U.S. Counterintelligence and the Problem Posed by Chinese Intelligence

Matthew Dorsett
Peace, War, and Defense and International Relations
University of North
Carolina
Chapel Hill, NC 27514
dorsettv@live.unc.edu

Abstract

Counterintelligence is a phrase used to describe actions taken, both defensive and offensive, to secure one's own agency, department or group. These actions vary, but examples include: prevention of infiltration by agents, the theft of state or trade secrets, and disruption of intelligence operations, identifying agents that have successfully infiltrated one's own organization and mitigating losses caused by these agents. However, these actions one would consider more defensive, where as offensive actions would be things like feeding false information on purpose, and placing one's own agents within the adversary's organization. The People's Republic of China poses perhaps the largest threat to U.S. security moving into the future. However, since the Communist Revolution in China, the U.S. and the P.R.C have been trying to get their spies into each other's governments. The U.S. has suffered several breaches by Chinese agents. This paper uses the story of one such breach, and uses it to highlight problems in the U.S. counterintelligence organizations, as well as what the U.S. counterintelligence should look at moving forward.

Keywords: Counterintelligence, U.S.-Chinese relations, Chinese Intelligence, U.S. Intelligence, FBI, Larry Wu-Tai Chin, Tiger Trap, Polygraphs, Counterespionage, Ministry of State Security

Introduction

Counterintelligence is perhaps one of the most important jobs that the United States intelligence community must tackle. Counterintelligence can be offensive, defensive and collection activities (Lowenthal, 2012). Examples of offensive counterintelligence include infiltration of an adversary's intelligence service in order to monitor and disrupt their operations (Lowenthal, 2012), whereas defensive counterintelligence are actions taken to try and prevent infiltration, as well as to catch any potential spies within one's own organization before damage can be done (Lowenthal, 2012), though as this paper will show, it seems that the moment people realize there is a mole is the moment they realize that there has been damage done, and thus the challenge is to prevent more damage. The United States employs several methods of internal safeguards to try and prevent infiltrations into its intelligence services. Most agencies will use a polygraph test during the application process (Lowenthal, 2012). A polygraph exam in an interview process, where the interviewee is being asked a series of questions, either about their lifestyle or previous jobs, while being monitored by a polygraph machine, which monitors heart rate, depth and frequency of breathing, as well as changes in skin temperature, and changes in these physiological events might indicate dishonesty or deception (Lowenthal, 2012). Another system used by the U.S. is the compartmentalization of its agencies, meaning no one person

(save for perhaps the top echelon) have access to all of the intelligence (Lowenthal, 2012). More offensive measures the U.S. can take include sending in agents into adversary's intelligence service. This can yield a lot of intelligence, including the adversary's HUMINT capabilities, the identity of clandestine service officers, possible penetration of one's own services, possible alliances the adversary has, and changes in the needs and wants of the adversary's organization (Lowenthal, 2012). It is difficult for the U.S, or any country's intelligence service for that matter, to be able to catch all spies and monitor all potential spies, as there are several reasons one would spy on one's own country, including, but certainly not limited to: financial issues or greed, ideology, vengeance against the country or officers above the spy, thrills, involvement with foreign nationals (this might be a romantic or sexual relationship or perhaps even friendship), drug addiction, which would be fed in order to get the potential spy to assist, and blackmail (Lowenthal, 2012). Certainly most if not all of these issues are being looked at by U.S. intelligence services when they are doing a background check of a potential employee. However, there have still be lapses in U.S. counterintelligence forces that have led to the infiltration of spies and the stealing of numerous classified documents, and perhaps the biggest threat to U.S. Intelligence agencies is China. The goal of this paper is to examine perhaps the worst case of infiltration into the U.S. Intelligence community by the Chinese intelligence service and the damage that was done by this infiltration. Then the goals of the Chinese intelligence services will be examined, as well as the tactics the Chinese intelligence community uses to recruit spies. The problems that the U.S. counterintelligence services are facing will then be confronted. Finally, this paper will attempt to provide some insight into how the U.S. might move forward with its counterintelligence services.

Larry Wu-Tai Chin and Tiger Trap

A prime example of the failure of U.S. counterintelligence and the success of Chinese intelligence operations is the EAGEL CLAW case, or the story of Larry Wu-Tai Chin. Chin was born in Beijing, China in 1922, and began work with the U.S. in 1944 as a translator for an Army liaison officer (Wise, 2011). This is when he was recruited by the Chinese to become a spy. When he was transferred to Korea during the Korean War, Chin acted as a translator for Chinese POWs, and Chin would turn over to the Chinese the names of Chinese POWs who agreed to return to China and spy for the U.S. (Wise, 2011). This act undoubtedly resulted in the death of many of these POWs when they were returned to China. In 1952, Chin began work for the CIA in the Foreign Broadcast Information Service (FBIS) in Okinawa, and in 1965 Chin received his U.S. citizen ship, passed a polygraph and background check, and was given a Top Secret clearance, meaning that Chin now has regular access to classified documents (Wise, 2011). Chin owned thirty-one properties in the Washington D.C. area, and two condominiums in Las Vegas, Nevada (Wise, 2011). When asked how he could afford all of this, Chin claimed to be an expert blackjack player who counted cards, when the truth was he was being paid by the Chinese to spy (Wise, 2011). The MSS serves as China's main intelligence agency, and was responsible for the handling of Chin (Wise, 2011). Chin would stuff documents into his clothing and briefcase, exit the building, take pictures of the documents, and hand the films over to Chinese intelligence service officers at a shopping mall in Toronto, Canada (Wise, 2011). At the age of fifty-nine, Chin actually retired from the CIA, received an award for his work as a translator and a week later he flew to Hong Kong and received forty thousand dollars from the Chinese for his work (Wise, 2011). Chin would not be found out until after his retirement.

Chin's downfall came when Yu Zhensan, a low level Chinese intelligence officer, wanted to leave the People's Republic of China due to longstanding family issues (Wise, 2011). Yu, whose codename was PLANESMAN, told the CIA, who later told the FBI, that there was possibly a mole within the U.S. Intelligence services (Wise, 2011). Tom Carson, a special agent of the FBI, was assigned to the task of finding this mole. Carson had several years of counterintelligence experience. It seemed that Carson's search would prove fruitless for a while, as Chin had done well to cover his tracks, and Chin had already retired. Carson received a break when Yu let him and the CIA know that the mole had taken a specific flight to and from Beijing. Carson examined the manifestos of these flights, and found only four U.S. citizens, and Chin was one of them, and the CIA would later realize that Chin had been their employee and had retired one year before Carson found Chin's name on that manifesto (Wise, 2011). Chin was immediately put under supervision, including an FBI wiretap (Wise, 2011). Carson managed to go through Chin's luggage at an airport en route to Hong Kong, and in this search, Carson found a hotel key, which they were able to use. Yu told the FBI that the mole had stayed at that particular hotel in that particular room (Wise, 2011). Yu did not have direct access to Chin's files, but dug around his colleague's files. It was in November of 1985 that the FBI confronted Chin in his apartment (Wise, 2011). Chin denied the allegation of espionage, but was unable to deny the proof that he was presented to him. Chin was convinced that Ou Qiming, his former handler at the MSS, had defected to the United States and as part of his defection had turned Chin over, and under the assumption that he had been turned over to the FBI, Chin confessed his entire story (Wise, 2011). Chin was tried and found guilty of espionage, and was sentenced to two life sentences, but committed suicide shortly after the trial. Larry Wu-Tai Chin's story is a long one that lasted over three decades of espionage, and had serious ramifications.

The infiltration of the CIA by Chin for over thirty years inflicted a lot of damage to U.S. intelligence efforts extended over several years. First and foremost, this case shows a true failure of U.S. counterintelligence efforts. Chin was able to walk out of offices with briefcases full of sensitive documents, including documents pertaining to Nixon's plans to try and normalize relationships with China (Wise, 2011). The MSS, with Chin's documents, would be able to know just how accurate U.S. intelligence was concerning China, as well as compromise a number of U.S. intelligence and counterintelligence operations (Eftimiades, 1994). Aside from compromising U.S. operations, the Chinese would have access to information that might inform them which members of the U.S. intelligence communities would be most likely to turn on the U.S. (Eftimiades, 1994). The MSS, through Chin's espionage, would be able to know information about U.S. diplomatic, political and economic policies towards China, knowledge concerning U.S. intelligence services knew and did not know when it came to China and Chinese intelligence operations, as well as details about secure communication capabilities (Eftimiades, 1994). The Chin case also highlights a problem with U.S. offensive counterintelligence operations, in that the U.S. did not have someone in the Chinese intelligence community or did not have someone who could penetrate the Chinese intelligence service deep enough to be able to find out about Chin's espionage activities (Eftimiades, 1994), a sign of either the strength of Chinese intelligence services counterespionage or a sign of the weakness of U.S. offensive counterintelligence. This particular case, however, is just a single example of U.S. counterintelligence problems, and one must realize that it is not the norm. However, this case, as well as others helps highlight what problems there are.

Problems Facing U.S. Counterintelligence

Over time, there have been failures of U.S. counterintelligence services, including Chin, Aldrich Ames, Robert Hansen and Anna Montes. These many infiltrations into U.S. intelligence services show U.S. counterintelligence to be reactive, as opposed to proactive. There are many reasons why U.S. counterintelligence services are lacking. Some authors cite U.S. arrogance and naiveté towards counterintelligence (Sims, 2009), meaning that the U.S. does not give counterintelligence the attention needed for it to be as effective as it could be. Another possible fault in U.S. counterintelligence is that the U.S. often fails to punish harshly spies caught unless there is a lot of proof that the accused spy is guilty (Sims, 2009), which may say more about the U.S. legal system than counterintelligence services. It also appears that the U.S. has trouble keeping aggressive counterintelligence strategies during times of strategic détente or heightened tension with a hard target, such as Iran, China, Russia, and even Al-Qaeda (Sims, 2009). The U.S. intelligence services also seem to be over reliant on the polygraph, however it is far from perfect technology. Chin, for example, passed his polygraph, and there is a debate in the science community on whether or not the polygraph is effective. Polygraphs do measure things like heart rate, breathing rate and skin temperature, which does help to curb casual discretion, however there is no universal psychophysiological response to lying (Polygraph, 2000), and so the test is not always reliable. In order to better its counterintelligence strategy against China, the U.S. must look towards the goals and objectives of the Chinese intelligence services and the methods used by the Chinese to recruit their spies.

China's Intelligence: Methods and Concerns

Firstly, China's intelligence goals should be considered in U.S. counterintelligence strategy. China's intelligence goals are broad and varied, much like the United States' goals. However, most of China's goals can be divided into soft and hard targets. The hard targets are the ones that China sees as presenting perhaps the most imminent threat to their security. These hard targets include the Commonwealth of Independent States (CIS), which consist of the former soviet republics, and goes back to China's longstanding ties and troubles with Russia. India also serves as a hard target for China (Eftimiades, 1994). Like Russia and the CIS, China has had confrontation with India, another regional superpower, and the two states share a distrust of one another over the 1962 border war and the Chinese subjugation of Tibet. The Chinese must also be concerned about Vietnam and the Vietnamese border, as well as the Muslim states north of Xingjiang (Eftimiades, 1994). The Xingjiang province has as substantial Muslim population, and Fundamental Islamist and extremists pose a threat to China and Chinese control in the province (Eftimiades, 1994). There are several soft targets as well, including the United States, Japan, South Korea, and Taiwanese movements in the Sea of Japan (Eftimiades, 1994). China's major other intelligence goals are the acquisition of foreign high technology, for both civilian and military uses (Eftimiades, 1994). Knowing the goals of the Chinese intelligence services is not enough, however, as the Chinese employ a number of different tactics to recruit spies and acquire technology.

The MSS and other Chinese intelligence services use numerous methods to recruits agents to spy on the U.S. and other targets. The MSS prefers to recruit people in Chinese territories (Eftimiades, 1994). They do this for a number of reasons, perhaps most likely because they can use the fact that the potential recruited person is on Chinese soil and subject to Chinese

law. Recruiting form those in or visiting China might be safer than trying to recruit abroad, and China saves money on having to keep service officers abroad (Eftimiades, 1994). The Chinese target a wide variety of potential agents, such as diplomats, government officials, academics, journalists and businesspersons (Eftimiades, 1994). Some of these targets cater more to the traditional intelligence targets of China, where others are target for their access to foreign technology. The MSS will use various means to try and recruit diplomats and government officials, such as blackmail and entrapment (Eftimiades, 1994). The MSS will send women to try and seduce male diplomats and government officials, and then use this relationship to leverage the person into spying on the U.S., either by having the seducer try and get the information from the target or blackmailing the target into spying. When the MSS wants to force a journalist to work for them, they will send the journalist an anonymous call or email stating that the person had valuable intelligence for the journalist. The journalist would then go to meet this informant and would get arrested by the Chinese authorities and given the option to either spy for the MSS or face prison time (Eftimiades, 1994). The Chinese also prefer to recruit ethnic Chinese people (Eftimiades, 1994), playing on the sentiment of helping China become the country they would want it to be, as well as leveraging any family members that still live in China against the potential spy. The Chinese will recruit either visiting Chinese people, or Chinese citizens traveling abroad.

The Chinese intelligence services utilize other methods when it comes to obtaining foreign high technology. Chinese intelligence services often invite foreign scholars to lecture in China as guests (Eftimiades, 1994). Usually the whole trip is paid for by the Chinese intelligence services, including room and board for the scholar and even their families. The scholars are then given rigorous itineraries meant to wear the person down physically and mentally, and then the scholars or businesspersons are brought to a cocktail party or some other such occasion and they are encouraged to consume copious amounts of alcohol (Eftimiades, 1994). This combination of alcohol and fatigue typically makes the people more pliable and more likely to talk with the agents and students the Chinese have placed in the party to ask questions. Sometimes, the Chinese will attempt to buy the technology, either by using co-opted people recruited in China to buy the technology and bring it back, having Chinese owned firms buying up companies that have the technology, or by having fronts in Hong Kong to buy it and bring it back to Beijing (Eftimiades, 1994). Alternatively, Chinese intelligence services will send over scientists as part of an exchange program in order to have these scientists act as moles, reporting on the projects they are cooperating on with foreign scientists (Eftimiades, 1994).

Conclusion

China presents a very serious and very complicated problem to U.S. Counterintelligence services. The Chinese employ a number of tactics when it comes to acquiring technology and recruiting spies. Moving forward, the U.S. must overcome two major challenges: one, U.S. counterintelligence forces must rid itself of notions of invincibility (Sims, 2009), meaning that the U.S. intelligence services must become less reliant on polygraphs and begin to develop new means of interviewing potential employees. Secondly the U.S. must attend to the new challenges of counterespionage faced with the rise of terrorism and technology-enabled espionage while not failing to respect the laws by which the organization are run by and the rights of the citizens these organizations seek to protect (Sims, 2009). In addition, the U.S. must adopt an aggressive and offensive counterintelligence strategy while continuing to bulk up its defensive

counterintelligence actions. The U.S. could strengthen its offensive counterintelligence capabilities by focusing on the regions that are critical to China, such as Vietnam and India. The U.S. can work to help strengthen these two regions, either through clandestine or covert operations, and force China to allocate more resources to areas that are already hard targets. Offensive Counterintelligence is about disrupting the adversary's intelligence service, and making it difficult for it to operate. China poses a unique and difficult challenge for the U.S. however, it is not impossible for the U.S. to meet this challenge with a combination of aggressive offensive counterintelligence and modernized and thorough defensive counterintelligence.

Refrences

Eftimiades, Nicholas. *Chinese Intelligence Operations.* (Naval Institute Press, 1994) 32-33

Lowenthal, Mark M.. *Intelligence: From Secrets to Policy* 5th edition. (CQ Press, 2012) 163

Sims, Jennifer E., Burton Gerber, eds. *Vaults Mirrors & Masks: Rediscovering U.S. Counterintelligence.* (Georgetown University Press, 2009)

Polygraph Testing and the DOE National Laboratories." *Science,* New Series, Vol. 290, No. 5493 (Nov. 3, 2000), pp 393-400

Wise, David. *Tiger Trap: America's Secret Spy War with China.* (Houghton Mifflin Harcourt, 2011) 202