholars and practitioners often like to distinguish counterintelligence work from security. The argument is that counterintelligence is solely focused on engaging and analyzing an adversary’s intelligence operations. It is thus the responsibility of security to obstruct or hinder the adversary’s ability to collect. However, for the purposes of this paper, security is considered a *passive defensive* form of counterintelligence. For a more detailed description of the distinction between security and counterintelligence see Sherman Kent’s *Counterintelligence for National Security*, available at [https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm](https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm). Or for a concise metaphorical explanation see former NCIX Joel Brenner’s speech entitled “Strategic Counterintelligence” to the American Bar Association Standing Committee on Law and National Security (Washington: March 29, 2007).
\(^11\) Table categories based on a lecture given by Jennifer Sims at Georgetown University (Washington, DC: April 13, 2010)
The theory that has come to dominate thinking on intelligence issues is that of decision advantage. As articulated by intelligence expert Jennifer Sims, decision advantage comes when one nation (or entity) provides critical information faster and more effectively to its policy makers than the adversary, thus providing the decision maker with timely and relevant intelligence to inform decisions.\(^\text{12}\) According to Sims, in order to achieve decision advantage a state’s intelligence services must do four things better than its opponent: collection, anticipation, transmission, and denial and deception. A superior service needs to collect intelligence, but it should not be expected to be omniscient. The superior intelligence service needs to anticipate significant events, but it is not expected to predict every major world event in advance. Collecting intelligence and anticipating significant events would be worthless, however, if the state’s decision makers do not receive the information in a timely, digestible manner.

and trust the information’s relevance. Lastly, the superior intelligence service is able to keep its intelligence secret (denial) while manipulating the intelligence process of its competitor (deception).

To best an opponent, states focus on optimizing the four functions (collection, anticipation, transmission, and denial and deception). However, a state can also strive to undermine their opponents’ ability to carry out those functions. This is the essence of counterintelligence, and Sims characterizes it as countercollection, counteranticipation, countertransmission, counterdenial and counterdeception. Decision advantage theory is not used merely for its utility in framing counterintelligence as a competition, but because it is the chosen paradigm of the ODNI.

Strategic intelligence is an elusive term that needs to be understood before one can define strategic counterintelligence. In his critique of America’s obsession with current intelligence, John G. Heidenrich has argued that the concept of strategic intelligence is often misunderstood, even among intelligence professional. Heidenrich defines strategic intelligence along the same lines as the Department of Defense (DoD) in that it is intelligence necessary to formulate a grand strategy. This

---


16 JP 1-02, 509 states that Strategic Intelligence is “intelligence that is required for the formulation of strategy, policy, and military plans and operations at national and theater levels.”

17 Heidenrich, 16
parsimonious definition carries more explanatory power when taken in the modern American political context. Policy makers are very busy people and are usually only concerned with intelligence that will help them make their next decision. In practice, American policy makers have little incentive to consume strategic intelligence.\footnote{18} U.S. policy makers are mostly politicians or political appointees whose strategic timeline rarely extends beyond the next election cycle. This lack of demand for strategic intelligence by policy makers has led to a decreased supply by the U.S. intelligence community.

Although strategic intelligence may struggle to retain its status in modern practice, at least the conceptual framework is solid and has a long history dating back to Sherman Kent’s seminal work in 1949.\footnote{19} Strategic counterintelligence, on the other hand, is still theoretically underdeveloped and not practiced in the United States. Michelle Van Cleave has found it particularly troubling that counterintelligence has not been afforded the same status as a strategic tool. She states:

For if strategic intelligence takes as its touchstone the whole of state interests and the sources of state power, then understanding the purpose and manner in which other states use their intelligence resources to gain advantage and \textit{mastering the capability to counter them} [emphasis original] would seem to be the other side of the strategic intelligence coin.\footnote{20}

\footnote{18} Ibid
\footnote{20} Michele Van Cleave, ”Strategic Counterintelligence: What Is It, and What Should We Do About It?” \textit{Studies in Intelligence} Vol.51 No.2
Van Cleave’s frustration is apparent. If intelligence is a competition where advantage is sought by competing states, then CI should be just as important as positive intelligence; like positive intelligence, CI can also be a source of state power.

Van Cleave provides a succinct definition of strategic counterintelligence. She states that strategic counterintelligence has “the potential for engaging CI collection and operations as tools to advance national security policy objectives.”\(^{21}\) In order to align the theories behind strategic intelligence and strategic counterintelligence, a reconciliation is needed. Therefore, strategic intelligence is defined in this work as intelligence needed to formulate strategy, and strategic counterintelligence is intelligence needed to frustrate the strategy of a competitor.

This project hypothesizes that the concept of strategic intelligence can be employed by reallocating CI resources according to the competing interests of a nation and one of its competitors, in this case between the United States and China. The PRC collects intelligence against the United States on a variety of targets using an array of methods to achieve many different aims. Some of those aims are in direct opposition to U.S. interests and national security, while other Chinese aims are less threatening. For example, Chinese intelligence services actively target U.S. defense and dual-use technologies to augment the capabilities of the People’s Liberation Army (PLA). These same services also spy on and intimidate Falun Gong members, Dalai Lama supporters, and pro-democracy Chinese dissidents living on U.S. soil. While these are both

\(^{21}\) Ibid, 2
Chinese positive intelligence endeavors and the responsibility of U.S. counterintelligence to address, they need not be given equal value. As Jennifer Sims has argued in regards to CI, “One is tempted to try to defend everything and thus to defend nothing adequately.”

This paper focuses primarily on CI issues regarding Chinese human intelligence collection (HUMINT). The reason for this is twofold: 1) the availability of data on Chinese HUMINT operations far exceeds any other collection discipline (i.e. signals intelligence or imagery intelligence); and 2) China relies disproportionately on HUMINT over other collection disciplines. HUMINT is not cheap, but it is still the most inexpensive way to collect intelligence. China is a developing country with over 1.3 billion people, so it should be no surprise that Chinese intelligence seeks to leverage its human resources. China’s cyber capabilities are also an important function of its intelligence collection but beyond the scope of this paper.

**Strategic Landscape**

This section explores some of the key issues that define the U.S.-China security relationship. According to decision advantage theory, intelligence should be viewed in the context of a competition among states or entities. A good intelligence service needs to clearly communicate to its decision makers the nature of that competition and the

---


character of the competitors. The competitor under consideration is the People’s Republic of China. The U.S.-Chinese relationship is complicated and describing it in depth is well beyond the scope of this paper. However, the following section is necessary to demonstrate the main points of contention between the two nations. This sets the framework of the competition in which each state’s intelligence services vie for advantage, in part by setting strategic priorities.

China’s positive intelligence collection against the United States is a critical national security issue. China’s economy has sustained annual economic growth rates of eight percent or higher for the last 30 years and is now the world’s second largest economy. What China does with its growing power, and how it interacts with its neighbors, the international community, and the United States, are all matters of grave importance for the whole world. A recent study done by the Center for Strategic and International Studies argues, “The direction that China and U.S.-China relations take will define the strategic future of the world for years to come.” China’s rise presents serious challenges for the United States and although there are many potential venues for cooperation, there are also areas of competition and opportunities for conflict.

The U.S. government came to appreciate this intelligence threat in the late 1990s. The 1999 Congressional study entitled *U.S. National Security and Military/Commercial Concerns with the People’s Republic of China* (also known as the Cox Report) was an

---

alarming account of the depth and breadth of Chinese economic, industrial, and political espionage against the United States.\textsuperscript{26} Shortly thereafter, in the fall of 2000, the U.S.-China Economic and Security Review Commission was created by Congress. The purpose of its three-to-four-hundred page annual reports is to investigate “proliferation practices, economic transfers, energy, U.S. capital markets, regional economic and security impacts, U.S.-China bilateral programs, WTO compliance, and the implications of restrictions on speech and access to information in the People’s Republic of China”\textsuperscript{27}

In 2000 the Department of Defense also began its annual China publication. The\textit{ Annual Report to Congress on Military and Security Developments Involving the People’s Republic of China} takes a detailed look at China’s military modernization. The Office of the National Counterintelligence Executive examines Chinese intelligence activities in its annual\textit{ Foreign Economic Collection and Industrial Espionage Report}. These studies, in both classified and unclassified forms, have done much to educate U.S. leaders and the public about Chinese espionage. The key purpose of enhancing American understanding of Chinese intelligence is to devise ways of improving U.S. counterintelligence.

In order for U.S. counterintelligence to frustrate the strategy of this competitor, must it be assumed that the United States knows what Chinese strategy is? There can be no presumption of truly knowing what Chinese \textit{grand} strategy is. However, China has several national strategies that can be understood independently: a security strategy,

\textsuperscript{26} U.S. House Select Committee on US National Security and Military/Commercial Concerns with the People’s Republic of China[Cox Committee], 105th Cong. 2d Session, 1999
\textsuperscript{27} U.S.-China Economic and Security Review Commission, iii
a development strategy, and a unification strategy, among others. Chinese security strategy includes developing area-denial capabilities aimed at the United States. The development strategy aims at moving from a low-end manufacturer to a high-tech manufacturer – with the help of stolen technologies. China’s unification strategy includes the ability to quickly overwhelm Taiwan while displaying enough force to deter U.S. intervention. The overarching theme behind these strategies is the Chinese belief that the first several decades of the 21st century will be a time of “strategic opportunity” in which China can develop economically without any eminent foreign-based national security threats.28

The competition is a complex and paradoxical one. The United States objectively profits economically from trade and investment in China. This trade and investment contributes to China’s rapid economic development. China’s economic development then leads to increased military power. This increasing Chinese military power then has the potential to threaten U.S. interests in East Asia.29

China’s faces a similar predicament when dealing with the United States. China feels strategic pressure, or “containment” from the United States. China feels that the strategic pressure can only be reduced if the United States has an economic decline that leads to U.S. military atrophy. However, a U.S. economic downturn would greatly

affect China’s economy as well, and the resulting geopolitical changes would create an uncertain world that might not necessarily be favorable to China.  

Essentially, the United States and the PRC each have a vested interest in each other’s stability. This is not a Cold War-like showdown with nuclear holocaust implications, but the stakes are still high. A closer look at China’s core national interests merits further discussion, as well as where those interests are in conflict with those of the United States.

As with any single-party authoritarian regime, staying in power is the Chinese Communist Party’s (CCP) first priority. As China expert David Shambaugh puts it, “maintaining the CCP in power is the bottom line.” Therefore, this paper will consider Chinese “interests” through the lens of the CCP, meaning anything that reinforces CCP rule. The traditional form of CCP legitimacy was derived from communist ideology and the cult of personality surrounding Chairman Mao Zedong. However, after Mao’s death and the subsequent economic reforms implemented by Deng Xiaoping that ideology was mostly forsaken. In its place, the CCP focused on what has commonly known as the “twin pillars” of economic growth and nationalism. A failure in either category could possibly lead to the demise of the Party. Although

__________________________

30 Ibid, 1
economic development and nationalism cannot by themselves explain how the Party remains in power, they remain the two key sources of CCP legitimacy.\textsuperscript{32}

On the surface, it would seem that these two sources of legitimacy are relatively benign and little cause for concern. However, there are serious implications that come with China’s economic development and the manner in which Beijing seeks to sustain prosperity. Furthermore, the nationalistic fervor which the CCP has fostered for the sake of Party legitimacy also acts to limit the flexibility of Chinese policy makers when dealing with sensitive issues such as Taiwan. This paper analyzes China’s national interests within the context of the two major “pillars” of CCP’s claim to legitimacy – economic development and nationalism.

\textit{Economic Development}: China’s first national priority is economic development, particularly by using industrialization based on technology.\textsuperscript{33} The PRC is trying to acquire more technology, by any means available, to aid in its economic development. Despite the population difference, the United States has five times more researchers dedicated to, and invests nearly four times more money in, scientific research and development than the PRC.\textsuperscript{34} Although China actually exports more high technology goods than the United States,\textsuperscript{35} it still does not have the capability to design and develop indigenous technologies at the level that most developed countries can. As will be

\textsuperscript{32}Ibid, 3
\textsuperscript{33}Zheng Bijian, “China’s ‘Peaceful Rise’ to Great Power Status.” \textit{Foreign Affairs}, vol.84 no.5 September/October 2005
\textsuperscript{34}Based on World Bank Data, accessible at: http://data.worldbank.org/indicator/SP.POP.SCIE.RD.P6/countries/1w-CN-US?display=default
discussed further below, the Chinese government actively sponsors, organizes, or otherwise encourages the theft of foreign technologies and trade secrets. The PRC fuels its economic growth in part with stolen technology and other trade secrets that Americans have paid large sums for in research and development.\textsuperscript{36}

China’s economic development is contingent upon its ability to use the oceans. U.S. Navy Rear Admiral Michael McDevitt said it plainly, “because China’s economic health depends upon unimpeded access to and use of the high seas, Beijing has been forced to think more seriously about how to secure its maritime frontier.”\textsuperscript{37} Ninety percent of China’s trade is transported by sea.\textsuperscript{38} Overseas oil imports and maritime resources such as hydrocarbons, minerals, and fishing also add to the importance of a safe maritime environment.\textsuperscript{39} Chinese shipping would be highly vulnerable in the event of a military conflict with a major power, especially since approximately eighty percent of China’s oil imports travel through the Straits of Malacca.\textsuperscript{40} These vulnerabilities are a major motivation in the expansion and modernization of the People’s Liberation Army Navy.

\textit{Nationalism:} Chinese nationalism comes with some dangerous components, one of them being a quest for great power status. Ever since the “Century of

\begin{itemize}
\item\textsuperscript{37} Michael McDevitt, “PLA Navy Building: Rationale and Prospects for the Future” \textit{Asia Policy} no.4(NBR, Washington: 2007)
\item\textsuperscript{38} Jonathan Holslag, “Embracing Chinese Global Security Ambitions” \textit{The Washington Quarterly} 32 no.3, July 2009
\item\textsuperscript{39} U.S.-China Economic and Security Review Commission, 114
\item\textsuperscript{40} Ibid, 115
\end{itemize}
Humiliation” when China was dominated by foreign powers, from the Opium Wars until Communist victory in 1949, the PRC has been eager to reclaim its status as a leading world power. Now that China is the world’s second largest economy, it seems having a military power to match would be the next logical step. David Shambaugh argues that China’s interest in “becoming a global power” is one of two main contextual drivers pushing for the PLA’s military development.41 The other contextual driver is Taiwan.

Much has been published concerning the areas where Chinese national interests are at odds with those of the United States. Robert Sutter argues that the biggest issues the Chinese have with the United States are (in order of importance) 1) U.S. support for Taiwan; 2) U.S. efforts to change China’s political system; and 3) United States playing the dominant strategic role in China’s periphery.42 This assertion is compelling because it is based solely on official Chinese government statements and Chinese news media. Both the Taiwan issue and U.S. strategic presence on China’s periphery are particularly important because those two issues have the most potential to induce conflict.

Taiwan’s independence would be considered a direct affront to the PRC’s sense of sovereignty and, due to the fervent nationalism attached to the issue, could potentially undermine the legitimacy of the Chinese Communist Party. Chinese nationalism is carefully cultivated by the state. Starting at a young age, each Chinese

---

school child is taught that Taiwan is an unalienable part of China. This notion has been embraced and reinforced to the point that if China “lost” Taiwan to formal independence it would be a political catastrophe for the CCP and could threaten the entire government. Chinese nationalism thus inhibits the CCP’s political flexibility with Taiwan and might someday instigate a conflict. The PRC has made it clear that it will use force to reclaim Taiwan if it should declare formal independence.\textsuperscript{43} The United States has conveyed that it would protect Taiwan if it was attacked by the Mainland. Expecting U.S. interference, China has been steadily developing area denial capabilities within the People’s Liberation Army and the PLA Navy that can inhibit United States access to the region in the event of a crisis.\textsuperscript{44}

The U.S. military presence along China’s periphery is an affront to Chinese nationalism and inhibits the Chinese sense of security. There are American troops stationed in South Korea, Japan, Guam, and now Afghanistan. The United States has mutual defense treaties and/or other military cooperation with South Korea, Japan, Australia, Thailand, Philippines, Taiwan, and several countries in Southeast Asia. The U.S.-India nuclear cooperation deal, first announced by President Bush and Prime Minister Singh in 2005 and approved by Congress in 2008, is understandably seen by China as a geostrategic decision and part of a larger “containment” strategy in Washington. Chinese sensitivities to U.S. military presence were made very clear in the run up to the joint U.S.-South Korean naval exercises in July, 2010. Originally planned

\textsuperscript{44} U.S.-China Security and Review Commission, 144
to take place in the Yellow Sea, the joint exercise aimed at North Korea had to move to
the other side of the Korean Peninsula, to the Sea of Japan, because of vehement
Chinese opposition. A Chinese Foreign Ministry spokesman was quoted saying, “We
resolutely oppose any activities in the Yellow Sea that may threaten Chinese
security.”

In addition to maintaining legitimacy through economic development and
nationalism, the CCP feels a critical need to control information and silence dissent.
This is a difficult job. For example, in each of the last four years there have been
approximately 90,000 reported protests or disturbances across the Chinese mainland.

Keeping these protests separated and out of the mainstream news requires a
concentrated, state-driven effort. The PRC carries out this mission both at home and
abroad as its intelligence officers and consular officials actively conduct surveillance
and harassment of Chinese dissidents residing in foreign countries, including the United
States.

The PRC’s fundamental national interests of security and economic stability are
not unlike most nation states. However, China, being nearly encircled by the U.S.
military presence in Asia, has cause to feel insecure in the current strategic landscape.
The United States wants to maintain that military presence and the Chinese would like

---
45 Chico Harlan, “South Korea and U.S. send Message to North Korea with Drills in Sea of Japan” The
dyn/content/article/2010/07/25/AR2010072500754.html
46 The Economist, “China’s Succession: The Next Emperor” (October 21, 2010) accessed at:
http://www.economist.com/node/17308123?Story_ID=17308123&fsrc=nlw|hig|10-21-
2010|editors_highlights
47 Ibid, 166
to see it dissipate. Furthermore, the CCP’s need to sustain its domestic legitimacy makes China overly dependent on economic growth, nationalism, and controlling political dissent; often in conflict with American interests. These are some of the forces driving Chinese strategy. The following section examines the way in which Chinese intelligence agencies seek to further their national interests.

**Chinese Intelligence**

Like any nation, China seeks to utilize political, economic, and military intelligence to make informed policy decisions. However, China’s unique political situation, along with its culture, history, human capital, and overall place in the world as a rising power have interesting implications for Chinese intelligence targets and collection methods. The U.S.-China Economic and Security Review Commission classifies Chinese intelligence collection into four categories: 1) “professional” intelligence sponsored and directed by Chinese agencies; 2) “actuarial” intelligence amassed together from a vast array of sources; 3) “enterprise-directed” theft of controlled technologies driven by Chinese state scientific research and development and military-industrial sectors; and 4) “entrepreneurial” industrial espionage and illegal technology exports carried out by private actors.48 Using the four categories as a framework, this section analyzes Chinese intelligence in terms of both actors and methods.

---

48 U.S.-China Economic and Security Review Commission, 154
The modern Chinese intelligence infrastructure was born out of a civil war. Prior to 1949, the CCP’s intelligence service was known as the Central Department of Social Affairs and its primary intelligence target was Chiang Kai-shek’s Kuomintang army. After the communists won the civil war, the organization became known as the Central Investigation Department (CID). The Central Investigation Department was abolished during the Cultural Revolution, and its duties were taken on by the military. Deng Xiaoping was originally removed from authority in 1976 with the help of CID cadres, which explains why he was reluctant to reinstate the organization after he came back into power.\textsuperscript{49} Regardless, the body was eventually remade in 1983 by combining the espionage, counterintelligence, and security functions of the Ministry of Public Security with the original investigation functions of the CCP central committee; renamed the Ministry of State Security (MSS).\textsuperscript{50} The MSS is and has been from its inception a Party organization.

Today the MSS is highly U.S. focused, as is evident by the organizations leadership. In March 2008, the CCP leadership appointed Geng Hui-chang to be Minister of the MSS. Mr. Geng, who is also a member of the powerful central committee of the CCP, was previously the vice minister of the MSS.\textsuperscript{51} Geng is a career intelligence professional and an America expert. Geng had also served as director of the University of International Relations and chaired the American Studies

\textsuperscript{50} Nicholas Eftimiades, \textit{Chinese Intelligence Operations}, (Annapolis: Naval Institute Press, 1994)
The fact that Mr. Geng is an America expert is an indicator of how important the United States is as an intelligence target.

China has an impressive “professional” human intelligence capability. This includes sending professional intelligence officers abroad to recruit assets in foreign countries. These professional intelligence officers come in all the traditional forms: embassy staff with diplomatic immunity under “official cover;” businessmen and women under “commercial cover;” and the Chinese are known to use journalistic cover (primarily through the state-run Xinhua news agency).

Chinese intelligence has become highly skilled in the use of front companies. The FBI believes there could be as many as 3,000 Chinese front companies currently operating in the United States. In 2007, it was discovered that one of these companies gained access to a secret National Security Agency (NSA) listening post in Hawaii. A Chinese translation company set up by the MSS was able to secure a contract with the U.S. Navy and NSA to translate intercepted communications. The company had worked on hundreds of thousands of intercepts before the breach was discovered. Not only did this operation give incredible access to U.S. SIGINT targets, sources, and methods, but it also allowed the MSS to taint the intelligence it translated and tailor it to China’s benefit. As the Hawaii operation grew, it began attempts to recruit Chinese-

---

52 [http://www.chinavitae.com/biography/3969](http://www.chinavitae.com/biography/3969)
54 [Stratfor](http://www.stratfor.com)
American Navy and civilian intelligence officers to spy for the MSS. Officials discovered this recruitment program in Hawaii when a Navy cryptographic technician was caught accepting free trip to China paid for by Beijing.

China’s People’s Liberation Army also conducts extensive intelligence operations. The Second Department of the Chinese General Staff (2nd PLA) oversees military HUMINT operations with both clandestine officers and overt military attachés. 2nd PLA is believed to focus its espionage activities on acquiring military technologies. The PLA also boasts the Asia Pacific’s most extensive SIGINT apparatus, operated by the General Staff’s Third Department and the General Staff’s Electric Countermeasures and Radar Department. The Military Intelligence Department’s main consumer is the Central Military Commission.

Another important intelligence collector is the CCP International Department (formerly the International Liaison Department). Very little scholarship has been devoted to this organization but it is a very important producer of political intelligence worldwide. The International Department (ID) is not necessarily a covert organization but it is involved in intelligence collection. In the past it had acted as a “missionary of revolution” by smuggling weapons to insurgent groups, acting as a propaganda agent, andconducting other forms of covert action. Today it is believed to be much tamer.

56 Mark A. Stokes, “China’s Strategic Modernization: Implications for the United States,” Strategic Studies Institute, Sept. 1999, 33
57 Ibid
and less powerful than in the past, but members of this Party organization still operate clandestinely in foreign embassies all over the world. The ID is solely a Party organization. It is able to maintain close relations with foreign minority and opposition parties, beyond official government relations, giving the ID excellent insights into the domestic political situation in countries where it operates. Experts also assume, although there is a lack of hard evidence, that ID attachés work closely with undercover MSS personnel abroad for intelligence collection and agent recruitment. What is clear is that the International Department of the Chinese Communist Party is in its own right a quality collection and analytic body for some of China’s best political intelligence.

Chinese intelligence cannot be understood by merely studying the actors involved; a closer look at their methods is necessary. Chinese intelligence collection is best known for its “actuarial” or “grains of sand” technique. This method is simply recruiting Chinese nationals who were already planning on going abroad as low-level “agents”.

These low-level collectors are under the supervision of the provincial MSS office, which is responsible for locating and recruiting the travelers. Many students, scholars, and businesspeople fall under this category. They often receive very little training, and are given very vague collection requirements. These travelers could be tasked to join dissident groups abroad in order to report on their activities, to report on business dealings of foreign companies, to gain access to scientific research, or to acquire a legal (but restricted for export to China) technology. According to a recent

59 Ibid, 32
60 Ibid, 45
61 Nicholas Eftimiades, 61
report by the private intelligence firm Stratfor, the Federal Bureau of Investigation (FBI) believes there could be hundreds of thousands of such agents currently in the United States.62

Slightly more sophisticated than “actuarial,” but not quite a professional intelligence technique, is “enterprise-directed” collection. The PRC often uses professional scientific visits, delegations, and exchanges to gather sensitive technology.63 The standard operation goes something like this: a scientific delegation is invited to China to attend a conference, symposium, or for a similar academic purpose. Upon arrival, the delegation is treated with superb hospitality but kept on an exhausting tourist schedule. The foreign guests are treated to fine meals with copious amounts of alcohol. With the combination of fatigue and alcohol setting in, the hosting scientists (often including intelligence officers) begin the battery of probing questions to illicit slip-ups from the unsuspecting foreigners. Meanwhile, Chinese intelligence personnel are rummaging through the hotel rooms of the visiting delegation, searching computers, suitcases, and phone messages.64 To help Chinese intelligence in this effort, many of the finer hotels in China are sufficiently bugged with listening devices already.65

The Chinese also send their scientists abroad on collection missions, utilizing the same techniques but with fewer resources at their disposal. The Cox Committee reported that the PRC acquires technological information through open forums such as

---

63 Cox Committee, 39
64 Cox Committee, 40
65 Stratfor, 8
arms exhibits and computer shows. In one case, a Chinese group stole a videotape displaying information on the U.S. Theater High Altitude Air Defense system while the Defense Department contractor left the booth unattended. 66 PRC scientists could then analyze the video frame-by-frame to gleam valuable intelligence. This type of espionage is not to be underestimated. In a congressional testimony, Chinese intelligence expert Nicholas Eftimiades claimed that “China’s most productive method of legally acquiring foreign technology is to send scientists overseas on scholarly exchange programs.” 67

Chinese intelligence agencies and government organs also try to monitor, influence, and harass dissidents living abroad. Chinese consular officials who have sought asylum in both the United States and Australia and have testified that MSS Officers have traveled to the embassies in Washington and Canberra for such purposes. 68 A Chinese defector to Australia produced an internal PRC document listing the “Five Poisonous Groups” of Falun Gong, Tibetan separatists, Uighur separatists, Taiwan independence activists, and pro-democracy activists. The document prescribed consulates with counter-strategies including increased monitoring and propaganda. 69 Chinese consulates in Australia levied quid pro quo economic pressure on Australian officials in an effort to undermine Falun Gong members. In 2008 a Falun Gong affiliated newspaper reported that PRC consular officials organized a series of assaults

66 Cox Committee, 41
67 Nicholas Eftimiades, Testimony before the Joint Economic Committee, United States Congress, May 20, 1998
68 U.S.-China Economic and Security Review Commission, 163
69 Ibid
against Falun Gong members in New York City.\textsuperscript{70} While actions like these may not directly affect U.S. national security interests, they are a sanctioned use of PRC intelligence resources on American soil that are of inherent interest to U.S. counterintelligence.

There are many recent cases that demonstrate the techniques listed above. Details of the cases of Chi Mak, “Greg” Dongfang Chung, Peter Lee, Wen-ho Lee, Gregg Burgersen, James Fondren, and others are all well documented and analyzed elsewhere. What is important for this analysis is how these spy cases further Chinese national interests at the detriment to U.S. national security. Chi Mak was an engineer working for Power Paragon, a U.S. defense contractor. Chi Mak provided the PRC with secret information on “Quiet Electric Propulsion” technology to be used in future U.S. Navy warships.\textsuperscript{71} “Greg” Dongfang Chung worked for Boeing and betrayed secrets relating to Boeing military aircraft and space shuttle technology; Chung even used Chi Mak as a courier for the stolen information.\textsuperscript{72} Peter Lee worked at Lawrence Livermore Laboratory and at the defense contractor, TRW. Lee had confessed to giving the Chinese sensitive naval technology related to detecting submarines under water, and he is suspected of passing on nuclear technology as well.\textsuperscript{73} By the late 1990s the PRC had stolen classified information on every currently deployed thermonuclear warhead in the

\textsuperscript{70} Ibid, 164
\textsuperscript{71} U.S.-China Economic and Security Review Commission, 155
U.S. ICBM arsenal. These are just some of the highlights from a very long list of counterintelligence losses to the Chinese, and each year the U.S. Department of Justice is flooded with Chinese economic espionage cases and illegal exporting of controlled items.

**U.S. Counterintelligence**

The counterintelligence challenges the PRC poses for the United States are severe. Chinese intelligence operations enjoyed relative impunity in the United States throughout most of the Cold War. With the Soviet Union seen as the existential threat, the Soviets claimed the vast majority of U.S. intelligence and counterintelligence efforts. It was not until after the Cold War that the United States could finally confront the magnitude of Chinese efforts. U.S. counterintelligence is still playing catch-up.

Despite the recent push for a more comprehensive, cohesive, and strategic effort, U.S. counterintelligence infrastructure remains, according to the WMD Commission Report, “fractured, myopic, and only marginally effective.” American CI has historically been reactive, defensive, and threat based. Whether it is in response to German saboteurs during World War I, Nazi sympathizers in WWII, or Soviets throughout the Cold War, ambivalence among senior policy makers in Washington

---

74 Cox Report, Chapter 2, page 68
75 Eftimiades, 5
76 The Commission on the Intelligence Capabilities of The United States regarding Weapons of Mass Destruction, Report to the President of the United States, March 31, 2005, 486
prevailed until specific threats were eminent. The FBI, Central Intelligence Agency (CIA), and military services were given considerable leeway to independently define their own counterintelligence missions and the manner in which they would execute those duties.

U.S. counterintelligence responsibilities are divided between the FBI, CIA, and DoD. Each entity has different equities and conducts counterintelligence to suit its own needs. This is partly by design and partly because of bureaucratic practice. A closer look at the individual agencies responsible for the collective U.S. counterintelligence mission merits further discussion in order to assess its strengths and weaknesses in comparison to Chinese positive intelligence collection.

*Federal Bureau of Investigation:* The FBI is America’s premier CI agency. In 1917, it was formally given responsibility “for identifying and neutralizing ongoing national security threats from foreign intelligence efforts”. Today the counterintelligence division is housed within its National Security Branch, along with the counterterrorism division and the directorate of intelligence.

Since WWII, the FBI has won the lion’s share of counterintelligence resources. Approximately three quarters of the total U.S. counterintelligence budget has been

---

78 Ibid, 73
79 Michelle Van Cleave, “Counterintelligence and National Strategy,” 12
allocated for domestic efforts and is thus entrusted to the FBI.\textsuperscript{81} Counterintelligence has moved to the FBI’s second mission priority after combating terrorism. The top three priorities within the counterintelligence division are counterespionage, counterproliferation, and countering economic espionage.

Since September 11, 2001, the FBI has tried to enhance its intelligence capabilities and improve intelligence management. Efforts included greatly increasing the number of analysts and linguists dedicated to intelligence and counterintelligence.\textsuperscript{82} Building on steady enhancements in the counterintelligence division workforce since 2002, there are now counterintelligence squads in all 56 FBI field offices.\textsuperscript{83} However, managing 56 counterintelligence divisions in a concerted, cohesive manner is still a challenge for the Bureau. FBI culture runs counter to central counterintelligence management. A FBI inspector general report conducted in 2006 found that many FBI Headquarters managers believed that they could not interfere with field office’s counterintelligence operations.\textsuperscript{84} This “hands off” approach essentially transformed Headquarters’ management role into a support role as managers were instructed to say “yes” to whatever the field office asked for unless the field’s actions contravened specific rules.\textsuperscript{85} The inspector general report listed this lax management style as one of

\textsuperscript{81}Van Cleave, “Counterintelligence and National Strategy,” 13
\textsuperscript{82}Sean Joyce, Executive Assistant Director of FBI National Security Branch, in a speech at Bipartisan Policy Center, October 6, 2010.
\textsuperscript{83}FBI Director Robert Mueller III, Testimony before U.S. Senate Judiciary Committee, December 6, 2006.
\textsuperscript{84}U.S. Department of Justice, Office of Inspector General. “A Review of the FBI’s Handling and Oversight of FBI Asset Katrina Leung.” Unclassified Executive Summary. May, 2006. 4
\textsuperscript{85}Ibid, 13
the contributing factors to the massive counterintelligence failure with the FBI asset Katrina Leung.\textsuperscript{86}

The FBI actively seeks to identify and survey foreign intelligence operatives. Whenever possible, the FBI will try to recruit foreign intelligence personnel to act as FBI assets. Double agent and dangle\textsuperscript{87} operations are also within the Bureau’s operational realm. It is through this kind of offensive counterintelligence collection that the FBI can undermine foreign positive collection. It was after the FBI had identified the KGB’s “order of battle” in the United States in the mid 1980s that President Reagan decided to expel a number of Soviet diplomats. Among the diplomats expelled were the KGB’s most effective intelligence officers; the less-competent officers were allowed to stay.\textsuperscript{88}

It is the Bureau’s responsibility to oversee the integration of its own law enforcement and intelligence responsibilities,\textsuperscript{89} but these are often competing interests with counterintelligence. For example, in a case where there is an employee within a U.S. intelligence organization who is selling information to a foreign government, an intelligence officer might want the employee fired right away to stop the leaking of

\textsuperscript{86}Katrina Leung was an FBI asset on China from 1982 until 2000. Throughout most of that time she was engaged in secret sexual relationships with two FBI Special Agents working in counterintelligence and turned out to be a double agent under the control of the Chinese MSS.

\textsuperscript{87}A dangle is a form of double agent operation but with different intentions. Where traditional double agent operations are for the purpose of providing false or misleading information to deceive an adversary service, dangle operations are used to collect information on the enemy service itself. By allowing a foreign service to recruit a dangle, the adversary’s methods of operation can be observed. Equally important, the employing service can surmise what the adversary knows and does not know based on what questions the adversary asks the dangle.

\textsuperscript{88}Godson, 111

\textsuperscript{89}FBI Director Mueller Senate testimony, October 6, 2006
classified information. Law enforcement, on the other hand, would need to allow the activity to carry on unhindered while evidence is collected and a legal case is constructed. Another common conflict often arises within the same given scenario. Perhaps law enforcement has already collected enough evidence and wants to make an arrest for the serious crimes committed, but counterintelligence wants to allow the activity to continue so that it can manipulate the information being passed to the foreign government. These are very common dilemmas that must be considered in almost any counterintelligence operation. The FBI has its own internal mechanisms for determining how an investigation should end, but it is an ongoing challenge and cause for friction within the Bureau.

Another important aspect of the Bureau’s CI mission is public outreach. The FBI maintains what it calls “strategic partnerships” with the private sector and academia. Individual FBI field offices join local chambers of commerce and provide various security briefings. There are also national partnership programs with the business community and university research institutions that aim to enhance security and awareness of foreign intelligence threats. Educating the private sector is important because without a clear understanding of foreign intelligence practices and targets private companies may not be inclined to make the necessary investments in security and CI. The same is true for universities and research institutions because foreign students often act as intelligence collectors on the United States.

---

Central Intelligence Agency:  

In 1947, the National Security Council Intelligence Directive No.5 stipulated that FBI’s counterespionage authority stopped at the nation’s borders, and that CIA was responsible for all foreign espionage and counterespionage. However, after the departure of CI legend James Angleton, the CIA has not been particularly interested in counterespionage. This separation of authority has created an opportunity for foreign governments to conduct hostile intelligence operations against the United States abroad. The Russians and the Chinese both have always preferred to meet recruited American assets in locations outside of the United States and beyond the reach of the FBI. The Soviets particularly favored Mexico City and Vienna for much of the Cold War while the Chinese still prefer to recruit whenever possible from China.

It is difficult to have an effective offensive CI capability when the CIA does not make it a priority. In a way, the CIA may have never fully recovered from the legacy of James Angleton. Angleton was the head of CIA counterintelligence office for over twenty years. A life in the murky world of CI, coupled with the defection of his close personal friend Kim Philby, led Angleton to conduct wide sweeping mole hunts

92 Godson, 104
93 The Felix Bloch case demonstrates this challenge. The FBI suspected Bloch might be meeting his Soviet handler in Paris and asked the French DST to conduct surveillance. DST videotaped the asset/handler meeting but it was inadmissible evidence in a U.S. court. See David Wise, Spy (New York: Random House, 2002).
94 Godson, 111
95 Kim Philby was the U.K. intelligence liaison officer assigned to the United States. He was one of the “Cambridge Five” and spied for the Soviet Union for decades before defecting in 1963.
within the agency. This paranoia damaged many careers and seriously undermined agency morale. For this reason, CIA director William Colby asked Angleton to resign in 1974. After Angleton’s departure, the Agency’s CI staff was drastically reduced. The stigma of Angleton had a lasting effect on the way that CIA viewed and attempted to use CI.

The CIA’s interest in CI is primarily for operation security, not as end in itself; to protect, but not interfere with CIA operations. Director of Central Intelligence (DCI) William Colby made that clear when he asserted that the CIA was in the business of foreign intelligence, not counterintelligence. This is a stark difference from the days of DCI Allen Dulles and DCI Richard Helms, who both believed that the Agency’s foreign intelligence could only be as good as its CI. Nor was counterintelligence the chosen career path for CIA’s best talent; career advancement came by recruiting foreign assets, not working in CI. Sometimes CI was merely a place the Agency put problematic employees, like Alrich Ames, for lack of a better use for them.

Although it may never hold the same importance as foreign intelligence collection, counterintelligence at CIA has improved in recent years. As during the Cold War, foreign intelligence personnel remain among the top of the list of CIA recruiting

---

97 Stephen Engelberg, “James Angleton, Counterintelligence Figure, Dies” New York Times, May 12, 1987
98 Godson, 112
100 Godson, 113
targets. Recruiting a bona fide member of a foreign intelligence service is one of the great counterintelligence coups and often yields highly valuable information about how a given service operates, what its targets are, what it knows, and what it does not know. The CIA also has the Counterintelligence Center Analysis Group that “identifies, monitors, and analyzes the efforts of foreign intelligence entities against US persons, activities, and interests.” This analytical body is an important departure from the cultural inclination at CIA to only regard counterintelligence as an operational role to protect collection.

Department of Defense: Counterintelligence activities in the DoD are carried out primarily by three bodies: Navy Criminal Investigative Service (NCIS); Air Force Office of Special Investigations (OSI); and Army Intelligence and Security Command (INSCOM). Each service has defined and practiced counterintelligence more or less on its own terms to suit individual service needs. NCIS and OSI are much more law enforcement based than INSCOM, for example. However, these services have not traditionally worked together in any meaningful way. Realizing this deficiency, and in response to Presidential Decision Directive 75, the Department of Defense created in

---

101 Michelle Van Cleave, Strategic Counterintelligence and National Security, 28
104 PDD 75 was signed by President Clinton on January 5, 2001 and was entitled “U.S. Counterintelligence Effectiveness – Counterintelligence for the 21st Century.” It was the document that created the NCIX and began a push for national-level CI system.
2002 the Counterintelligence Field Activity (CIFA) to act as a central manager of Defense counterintelligence.\textsuperscript{105}

CIFA was not an optimal architecture for managing DOD counterintelligence. In 2008, at the behest of DNI James Clapper, who was then Undersecretary of Defense for Intelligence, CIFA was subsumed by the Defense Intelligence Agency (DIA). Now the three services are under the authority of the newly-created Defense Counterintelligence and Human Intelligence Center. Combining HUMINT and counterintelligence enhanced the effectiveness of both. Now that DIA has authority over all three Defense CI services it is capable of carrying out “strategic offensive counterintelligence operations,” according to the Center’s director, Mike Pick.\textsuperscript{106} This is actually a credible claim. Drawing on the differing strengths of NCIS, OSI, and INSCOM, under the strong central management of DIA, and with U.S. military bases and liaisons all over the globe, Defense CI finally has the ability to execute integrated, strategic operations.

\textit{U.S. Counterintelligence as a community:} Interagency cooperation has come a long way, but it cannot yet be considered a unified, strategic enterprise. The FBI keeps over 50 liaison personnel at CIA headquarters in Langley, and also has personnel stationed permanently at NSA headquarters at Fort Meade.\textsuperscript{107} Within a historical context, this is a considerable improvement. There was a time when the FBI and CIA


\textsuperscript{107} Sean Joyce, Speech October 6, 2010
would hardly talk to each other, and each had equal disdain for the military services.\textsuperscript{108} There was a steady improvement throughout the Cold War, but after 9/11 the pressures and legal measures for cooperation increased dramatically.

The NCIX is supposed to be the CI community leader. Created in 2001, and subsequently folded into the ODNI, the ONCIX is tasked with 1) integrating the activities of all U.S. counterintelligence programs to make them coherent and efficient, 2) coordinating CI policy and budgets to the same end, and 3) evaluating the performance of the counter-intelligence community against the Strategy.\textsuperscript{109} However, the NCIX has no operational authority to implement strategies or to compel cooperation. The NCIX cannot command the FBI, CIA, or Defense agencies to change habits, alter behavior, adjust budget priorities, or carry out specific operations.

The individual agencies have very little motivation for change, especially if it means relinquishing turf, authority, or autonomy. Even though there is a push within the intelligence community leadership for more integrated and strategic CI capability, individual agencies believe that their own current capacity is satisfactory and not in need of adjustment. This is an understandable assessment, not merely because of the dynamics of bureaucratic infighting but because over the years all of these organizations have honed their CI practice to suit their individual needs. FBI, CIA, and Defense agencies believe that another level of bureaucracy will not improve their individual

\textsuperscript{108} James Olson, “The 10 Commandments of Counterintelligence” \textit{Studies in Intelligence} Fall/Winter 2001
\textsuperscript{109} U.S. NCIX Joel Brenner speech, March 29, 2007
abilities to conduct counterintelligence. Individually, FBI, CIA, and DoD counterintelligence capabilities are satisfactory when measured according to their own metrics, but as former NCIX Michelle Van Cleave would argue, “the whole [of U.S. counterintelligence] is less than the sum of its parts.” 110 In a way, Defense counterintelligence is ahead of the rest of the community. DoD has created what many would like to see the NCIX have – a vertical counterintelligence hierarchy that is institutionally joined with positive intelligence.

As it stands, U.S. counterintelligence infrastructure remains divided. American CI efforts are incongruent with the threats posed by Chinese intelligence while the current CI architecture makes facilitating a unified response difficult. The following section offers recommendations on how policy makers can improve CI efficacy without fundamentally changing that architecture.

**Policy Implications**

Chinese intelligence collection on the United States illuminates deficiencies in the current state of U.S. counterintelligence. Clearly, Chinese positive intelligence operations are too much for any one American entity to handle. The quantity of operations undertaken by actuarial, enterprise-directed, and entrepreneurial collectors are in themselves enough to overwhelm U.S. counterintelligence, thus leaving fewer resources to address the greater threat of professional Chinese intelligence operations. Despite the improvements in interagency cooperation in recent years there are still

---

110 Michelle Van Cleave, “Counterintelligence and National Strategy,” 24
geographic and bureaucratic seams in the U.S. counterintelligence system that are constantly being exploited by foreign adversaries.\textsuperscript{111}

The Chinese are clearly achieving some of their strategic goals. Stolen technology is feeding the Chinese economy and expediting the PLA’s military development – both at America’s expense in R&D investment. The military balance between the PRC and Taiwan is now deeply in the Mainland’s favor and with time China’s area-denial capabilities designed for the United States only improves. As late as 2003, scholars were still finding that Taiwan had a military advantage in fending off a Chinese attack.\textsuperscript{112} A RAND report published just six years later reassessed that balance as “substantially less optimistic for the Taiwan (and U.S.) side.”\textsuperscript{113} Anti-ship ballistic missiles, submarine prowess, and anti-satellite weapons already give the Chinese formidable capabilities to threaten the U.S. ability to intervene in Taiwan and in a crisis could threaten U.S. access to East Asia writ large.

Van Cleave would argue that the Chinese intelligence threat is strategic, while the U.S. response is piecemeal.\textsuperscript{114} Van Cleave goes on to point out the obvious fact that a foreign intelligence service does not merely target an FBI field office or a CIA

\textsuperscript{111} Godson, 111
station abroad but rather targets the United States itself. Without strategic guidance, the reactive and disparate response of U.S. counterintelligence agencies measure only tactical successes like catching the spy, finding the audio bug in the embassy wall, or discovering the true owners of a front company. \textsuperscript{115} These tactical successes might suffice if they prevented, dismantled, or manipulated a majority of Chinese collection efforts, but there is no evidence to suggest U.S. counterintelligence is more than marginally successful in this regard. \textsuperscript{116}

The most important factor in creating strategic counterintelligence is the policy maker. Policy makers have a crucial role in the collection of positive intelligence as they set collection requirements for the intelligence community; policy makers ask questions, and the intelligence community goes out to find the answers. However, no such relationship exists with CI. Policy makers should be an integral part in setting counterintelligence priorities. What successes U.S. counterintelligence does achieve would be better served if those successes were part of a national strategy in conjunction with American foreign policy or national security goals. Designating and prioritizing foreign and national security policy is beyond the mandate of FBI, CIA, or DoD. In fact, in order to preserve integrity and the ability to “speak truth to power,” U.S. intelligence entities have been purposefully precluded from making foreign policy.

\textsuperscript{115} Ibid, 16
\textsuperscript{116} This argument is based on the WMD Commission Report’s assessment. The Commission on the Intelligence Abilities of the United States Regarding Weapons of Mass Destruction, \textit{Report to the President of the United States} (Washington, March 31, 2005) 486
What secrets or technologies are most important to protect? What areas are less critical and thus require fewer counterintelligence resources? When and where should an adversary be denied and when and where should an adversary be deceived? Should a discovered Chinese penetration be arrested or should an information manipulation operation be conducted? These are all questions that should be answered by policy makers (e.g. the National Security Council staff) so that counterintelligence can be leveraged to further national interests. Otherwise, the individual CI agencies are left guessing about what is important and what is not.

Policy makers, to the benefit of U.S. counterintelligence, could prioritize among the many known Chinese intelligence activities. For example, the harassment of Chinese dissidents and activists residing in the United States by Chinese intelligence officers and consular officials may be egregious, but it is not necessarily an American national security concern. It is, however, a national security concern for the CCP to have Chinese democracy advocates undermining the Party’s rule, whether at home or abroad. As much as the United States might like to see a democratic government in Beijing, U.S. (short term) interests would not be served by inciting a CCP legitimacy crisis, especially if a legitimacy crisis leads to aggressive, militaristic behavior to shore up nationalistic support. For this reason, there may be justification for devoting less CI resources to this type of Chinese intelligence activity. Or, Chinese spying on political dissidents in America could be determined to be an unacceptable violation of U.S. sovereignty. America, as the world’s foremost promoter of democracy and freedom, might decide that it is imperative to protect the free speech of dissident Chinese
Diaspora. Again, this is not a decision that should be made by intelligence personnel, but by the policy maker.

As the Chinese are currently active in stealing sensitive technologies in a variety of sectors, the need for policy makers to set priorities is eminent. In a recent report, the ONCIX listed clean coal technology as vulnerable to Chinese theft. This is a key area of competition between the United States and China as both strive to develop the technology that will be adopted worldwide as the clean coal standard.\textsuperscript{117} An argument could be made that the United States and China have a shared interest in reducing the effects of climate change. In 2009, China accounted for over 46 percent of the world’s coal consumption.\textsuperscript{118} China’s dependence on coal for domestic energy production means that any marginal gains in coal efficiency would have profound reductions in greenhouse gas emissions. For these reasons, counterintelligence resources might be more advantageous if concentrated elsewhere. Then again, there is an economic argument to be made. The United States has invested a lot of money into the development of its clean coal technology, and if it were to be adopted worldwide there is opportunity for huge returns on that investment. Either way, this is a policy decision that should not be left for the intelligence community to make.

China is seemingly indiscriminate in the technologies it seeks to obtain. As the PRC uses professional, long-term operatives to obtain the most sensitive technology

secrets (e.g. nuclear warheads and quiet electric propulsion), there is a constant barrage of Chinese nationals seeking acquire anything they can get their hands on.

The FBI is not equipped to protect the entire nation from economic and industrial espionage on its own. As of March, 2010, there were 13,514 Special Agents in the FBI, only a fraction of those Special Agents are dedicated to conducting CI while the rest carry out the FBI’s other missions. If Chinese intelligence is believed to deploy hundreds of thousands of low-level collectors and operate over 3,000 front companies in the United States, how can the FBI be expected to keep tabs on all that activity when there are still Russian, Cuban, Iranian, and other hostile foreign intelligence services to worry about? For this reason, the FBI should focus on the most significant threats posed by professional foreign services. To mitigate the threat posed by less-skilled adversaries, the private sector must be equipped to better manage its own CI. Outreach programs like the FBI’s Business Alliance, Academic Alliance, and Infragard are a good start, but more could be done to educate the private sector on the specific foreign intelligence threats and ways of mitigating that risk.

The ongoing theft of U.S. military technology by the Chinese must be a top CI priority. However, the defensive posture of the United States in this CI arena is entirely inadequate. U.S. defense contractors have some of the highest security standards of the

---


120 Infragard is an FBI/private sector partnership whereby relevant intelligence is shared regarding counterintelligence, counterterrorism, and critical infrastructure protection. For more information see: http://www.infragard.net/
private sector, yet Chinese intelligence efforts still frequently succeed. Often by the time an espionage case is discovered, most of the damage has already been done. As the FBI investigates an espionage case, the damage continues until an arrest is made or other action is taken. This is an inadequate model when the stolen technology involves weapons that could be used against Americans (e.g. in a Taiwan Strait crisis).

It is with protecting military technology that interagency cooperation and policy guidance are most crucial. DoD should work closely with the civilian CI agencies in identifying the military technologies the United States is most concerned with the Chinese acquiring. Once the most lucrative targets are indentified, a purely defensive approach, no matter how stringent, will be insufficient. An offensive CI posture should be assumed.

U.S. counterintelligence has had success with offensive efforts in the past. In the 1980s the United States carried out an elaborate offensive CI operation against a KGB technology-theft network. The operation is now known as Farewell, named after the French source that initially alerted the United States to KGB technology collection targets, and involved the alteration of technological designs that were to be stolen by the KGB.121 These systems were engineered in way that would render them useless (or worse), and then made available to be clandestinely acquired by the Soviets. The most brilliant aspect of this operation is that even if the Soviets discovered the ruse, the CI success would be assured because the Soviets would then have to doubt the fidelity of

---

121 Michelle Van Cleave, “Counterintelligence and National Strategy,” 9
every technology stolen up to that point. Although this example may not be directly applicable to the PRC, it does show what can be accomplished with a unified CI effort across U.S. agencies directed towards a strategic goal.

It is unlikely that the basic architecture of American CI will change anytime soon. The interests of the FBI, CIA, and Defense to maintain their autonomy, authority, and CI “turf” will prevent the NCIX from asserting any kind of strategic control over U.S. counterintelligence. However, this does not necessarily mean that the United States cannot employ a strategic CI posture vis-à-vis the PRC. To be sure, changes need to be made to facilitate more cooperation but this must be a policy-driven effort. If policy makers tasked CI priorities and missions as they assign positive intelligence priorities, then CI could be aligned with foreign policy in a manner that is advantageous to American national interests. This can be done without fundamentally changing the current CI architecture – with proper policy guidance. The conflicting interests between the United States and the PRC are quite clear. U.S. counterintelligence posture should be adjusted accordingly.

\[122\] Ibid
Bibliography


Center for Strategic and International Studies, China: The Balance Sheet (New York: Public Affairs, 2006)


The Economist, "China’s Succession: The Next Emperor" October 21, 2010


Gaylord, James. Chi Mak affidavit, submitted by FBI Special Agent James Gaylord, October 28, 2005


Heidenrich, John G. “The Intelligence Community’s Neglect of Strategic Intelligence” *Studies in Intelligence* Vol. 51, No. 2


Joyce, Sean, Executive Assistant Director of FBI National Security Branch, speech at Bipartisan Policy Center, October 6, 2010


Mueller III, Robert. Testimony before U.S. Senate Judiciary Committee, December 6, 2006


Stokes, Mark A. “China’s Strategic Modernization: Implications for the United States,” *Strategic Studies Institute*, Sept. 1999


Tan Po. “Communist China’s Intelligence, External Affairs Research Organs.” *Cheng Ming* (Hong Kong), Sep 1, 1996.


“Fact Sheet: Major U.S. Export Enforcement Prosecutions in the Last Two years.” October 28, 2008

Federal Bureau of Investigation, Facts and Figures 2010-2011


“Strategic Counterintelligence: What Is It, and What Should We Do About It?” Studies in Intelligence Vol.51 No.2


Zheng Bijian, “China’s ‘Peaceful Rise’ to Great Power Status.” *Foreign Affairs*, vol.84 no.5 September/October 2005