(U) Foreign Espionage

(U) The "Classical" Method of Targeting the United States

(U) *Russian Federation*

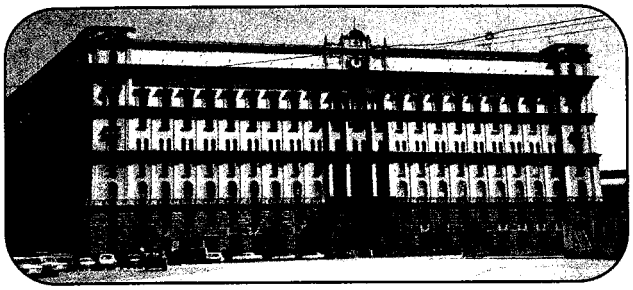
[redacted]

(U) The Russian Federation has a significant intelligence capability inherited from the former Soviet Union. Much of this intelligence collection infrastructure continues to focus on collecting information concerning the United States. Russian intelligence operations against the United States have increased in sophistication, scope, and number; and they are likely to remain at a high level for the foreseeable future.[11]

(U) Russia has two main active intelligence services: the Russian Foreign Intelligence Service (SVR) and the Main Intelligence Directorate of the General Staff (GRU). Intelligence activities are overseen by the Russian National Security Council and coordinated through the Permanent Interbranch Commissions of the National Security.[12]

(U) In addition to the three foreign intelligence agencies, the Russian intelligence community also controls the Federal Customs Service and the newly organized Federal Security Service. The Federal Customs Service can provide the intelligence services with detailed information on the movement of goods and equipment in and out of Russia. Proprietary information, such as customer lists, is available in decla-

rations made to the Federal Customs Service. After the dissolution of the Soviet Union, the KGB was broken up into eight different agencies—most are responsible for internal security matters. The Federal Security Service incorporates the functions of the Main Administration for the Protection of the Russian Federation and the Federal Counterintelligence Service. The combination of these functions has returned much of the internal security and counterintelligence functions, formerly held by the KGB, to a single agency.[13]



(U) The "classic" HUMINT collection process used by the former Soviet Union, its allies, and many intelligence services of the West shares a number of general features.

(U) First, the main consumers of intelligence are factories, research institutes, and government agencies. Second, their critical information needs are addressed through a centralized intelligence requirements list maintained collectively by the intelligence services. Third, when specialized intelligence is needed, a requirement is levied on the intelligence services, which sometimes collect the desired information through covert operations. Because the "consumers" of intelligence do not know the source of the information they ultimately receive, one strength of this approach to intelligence collection is that it is relatively secure. Another is that the hands-on operational activity is accomplished by professional intelligence officers extensively trained for such work. One weakness of the classical approach is that, because it is difficult to deploy and maintain extremely large numbers of intelligence officers abroad, the collection process has a limited capacity. Another weakness is that the professional intelligence officers involved in the process may not always know enough technical detail about Russia's critical information needs to target the best information.

The Ames Case

(U) One of the most serious examples of a HUMINT operation conducted by Russia is the case of Aldrich Ames, a Central Intelligence Agency (CIA) employee working in the Directorate of Operations. In April 1985, Ames had official- business contacts with diplomats at the Soviet Embassy in Washington, DC and seized this opportunity to volunteer his services to the KGB. He provided extensive information on CIA operations targeting the former Soviet Union and, later, Russia. Ames compromised, by his own admission, "virtually all Soviet agents of the CIA and other American and foreign services known to me." In addition, he provided the former Soviet Union and Russia with a huge quantity of information on U.S. foreign, defense, and security policies. He continued to work for the SVR after the breakup of the Soviet Union, until his arrest in February 1994. Ames was paid at least $2.5 million for his services.[238]

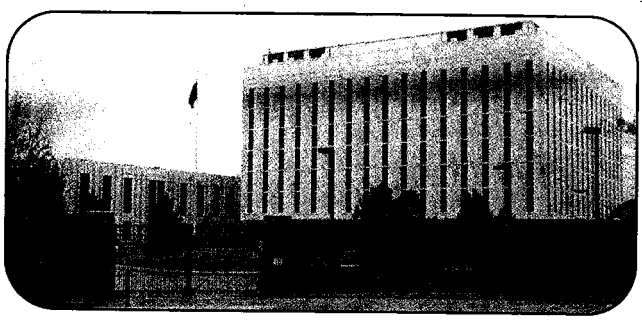
(U) The Soviet or Soviet-trained approach to intelligence collection poses two main problems for OPSEC managers: determining the activities of the adversary's intelligence officers, and monitoring the activities of employees to see if they are in contact with the intelligence officers. Further, because of the professionalism of the intelligence officers, it may be extremely difficult for U.S. counterintelligence authorities to identify them. Even if intelligence officers are successfully identified, it may be problematic to determine if their activities are intelligence-related or whether they have had contact with an employee.

(U) Russian Intelligence Organizations

(U) *SVR, the Russian Foreign Intelligence Service*

(U) The SVR, the successor to the First Chief Directorate of the KGB, is responsible for collecting foreign intelligence. It was created when the KGB was dismantled in the aftermath of the August 1991 coup against the Gorbachev government. The Chairman of the KGB, Vladimir Kryuchkov, and other senior officials were involved in the plot to overthrow Gorbachev. As a result of this attempted coup, the KGB was broken up. The internal security, counterintelligence, border guard, and protection service missions formerly assigned to the KGB were given to newly created organizations. The SVR concentrates on collecting political, economic, scientific, and technical information, as well as conducting covert action operations.[14] The majority of SVR case officers operate under diplomatic cover from Russian embassies and consulates.

(U) Although the number of SVR personnel has reportedly been reduced by 30 percent, the agency continues active collection operations. For example, after an operational hiatus following the collapse of the Soviet Union, the agency continued to operate FBI Special Agent Robert P. Hanssen as a penetration of the U.S. Intelligence Community. Further, Russian President Vladimir Putin, who served for 16 years as a KGB foreign intelligence officer, has placed other former intelligence officers in key government posts and has carried out a vigorous domestic campaign to laud the exploits of Russia's intelligence services, both during the Soviet era and afterwards. The SVR may also continue to be involved in conducting propaganda and influencing operations abroad.[15]



(U) *GRU, the Main Intelligence Directorate of the General Staff*

(U) The GRU and the Ministry of Defense supported Gorbachev against the August 1991 coup and, unlike the KGB, the GRU survived the aftermath of the coup largely intact. The GRU is responsible for providing strategic, operational, and tactical intelligence to the Russian armed forces. Principal missions include the collection of indica-

(U) An instructive example of the changing environment now faced by OPSEC and its need to field a diverse defense is evidenced in the series of events that led to the discovery of a microphone planted in a conference room of the State Department.

The Gusev Incident

(U) In December 1999, Stanislav Borisovich Gusev, a Russian diplomat, was apprehended by U.S. agents as he positioned a Russian embassy car in a parking space to monitor a listening device that had been planted on the building's seventh floor, which houses State Department's executive suite. According to reports, Gusev first came to the notice of U.S. counterintelligence and security officials months earlier, when an FBI surveillance team involved in another case noticed him repeatedly parking and re-parking his vehicle in different locations close to State Department's main building.[236] Since the car bore the distinctive tags issued to foreign legations by State Department's Office of Foreign Missions, the FBI personnel knew at a glance that its occupant, who would usually leave his vehicle and sit quietly on a nearby park bench for hours, was a diplomat from the Russian Embassy.

(U) Subsequent observation of Gusev's suspicious routine raised the possibility that his vehicle, which he kept within sight of the park bench, might contain audio monitoring equipment. A systematic search of the building with sophisticated counter-audio equipment was undertaken, and this eventually located a battery-powered transmitter concealed within a section of chair rail in an executive-level conference room. The room was on the same corridor as the Secretary of State's conference area and was usually left unlocked.

(U) Investigation determined that access to the conference room might have been available to Russian diplomats, since closer diplomatic relations with Russia had, some time earlier, led the State Department to issue Russian diplomats "no escort required" badges to wear during visits to the building. Stanislav Borisovich Gusev was quickly expelled from the U.S. for his espionage activities.[237]

(U//FOUO) It is worth noting that this audacious intelligence attack was made possible by the combination of technology—battery and radio design advances allowed for the construction of a very small, very powerful device—and geopolitical changes caused State Department policymakers to make a gesture of trust to Russian diplomats by granting them unescorted access. Nonetheless, it was still necessary for an intelligence officer to get physically close to the building to turn the implanted microphone on and record its transmissions.

(U//FOUO) On the other hand, discovery of the attack was also made possible by a combination of factors. For one thing, State Department is obviously a high-profile terrorism target, and frequent parking and re-parking of a vehicle on its perimeter was bound to draw the attention of security personnel. In addition, the distinctive diplomatic tags of the car immediately identified it as of potential counterintelligence interest. The tags were a requirement of the Office of Foreign Missions, created in the early 1980s to impose on foreign officials the same sort of treatment, including distinctive vehicle tags, that U.S. officials encountered overseas. Further, the FBI surveillance officers were at the site to investigate another matter and noticed the suspicious activity by chance. Although no single element of State Department's defenses was specifically designed to stop Gusev's intelligence activities, the combination of defenses there for other purposes served to identify him and place him under scrutiny, leading to the neutralization of the penetration.

tions and warning intelligence, data on advanced military technologies, and specific information on the intentions and military capabilities of potential adversaries. Collection techniques include gathering open-source information, acquiring overt and clandestine HUMINT, conducting satellite and aircraft imagery reconnaissance, and collecting signals intelligence from various platforms (ships, aircraft, satellites and ground stations).[16] The GRU also is interested in exploiting opportunities to penetrate U.S. intelligence; and at one point early in his lengthy espionage career, renegade FBI Special Agent Robert P. Hanssen worked as an agent of the GRU, in the process providing his Soviet military handlers the identity of one of the most valuable U.S. agents, who eventually was arrested and executed.

(U) Specialized GRU technical collection activities that directly threaten U.S. interests are those under the First Deputy Chief and the Space Intelligence Directorate. The Space Intelligence Directorate, in coordination with the Fleet Intelligence Direction of the Fifth Directorate, manages the Russian space reconnaissance program. The Fleet Intelligence Direction is responsible for space systems that provide intelligence supporting naval forces. The Space Intelligence Directorate is responsible for the development, manufacture, launch, and operation of Russian space-based reconnaissance systems. It operates its own cosmodromes, several research institutes, supporting mission ground centers, and a centralized computer processing facility.[17] The GRU's Sixth Directorate uses more than 20 different types of aircraft, a fleet of 60 collection vessels, satellites, and ground stations to collect signals intelligence.[18]

(U) GRU analytical activities are organized into geographical sections and a limited number of functional activities that cut across geographic areas. An example of functional orientation is the Ninth Directorate, which acquires and assesses scientific and technical data for the military design bureaus.[19] Of particular interest to the OPSEC manager is the Institute of Information, which operates separately from the directorates. It is responsible for developing intelligence products based on the fusion of open-source materials and classified information.[20]

(U) *FSB, The Federal Security Service*

(U) The FSB is one of the successors of the KGB, and remains headquartered in several buildings in Moscow's Lubyanka Square and staffed by approximately 75,000 employees. Its responsibilities are similar to those of the FBI in the United States and include counterintelligence operations, investigation of organized crime, and counterterrorism. The FSB also works outside Russia in certain target areas in cooperation with other Russian intelligence services. The Federal Security Service has arrested some people on false pretexts for expressing views critical of the Government, and, in particular, for voicing criticism of the security services. The FSB has also targeted national security and environmental researchers. On some occasions, Russian citizens interested in military issues or military-industrial polluters have become a target of the FSB.

(U) Lt Colonel Alexander Litvinenko, a former FSB officer granted political asylum in Britain, has described one recent Russian intelligence-service tactic:

> (U) *"Once the FSB or SVR officer targets a Russian émigré for recruitment, they approach them, usually at their place of residence, and make an effort to reach an understanding. If he or she*

The Expulsion of Colonel Ismaylov

(U In May 1985, an assistant air attaché at the Soviet Embassy in Washington, D.C., approached a high-ranking U.S. Air Force officer to spy for the Soviet Union. The Soviet representative, Colonel Vladimir Makarovich Ismaylov, was, in actuality, a GRU officer and, as such, part of a military intelligence collection effort so aggressive that its officers sometimes knocked on the doors of U.S. military personnel in the dead of night to request classified documents. Ismaylov pressed the Air Force officer for classified documents on the Strategic Defense Initiative, the Cruise Missile, stealth technology, and other sensitive subjects. The inducement for the officer to commit espionage was the most common one: money.

(U) As required by regulations, the U.S. officer reported the contact with Ismaylov, and Air Force and FBI counterintelligence investigators thereupon initiated a double-agent operation, using the situation to study the techniques the GRU would employ to target U.S. critical information.

(U) After a number of increasingly clandestine meetings with the officer, the GRU accepted him as a recruited, clandestine agent and decided to use impersonal agent communication techniques to handle messages to and from him in the future. Ismaylov explained that he wanted the officer to put the secret documents into a plastic trash bag and bury the bag at an agreed-upon "drop" site, where Ismaylov could retrieve it at his convenience. The GRU intelligence operative later provided the Air Force officer a schedule on which to make his drops. He was to signal it had been done by leaving an orange soda can near a certain stop sign as a "flag" for the Soviet. Ismaylov also provided a spy camera to make copies of documents that were too dangerous for the officer to smuggle out of his office.

(U) In mid-1986, counterintelligence officials decided to bring the case to a close in a way which would support the U.S. policy of drawing down the large personnel infrastructure the Soviets had established in the U.S. to facilitate clandestine operations. If FBI agents could catch him red-handed in an act of espionage, Ismaylov would be sent home, and the diplomatic slot he occupied also would be abolished. Late one evening in June of 1986, Colonel Ismaylov was detained by FBI agents as he dug up a bag of classified documents left for him by the double agent. He was declared persona non grata and compelled to return to the Soviet Union.[239]

refuses, the intelligence officer then threatens the would-be recruit with legal prosecution in Russia; and if the person continues to refuse, the charges are fabricated."

(U) According to Litvinenko, extradition proceedings are then immediately launched. Litvinenko was himself convicted in absentia by a Moscow court in June 2002.[21]

(U) *Former FAPSI, the Federal Agency for Government Communications and Information*

(U) The FAPSI, created in October 1991, was abolished in March 2003 by President Putin who divided its functions between the FSB and the Ministry of Defense. Elements of what was FAPSI are responsible for both communications security for the Russian Federation and SIGINT operations against targeted foreign activities. It is also responsible for the development and maintenance of databases and communications systems to support Russian intelligence and law enforcement activities. FAPSI is chartered to lease government communications lines to private investors, to set up communications activities in the territory of other sovereign states, and to conduct foreign business activities. The access provided through such activities allows FAPSI to monitor communications systems and permits the purchase of advanced telecommunications technologies from foreign companies. The former Soviet Union and now, Russia, have been denied the opportunity to purchase advanced communications and information systems from the West. The Russians hope that the entrance of FAPSI into the commercial telecommunications market will end this isolation.[22]

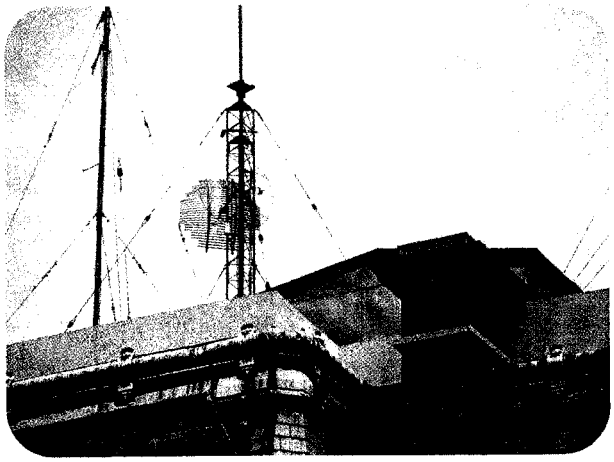
(U) Even after the failure of August 1991 attempted coup, the number of HUMINT operations conducted by the SVR and KGB targeting the United States and the West continues to rise. This is due to a number of factors. First, as a result of arms control treaties, joint business opportunities, and cultural and economic exchanges, the Russian intelligence services have greater access to Western society, government, and industries. In addition, there has been a significant influx of Russian émigrés into the United States. The FBI estimates that more than 105,000 Russians immigrated to the United States in the late 1980s. The Russians, like many intelligence services, have traditionally used émigrés to gather intelligence. In fact, there has been a substantial influx of Russian students into the United States, and many of them are studying technical disciplines to improve Russian military and civil industries. Finally, travel restrictions on Russian diplomatic and consular personnel in the United States have been lifted, making it easier for them to collect information on U.S. activities.

The number of HUMINT operations conducted by the SVR and KGB targeting the United States and the West continues to rise.

(U) Signals Intelligence

(U//FOUO) The GRU, elements of the former FAPSI, and the Cuban intelligence service jointly operate a SIGINT facility at Lourdes, Cuba, which is one of the most signif-

icant intelligence collection activities targeting the United States. This facility, less than 100 miles from Key West, Florida, is one of the largest and most sophisticated SIGINT collection facilities in the world. The Lourdes complex is manned by over 1,000 Russian personnel and is capable of monitoring a wide array of commercial and government communications throughout the southeastern United States and between the United States and Europe. Lourdes intercepts transmissions from microwave towers in the United States, communication satellite downlinks, and a wide range of shortwave and high-frequency radio transmissions. It also serves as a mission ground station and analytical facility supporting Russian SIGINT satellites. The facility at Lourdes, and a sister facility located in Russia, monitor all U.S. military and civilian geosynchronous communications satellites. It is believed that the Lourdes facility monitors all White House communication activities; launch control communications and telemetry from the National Aeronautics and Space Administration (NASA) and Air Force facilities at Cape Canaveral; as well as financial and commodity wire services and military communications links.[23] According to one source, Lourdes has a special collection and analysis facility responsible for targeting financial and political information. Specially selected personnel man this complex, and it appears to be highly successful in providing Russian leaders with political and economic intelligence.[24]

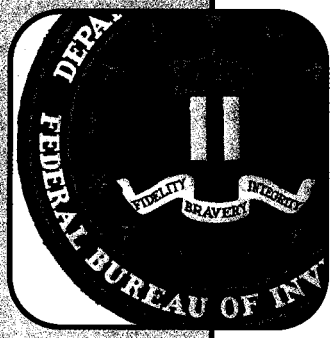


(U) The former Soviet Union also used a variety of other means to collect signals intelligence, and it is believed that Russia continues these activities in the United States. The locations of a number of Russian diplomatic facilities in the United States facilitate SIGINT access to sensitive information. Russian collection activities could derive sensitive government policy information by monitoring activities in the Washington, D.C. area, and sensitive financial and trade information by using Russian facilities located in New York, San Francisco, and Seattle. The fact that microwave towers and cellular communication repeaters are located near Russian diplomatic facilities in these cities increases the risk of collection activities.[25]

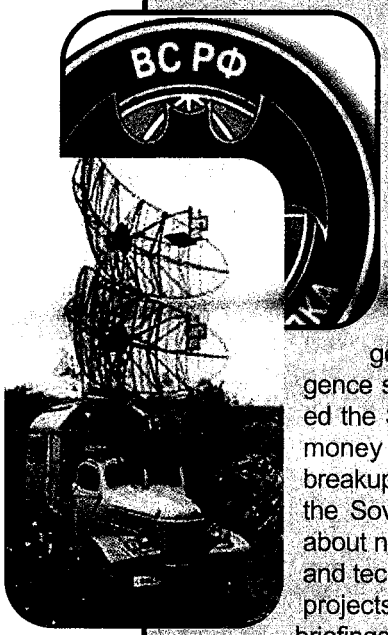
(U) There is little doubt of past SIGINT collection of this sort. For example, vans from the former Soviet Mission to the United Nations (UN) were observed in the vicinity of the General Electric Americom satellite ground station in Vernon Valley, New Jersey. In addition, Soviet San Francisco consulate vans made unexplained trips to the vicinity of AT&T microwave towers in northern California. In both cases, the vans appeared to be conducting SIGINT monitoring of these facilities.[26]

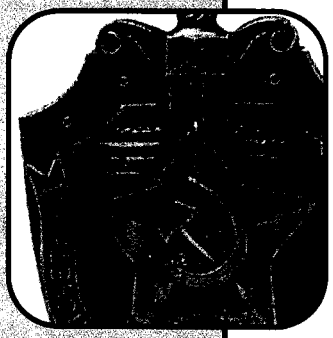
The Robert Hanssen Case

(U) In February 2001, FBI Special Agent Robert P. Hanssen was arrested by the FBI after filling an intelligence drop site with classified documents intended for the SVR. As details of the case became known, both the public and government officials were shocked by the extent of damage to the national security caused by this apparently exemplary man with a large family and devout religious beliefs. In the late 1970s, Hanssen, beset with credit card debt from his young and growing family, living in an expensive suburb of New York City, and innately curious about what it would be like to be a spy, used his position on an FBI counterintelligence squad to develop a way to safely contact Soviet military intelligence, the GRU. Hanssen passed information to a local GRU officer several times, including the identity of a Soviet Army general cooperating with the West, in return for a total of about $30,000. After his wife became suspicious of his activities, Hanssen broke off contact with the Soviets. Paying something each month, he began to donate most of the money he had received from the GRU to charity. The Soviet general Hanssen had compromised eventually was arrested and executed.



(U) In late 1985, Robert Hanssen was on the verge of leaving a job at FBI Headquarters in which he supervised a group of analysts studying Soviet intelligence techniques. In that position he had also acquired a reputation as someone who could understand and succinctly explain the technical aspects of intelligence projects undertaken by agencies such as NSA and CIA, and so he frequently was called upon to be the FBI's representative at interagency meetings and briefings about sensitive projects. Again Hanssen was deeply in debt, this time because of continuing family expenses and a high-rate mortgage with an impending balloon payment, and again he was fascinated at the prospect of personally succeeding as a spy. Using his expert insider knowledge of both Soviet intelligence practices and the FBI's counterintelligence strategies, Robert Hanssen again contacted the Soviets, this time the KGB, and asked for money in exchange for information. Until the breakup of the Soviet Union, Hanssen provided the Soviets with a steady stream of information about not only U.S. counterintelligence operations and techniques but also the intelligence-gathering projects of other intelligence agencies, whose briefings he had attended on behalf of the FBI. He even compromised part of the plan the United States had developed to safeguard the President and other senior government officials in the event of a surprise attack by another country. After the fall of communism,

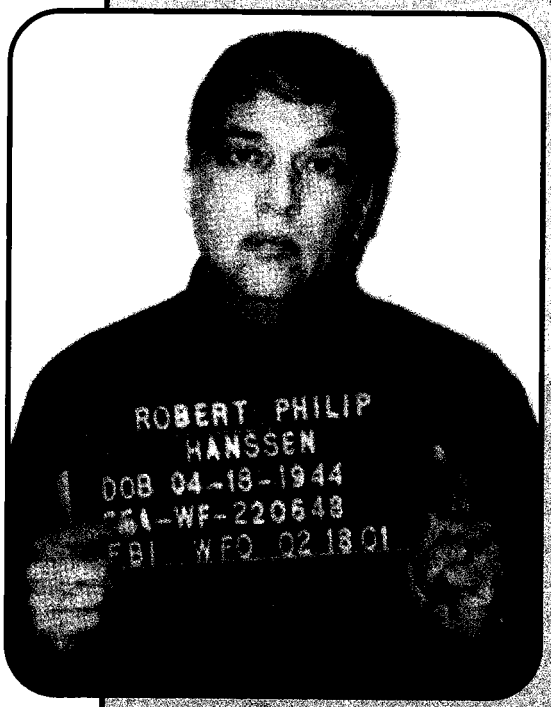




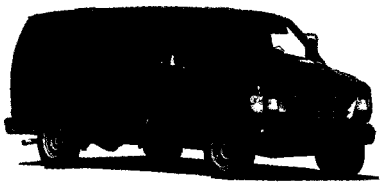
Hanssen broke off communications with the KGB, for security reasons. In 1999, however, Hanssen contacted the SVR, one of the Russian successor agencies to the KGB, and resumed passing intelligence, this time because of college expenses for his children and the desire to remodel his kitchen.

(U) In late 2000, U.S. counterintelligence, which had sustained losses that could only be explained by a traitor from high up within its own ranks, succeeded in obtaining from a source deep inside Russian intelligence the file the KGB had kept on Hanssen. Although the KGB apparently did not know his identity, there was sufficient detail in the file materials to lead investigators to Hanssen.

(U) In exchange for his cooperation in damage assessments and ongoing debriefings, Hanssen was spared the death penalty and his wife allowed to collect the survivor's benefit on his government pension, which normally would be forfeit because of his espionage crimes. Although he has apologized publicly for his crimes, Robert Hanssen's betrayal compromised a wide array of U.S. intelligence capabilities and directly led to the arrest and execution of a number of agents the United States was operating inside the Soviet Union. In May 2002, Hanssen was sentenced to life in prison without chance of parole.



(U) From an OPSEC perspective, the Hanssen case is one of the best examples of the damage that a trusted insider can do, once he has decided to betray his employer. Because no organization can defend itself against all possible threats and still continue to function, it was no problem for Hanssen to defeat the FBI's defenses against the Soviets, for the simple reason that he was one of the individuals entrusted with designing and studying those very defenses. In addition to that specialized counterintelligence information, Robert Hanssen also had access to foreign intelligence information about technical collection programs, U.S. intelligence policies, etc. So, Hanssen not only had the means to defeat the FBI's defenses but also access to information of extreme intelligence value. While Robert Hanssen went to great pains to try to conceal his identity from his intelligence handlers, over time he left behind a series of clues sufficient to identify him as a spy. When he was finally identified, it was because of information provided by another trusted insider, one on the other side.



(U//FOUO) The Russians have probably continued the Soviet practice of using covert mobile collection platforms not assigned to their diplomatic facilities. During the Cold War, for example, the Russians frequently used tractor-trailers and other vehicles with concealed SIGINT collection equipment to gather intelligence in Western Europe. The Soviets allegedly used clandestine collection vans located in Mexico to monitor activities at White Sands Missile Range in New Mexico and Vandenberg Air Force Base in California. Vans operating from Tijuana, Mexico, were reportedly able to monitor all of southern California and western Arizona. There have also been reports that Russian Aeroflot aircraft and clandestine collection vehicles collected SIGINT data inside the continental United States.[27]

(U//FOUO) The Russians continue to use satellites for collecting SIGINT. The first Soviet SIGINT satellite was the Cosmos 189 ELINT satellite, launched in 1967. Over the next 24 years, the Soviets placed over 200 SIGINT satellites into orbit, and the Russians continue to maintain a robust presence in space. During 1994, the Russians conducted 48 spacecraft launches. Fifty percent were military missions, including advanced imagery systems, ocean reconnaissance, and electronic intelligence collection. In 1995, the Russians space program included another 48 space launches; again, approximately half were military missions.[28]

(U) Open-Source Intelligence

(U) The Russian Institute of Automated Systems at Moscow State University hosts the National Center for Automated Data Exchanges (NCADE) with foreign computer networks and data banks. NCADE was subordinate to the KGB and is now believed to play a central role in SVR's computer intelligence collection activities. NCADE has direct access to data networks in the United States, Canada, France, Germany, and the United Kingdom, and it is a client of several online databases. These databases include the U.S. Library of Congress, the LEXIS/NEXIS data service, the United States National Technical Information Service, the British Library, and the International Atomic Energy Agency. The Russians have also established accounts with multiple Internet service providers, such as America Online, COMPUSERVE, TYMNET, and the European Union's EuNet.[29]

(U) Russian Intelligence Collection Trends

(U) Russia is likely to continue aggressive use of its intelligence services to gain information concerning the United States, with increased emphasis on obtaining commercial or dual-use technology. Defectors and former intelligence officers from the former Soviet and Russian intelligence services predict that industrial espionage activities will escalate in the years ahead. Russia requires advanced technology to bolster its economy and foster increased technological progress. Defectors have stated that the SVR will target the increasing number of U.S. and Russian joint business ventures in an effort to obtain, legally or illegally, desirable Western technologies. In many

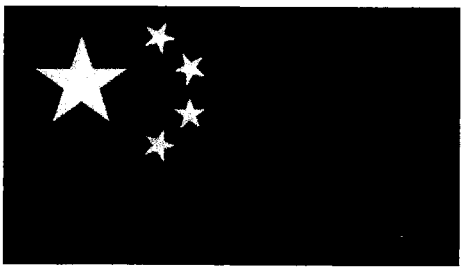
cases, the Russians cannot pay for the items needed to improve economic growth, so they are willing to steal or obtain them through other illegitimate means. Additionally, the Russians must still contend with restrictions on certain technologies that they desire.[30]

(U) Even though the opportunity to collect HUMINT expanded as a result of the relaxation of U.S. security standards focused on Russia, the reduction in the number of SVR intelligence officers, the closing of diplomatic facilities throughout the world, and the loss of access to former Warsaw Pact intelligence services will lead to a overall reduction in intelligence acquired through HUMINT. HUMINT may be more carefully targeted to gain information not readily available through technical intelligence collection or through open-source exploitation.[31] The Russians have always relied on open-source information and will continue to analyze public data and compare it with intelligence derived through classified sources. The Soviets previously used a variety of research and political institutes for the analysis of open-source data. The Russians retained a majority of these institutes. They are probably performing the same roles as they did under the Soviet Union.[32]

Defectors have stated that the SVR will target the increasing number of U.S. and Russian joint business ventures in an effort to obtain, legally or illegally, desirable Western technologies.

(U) A Different Approach to Targeting the United States

(U) *People's Republic of China*



(U) The People's Republic of China (PRC) practices a different approach to intelligence collection, compared to U.S. or Russian philosophies in this area.[33] The United States is a primary intelligence target of China because of the U.S. role as a global superpower; its substantial military, political, and economic presence in the Pacific Rim and Asia; its role as a developer of advanced technology that China requires for economic growth; and the large number of Americans of Chinese ancestry, who are considered prime intelligence targets by the PRC.[34]

(U//FOUO) With seven diplomatic establishments and an estimated 2,750 commercial offices, the PRC has established a large physical presence in the United States. Official and private exchange programs have raised the number of current and former PRC students in the United States to over 100,000. In addition, more than 27,000 PRC delegations visit the United States each year. Legal immigration is limited to 20,000 China-born individuals per year, but estimates of illegal entry by Chinese nationals run to many times that figure. The overall PRC presence in the United States is of intelligence significance because a large portion of the PRC's collection efforts against common targets like technology is conducted directly by PRC students, delegations, and commercial enterprises.[35]

(U) China's Intelligence Collection

(U) Although the PRC has a large professional intelligence apparatus, one of the hallmarks of its distinctive approach to intelligence collection is that many intelligence operations, especially those directed at science and technology targets, are not directed and controlled by the PRC intelligence services. As a rule, it is the "consumers" of intelligence such as institutes or factories that concoct and implement collection schemes, even when clandestine activity is required. These consumers of intelligence are able to carry out these strategies because of the large numbers of PRC students and visiting delegations coming to the United States and the large numbers of knowledgeable U.S. visitors going to China in reciprocal visits.[36]

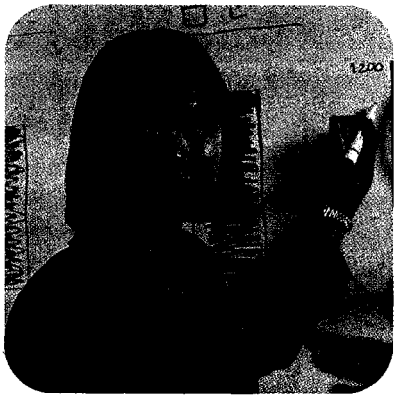
(U) In some instances, a delegation will visit a PRC consulate in the United States and identify the company that produces the technology or information the delegation is interested in. Intelligence officials will give the delegation members the names of company employees with whom the officials have established ties, and the delegation will appeal to them for covert assistance in obtaining a restricted item. If successful, the delegation may ask the consulate to use the diplomatic pouch to mail it back to China.[37]

(U) Another important dimension is that when delegations and PRC students or researchers have contact with U.S. laboratories or advanced research facilities, they as a rule do not attempt to steal or covertly acquire restricted information; they simply identify what they need and invite knowledgeable individuals to make reciprocal visits to the PRC. While there, the Chinese hosts will attempt to persuade the American guests to make unauthorized disclosures. The PRC students or delegation members thus become vectors, not for theft of information, but for convincing U.S. experts that they should give their technical knowledge away.[38]

A large portion of the PRC's collection efforts against common targets like technology is conducted directly by PRC students, delegations, and commercial enterprises.

(U) Because the "consumers" of critical information in the PRC in many instances know the identity of the U.S. source who provided it, one weakness of China's approach to collection is that it is relatively insecure. Another vulnerability is that, since the effort is dispersed among many collectors instead of channeled exclusively through the intelligence services, the methods used to obtain information can be extremely unsophisticated and inefficient. The main strengths of the PRC approach to collection are that the number of potential intelligence collectors is virtually limitless and the individuals who do the collecting know exactly what critical U.S. information will best suit their intelligence needs.[39] It is a system that is inefficient but not ineffective.

(U) For the OPSEC manager, China's approach poses the same basic questions as the Russian approach: which foreign nationals are attempting to collect restricted information and which employees are being targeted in the process? In the case of PRC intelligence activities, however, the problem is identifying suspects from among the people who are not intelligence officers, including tens of thousands of PRC nationals who enter the U.S. as students or visitors. The OPSEC task is further complicated by the fact that China's "cottage industry" intelligence collection is normally accomplished as an adjunct to normal, approved contacts with the employees of a targeted company. Many Chinese intelligence operations thus try to "piggyback" on sanctioned relationships. This means that OPSEC managers can face a much different problem when looking for intelligence situations involving China, because in China's approach to intelligence, the question is whether a given individual has had contacts of an unauthorized extent or nature with an individual he or she has permission to deal with. This contrasts with the Soviet-style problem, where the question usually is whether the individual has had a contact of some sort with someone he or she does not have permission to deal with.



(U) The potential impact on OPSEC of this approach to intelligence collection was vividly demonstrated in the investigation of Los Alamos scientist Wen Ho Lee and its aftermath. From the prosecutor's point of view, Lee had simply stolen copies of highly classified nuclear weapons design and test data, perhaps with a view to providing them to scientists in the PRC, with whom he had developed relationships much deeper than what he had reported to Los Alamos security officers. Lee's defenders argued that his contacts with counterparts in China were part of his normal, official duties, and his travel had been approved by Los Alamos administrators.

(U) PRC Intelligence Collection Organizations

(U) China has seven intelligence services, but only three conduct the PRC's covert intelligence operations against the United States: the Ministry of State Security (MSS); the Military Intelligence Department (MID); and the Liaison Office of the General Political Department (LO/GPD) of the People's Liberation Army. In addition to intelligence service collection operations, there is frequent direct intelligence collection by individual PRC institutes and factories, acting on their own behalf and beyond the control of the intelligence services. Signals intelligence and computer support for the operational services and other intelligence collectors is available from the Technical Department (also known as the Third Department) of the People's Liberation Army.[40]

(U) *MSS, the Ministry of State Security*

(U) The Ministry of State Security is the preeminent civilian intelligence collection agency in China. It was formed in June 1983 by combining the espionage, counterintelligence, and security functions of the Ministry of Public Security (MPS) with the

Investigation Department of the Chinese Communist Party, which had primary responsibility for acquisition of foreign intelligence. At the formation of the MSS, its MPS components were predominant. It continues to have a very strong and aggressive approach to counterintelligence, in particular regarding the suspicious activities of foreigners in China.[41]

The PRC's intelligence philosophy is to try to recruit agents before there is a specific need, and to recruit as many as possible.

(U) The MSS is divided into a number of different bureaus. Some focus on regions, e.g., the North American Affairs Bureau, while others such as the Counterespionage Bureau, are responsible for counterintelligence against all potential adversaries. Additionally, the MSS's Institute of Contemporary International Relations prepares all-source studies for the PRC leadership.[42]

(U) Most MSS officers in China are stationed at field offices in metropolitan areas. These offices are in many senses independent and do not appear to be closely supervised by MSS Headquarters in Beijing. This may account for the fact that some MSS offices, such as its Shanghai Bureau, are notably more aggressive against U.S. targets than other MSS offices. The Guangzhou and Beijing MSS field offices also target Americans more aggressively than other MSS components.[43]

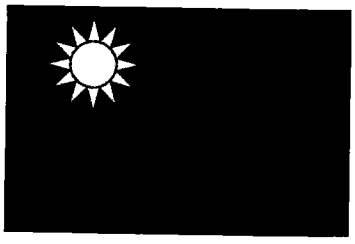
(U) As might be expected, MSS officers may occupy cover positions in virtually any PRC ministry, trading corporation, or private enterprise within China. They also use undercover slots abroad as diplomats, officials, businessmen, and students. In addition, it is very easy for MSS officers to join almost any PRC delegation traveling abroad, either for operational activity or for general familiarization purposes. Although there are specific MSS components charged with running technology-collection operations and there are standing intelligence requirements for such collection, the MSS does not appear to be notably active in organizing covert operations to collect U.S. technology.[44] Senior FBI officials have stated that the PRC intelligence services have made extensive intelligence use—most often for cover—of the thousands of commercial offices that China has opened in the United States.[45]

(U//FOUO) The primary operational focus of the MSS is "Taiwan work," namely, conducting intelligence activities against Taiwan in every intelligence and covert political action arena. To accomplish its objectives, the MSS also is heavily involved in assessing, developing, and recruiting ethnic Chinese targets. This ethnic recruitment approach to solving intelligence challenges is so pronounced that the Chinese-American community, (which is no more than one percent of the total U.S. population) is the target of an estimated 98 percent of MSS agent recruitment efforts. This practice is in marked contrast to the strategy of other U.S. intelligence adversaries,

The Larry Wu-Tai Chin Case

(U) One of the most serious PRC espionage cases to date was that of Larry Wu-tai Chin, who worked in various positions for the U.S. Government for more than 35 years. Chin, was recruited as a Chinese Communist Party member near the end of World War II, and his strong language skills earned him employment first at one of the U.S. consulates in China and then as an interpreter assisting with interrogations of captured PRC soldiers during the Korean Conflict. Some of the most serious intelligence damage done by Chin stemmed from the military information he passed to the PRC during that assignment. After Korea, Chin joined the Foreign Broadcast Information Service, a component of the CIA and was eventually stationed at its headquarters in Washington, D.C. From this post Chin also passed a large volume of information on U.S. policy regarding China and also some information on CIA operations he had access to. Chin, a frequent gambler at casinos, was motivated by money and was paid in excess of $300,000 for his services. He was run by a counterintelligence unit that later merged into the MSS. Chin provided his information on rolls of 35mm undeveloped film of documents that he smuggled out of his workplace overnight. His espionage activities were facilitated by frequent home-leave travel to Hong Kong. After retirement, he attempted to continue gathering information on the activities of his former coworkers. Chin was arrested and convicted of espionage in 1985 and committed suicide in his jail cell in early 1986 while awaiting sentencing.[240]

who, as a rule, focus only a fraction of their recruitment energies on members of ethnic communities. For example, while the Soviets also ran ethnic Russian agent recruitment operations, they were no more than about a quarter of their total HUMINT effort. There is no evidence that the PRC considers Chinese-Americans to be more vulnerable to approach than any other group. It is likely the PRC has adopted its distinctive ethnic-targeting intelligence strategy because it is much more capable of mounting effective approaches against individuals of ethnic Chinese ancestry than those of any other background. Also, the selling point in a normal PRC recruitment operation is not an appeal to ethnicity per se, but to whatever feelings of obligation the targeted individual may have towards China, family members in China, old friends in China, etc. The crux of the PRC's approach is not to try to exploit a perceived vulnerability but to appeal to an individual's desire to help China out in some way. Whatever the reason, ethnic targeting to arouse feelings of obligation is the single most distinctive feature of PRC intelligence operations.[46]

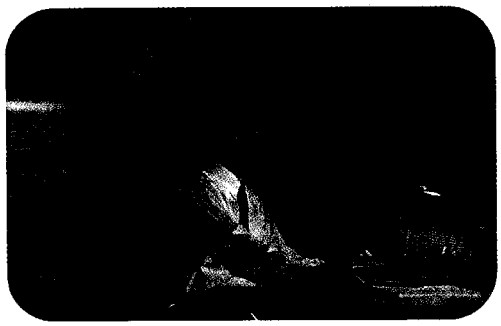


(U) The MSS operates under different intelligence concepts than the West, although some of its techniques are completely familiar. For example, in "secret work," some

MSS components are devoted to penetrating the intelligence services of PRC adversaries and to running secret agents of various types. Other MSS activities, however, would not normally be conducted by a Western service. "Strategic intelligence," for example, consists of culling information from sources such as *People* magazine, talking to pundits about prognostications, and then combining the two into a classified intelligence product for consumption by PRC leaders. The MSS considers it to be worthy of assigning intelligence resources to this product; in the West this would be considered only news or news analysis.[47]

The crux of the PRC's approach is not to try to exploit a perceived vulnerability but to appeal to an individual's desire to help China out in some way.

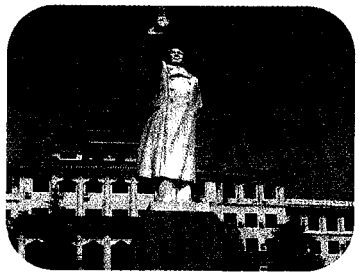
(U) Another intelligence practice that differs from Soviet and Western concepts is the use of recruited agents. The Soviet and Western intelligence services recognize that recruiting agents can be difficult, time-consuming, and expensive. They will not attempt to recruit an agent until a specific intelligence target emerges, so as to realize the full benefit from the agent's services. The PRC's intelligence philosophy is to try to recruit agents before there is a specific need, and to recruit as many as possible. Although this sort of approach consumes profligate amounts of time and effort, the PRC has the manpower resources to pursue this strategy. Moreover, when using recruited agents, the MSS prefers to gather a small amount of intelligence from many agents rather than concentrating on collecting as much as possible from just one. The entire process is sometimes referred to as "actuarial intelligence," because its basis is not unlike the principles that insurance company actuaries apply to determine the profitability of insuring large groups of people. This means that successful MSS attempts to recruit a Chinese-American are not always followed up with intelligence activity. Even when intelligence activity occurs, it may be slight.[48]



(U) *MID, the Military Intelligence Department*

(U) The MID, often referred to as the Second Department, is responsible for the collection and dissemination of the intelligence required to support the military command structure. The MID's realm of activities includes tactical, strategic, and technical intelligence operations. The MID reports directly to the General Staff Department (GSD) of the People's Liberation Army (PLA). MID intelligence gathering focuses primarily on the acquisition of order of battle, military geography, military doctrine, intentions, military economics, biographical intelligence, nuclear targeting, and military intelligence watch centers. In addition to the collection of relevant military information, the MID pursues foreign technological information, such as dual-use technologies. Taiwan is the MID's main intelligence target, but the United States is the second concern.[49]

(U) The MID is organized into numerous divisions and bureaus. HUMINT activities are conducted along functional lines by two collection bureaus, four analytical bureaus, and one bureau dedicated to science and technology. Of significant interest are the Western Nations Analysis Bureau, which conducts open-source intelligence collection; the Bureau of Science and Technology, which operates a number of technology-collecting enterprises; and the First Bureau, which is primarily engaged in the collection of military intelligence.[50]



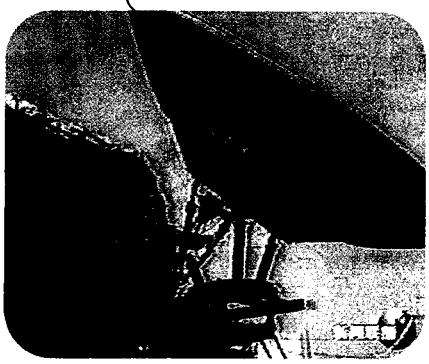
(U) The Beijing Institute for International Studies (BIIS), and the PLA Institute for International Relations provide academic analysis and training in support of PRC military intelligence needs. The BIIS is not openly associated with the MID, despite the fact that almost all of the institute's faculty are current or former PLA officers. It is not officially associated with the intelligence community, out of a fear that such an association would limit professional and academic contacts of the institute's members, hurting them both professionally and operationally. The PLA Institute for International Studies, formerly known as the Nanjing International Relations Institute, is responsible for teaching MID personnel techniques and methodology used in intelligence operations.[51]

(U) *LO/GPD, the Liaison Office of the General Political Department*

(U) The Liaison Office/General Political Department (LO/GPD), which is a component of the PLA, used to concentrate on targeting senior Taiwan military figures. The LO/GPD is also targeting the United States in military intelligence areas, but very little information on this has come to public notice.[52]

(U) *TD, the Technical Department*

(U) The Third Department (TD), known as the Technical Department, is responsible for Chinese SIGINT operations. The TD has the world's third-largest SIGINT effort. The Third Department was founded in the 1950s with equipment supplied by the Soviet Union. The Third Department maintains the most extensive SIGINT capability in the Asian-Pacific region. There are no reported instances of TD signals intelligence collection in the United States or elsewhere in the West, but TD officials occasionally travel to the United States in search of new technical equipment.[53]



(U) The TD can also provide technical surveillance of targeted Americans in China during their communications home. In addition, TD code breakers apply sophisticated, world-class technology to the task of breaking commercial code systems that travelers to China use to encrypt the data on their laptop computers.[54] It is not considered safe practice to assume that computers left in hotel rooms in China are safe from compromise by China's intelligence collectors, no matter how much commercial encryption is used to safeguard a visitor's files.

(U) PRC Intelligence Operations

(U) *HUMINT Operations*

(U) The MSS is the primary Chinese HUMINT collection organization for civilian and military intelligence, though the MID also engages in HUMINT collection operations regarding order-of-battle data and technology with military applications. The MID collects technical information through visits to trade shows, military exchange programs, and through its military attaché program. Both services collect overtly and covertly.[55]

(U//FOUO) The primary objective of Chinese intelligence operations targeting the U.S. government and its industry is to collect technical and economic information, with the dual purpose of making the Chinese military industrial base more sophisticated and the economy more competitive. In recent years, the Chinese have been the subject of approximately half of the cases initiated by U.S. law enforcement agencies concerning the illegal diversion of technology from the United States. The PRC also seeks information on U.S. trade positions and intentions, dual-use technologies, and trade secrets. In addition, the Chinese seek information regarding U.S. strategic interests in the South Pacific. While not particularly efficient in organization or practice, the Chinese have the ability to overwhelm U.S. law enforcement and counterintelligence because of the sheer quantity of operations they undertake.[56]

In recent years, the Chinese have been the subject of approximately half of the cases initiated by U.S. law enforcement agencies concerning the illegal diversion of technology from the United States.

(U) Chinese HUMINT operations primarily rely on collecting a small amount of information from a large number of people. To facilitate this collection strategy, the PRC relies on both recruitment and exploitation operations. The PRC attempts to recruit or at least "make friends with" as many Chinese-Americans as possible, apparently hoping that at least some will perceive an obligation to help China, perhaps on a confidential basis. Although their attempts to recruit agents only occasionally result in developing someone who will provide sensitive or classified information, the Chinese seem well satisfied with their strategy, perhaps because they attempt to develop confidential relationships with large numbers of people.

(U//FOUO) The PRC also attempts to exploit knowledgeable individuals visiting China, regardless of ethnic origin. Intelligence is obtained from unwitting sources through various elicitation techniques, primarily by maneuvering the individual into a social or professional situation in which he can be embarrassed or cajoled into providing at least a little extra information. The actual elicitation in China is done by Chinese intelligence "consumers" themselves, although intelligence officers may have a role in manipulating a targeted individual into a situation where he is at a disadvantage. For example, it is not uncommon for the Chinese to arrange for a targeted visitor to go on an all-day sightseeing excursion, after which they will throw a cock-

tail party in his honor, toast him with potent Chinese liquor as much as possible, and then surround him with a small group of questioners asking about sensitive topics. Under the strain of fatigue, alcohol, and group pressure, some U.S. visitors have made indiscreet statements or unauthorized disclosures. Some ethnic Chinese targets may be exploited through elicitation in this manner while they are also being assessed for an eventual recruitment approach.[57] It is probable that the intelligence product produced by China's exploitation operations is many times larger than that produced by recruited agents, though by its nature it is hit-or-miss.

(U//FOUO) The PRC intelligence services have also dispatched agents or staff officers to the United States to become long-term "sleepers" with absolutely no immediate intelligence function. They believe if large numbers of PRC nationals leave China and settle permanently in the United States, some of them may some day find their way into positions of intelligence potential. When they are in position, these individuals will be approached on the basis of loyalty to their ancestral land, and some may be persuaded to cooperate, at least on a limited basis.[58] Again, this appears to be a symptom of China's "actuarial" approach to intelligence.

(U) Examples of PRC HUMINT Operations

(U) *The Peter Lee Recruitment Case*

(U) In 1997, physicist Peter Lee pled guilty to filing false statements and to divulging classified information to PRC scientists. Lee, who grew up in China and Taiwan, immigrated to the U.S. with his family, graduated from the California Institute of Technology with a PhD in Aeronautics, and became a naturalized citizen in 1975. From 1976 to1984, he worked as a physicist in a program at Lawrence Livermore National Laboratories that specialized in the use of laser power to initiate nuclear reactions. In 1981, he began a correspondence with scientists in the PRC that by 1997 included over 600 letters or E-mail messages.[59]

(U) In 1984, Lee moved to Los Alamos National Laboratory, where he worked on a laser program as a contract employee. In early 1985, Lee traveled to China with a group of scientists at the invitation of a Chinese visitor to his laboratory. Lee was supposed to act as a translator for the American delegation. Lee later recounted that a Chinese nuclear-weapons scientist visited him in his hotel room and asked for his help, saying that China was a "poor country." The Chinese scientist drew a diagram and asked questions about Lee's laser research. Lee discussed problems the United States was having in its nuclear weapons testing simulation program, later explaining that he decided to help because he wanted to bring

China's scientific capabilities "closer to those of the United States." The next day, Lee was picked up at his hotel and driven to another hotel to meet a group of Chinese scientists. He answered their questions for two hours, drawing diagrams and providing specific mathematical and experimental results related to laser fusion research.[60]

(U) Lee stayed at Los Alamos until 1991, when he went to the space and electronics group of TRW Inc., in Redondo Beach, California. At TRW, he worked on a classified satellite radar imaging research program. Lee divulged information about the program, which had submarine-detection military applications, in a two-hour lecture in Beijing in May 1997. He was questioned about his work's applications for antisubmarine warfare, and showed the audience a surface ship wake image that he had brought with him from his lab. After a detailed discussion of the physics of his work, he tore the ship wake image to shreds after leaving the meeting. On his return to the US, he filed a false trip report to TRW security officers, claiming that his trip to China had been for pleasure, not business.[61]

(U) Government officials originally planned to charge Lee with espionage, but this was made problematic, since the information he had divulged in 1985 was subsequently declassified, and the U.S. Navy was unwilling to disclose radar information needed to support an espionage prosecution in open court.[62] At his sentencing hearing, Lee told the judge that he had been carried away by "scientific enthusiasm." U.S. and PRC scientists also circulated a petition decrying the prosecution as an infringement of scientific freedom. Over the strenuous objections of federal prosecutors, the judge declined to put Lee in prison and sentenced him to 12 months in a halfway house with three years' probation and a fine of $20,000.[63]

(U//FOUO) *A PRC Intelligence Exploitation Attack On a Senior U.S. Science Official Visiting China*

(U//FOUO) In 1980, a senior scientist from Los Alamos National Laboratory traveled to a research institute in the PRC to talk about his specialty, nuclear fusion. Although he was knowledgeable about U.S. nuclear weapons design information, he was determined to stick to his topic and not wander into loose talk about secret information. Nonetheless, the scientist found himself being peppered with increasingly detailed inquiries that related directly to nuclear weapons. Benign inquiries about fusion and astrophysics soon gave way to pointed requests for information about such highly classified matters as the ignition conditions of the hydrogen isotopes deuterium and tritium - and about the then-new neutron bomb.[64]

(U//FOUO) The scientist did his best to fend off the demands for specifics, but at a cocktail party thrown in his honor by his hosts, he did compromise on his previous position by offering an analogy. What would happen, he mused to a group of questioners, if you rolled deuterium and tritium into a ball and then rolled the ball off the end of a table? Deuterium and tritium ignite at such low temperature levels, he told

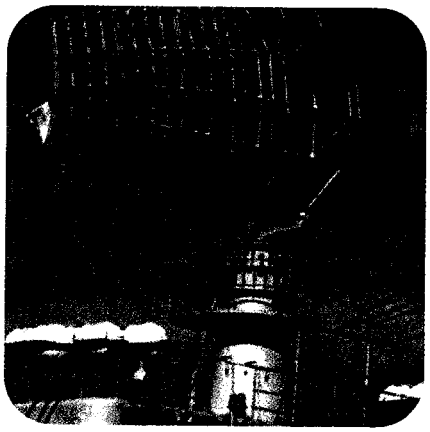
his listeners, that you could just about get ignition by dropping them on the floor. Although the scientist did not consider this particular piece of information to be critical to neutron bomb design, it may have launched his PRC counterparts along a new and more productive line of experimentation than what they had been working on.[65]

Completely benign conversations can turn into uncomfortable situations in China.

(U//FOUO) His experience made a deep impression on the scientist, who even years later used this example many times to show younger colleagues "how completely benign conversations could turn into uncomfortable situations in China." Given the PRC's intelligence strategy of trying to collect small amounts of intelligence from many individuals over a long period of time, it is likely that a number of knowledgeable U.S. scientists had similar experiences but did not report them in as much detail.[66]

(U) SIGINT

(U//FOUO) As mentioned earlier, the PRC has the third largest SIGINT effort in the world. The Technical Department provides the PRC with a wide range of SIGINT capabilities. They monitor signals from India, Japan, Russia, South Korea, Southeast Asia, and Taiwan. Signals from U.S. military units located in the region are of particular interest to these monitoring stations. In addition, the Chinese appear to be developing a spaceborne ELINT system mounted on photoreconnaissance and communications satellites. There is no indication that this capability presents a significant threat to U.S. forces in the region. The recent acquisition of Hong Kong offers the Chinese additional facilities in the region; it is likely that these will used to monitor communications to and from Hong Kong. Additionally, the Chinese have developed a series of SIGINT collection vessels that monitor U.S. military operations and exercises in the Asian-Pacific region.[67]



(U//FOUO) The Third Department maintains several dozen SIGINT ground stations throughout China. These stations actively monitor U.S., Indian, Japanese, Korean, and Russian communications in the region. The majority of these stations are located within several hundred miles of the PRC's borders or coast. In addition, the Chinese navy operates several vessels with SIGINT capabilities. Furthermore, the acquisition of Hong Kong provides the PRC with an additional listening station to monitor transmissions within Hong Kong. In addition to sites located within China's borders, the Third Department maintains several SIGINT facilities, such as in Burma; Rocky Island, in the Paracel Archipelago; and the Cocos Islands, in the Andaman Sea. This gives China an extensive capability to conduct sophisticated SIGINT operations throughout Southeast Asia.[68]

(U) IMINT

(U//FOUO) The Chinese have a limited spaceborne photoreconnaissance capability that focuses on collecting imagery over the Russian border. They also use a variety of fixed-wing aircraft to collect photographic imagery. None of these systems presents a substantial intelligence collection threat to U.S. forces in the region. U.S. intelligence agencies believe that China will probably develop a mid-resolution imaging system in the future that will improve Chinese capabilities.[69]

(U) PRC Intelligence Collection Trends

(U) The PRC spent more than two decades establishing a large and diverse intelligence infrastructure in the United States but only relatively recently gained attention by drawing upon its intelligence capabilities. Recent investigations of PRC political influence operations directed at U.S. legislators and of apparent PRC nuclear espionage operations targeting the U.S. national laboratories are just the tip of the iceberg of an already-large and increasingly capable PRC intelligence effort.[70] While it is expected that China will improve its SIGINT and IMINT capabilities-increasing the collection threat to the United States-the majority of intelligence will probably continue to come from HUMINT and open-source collection activities.[71]