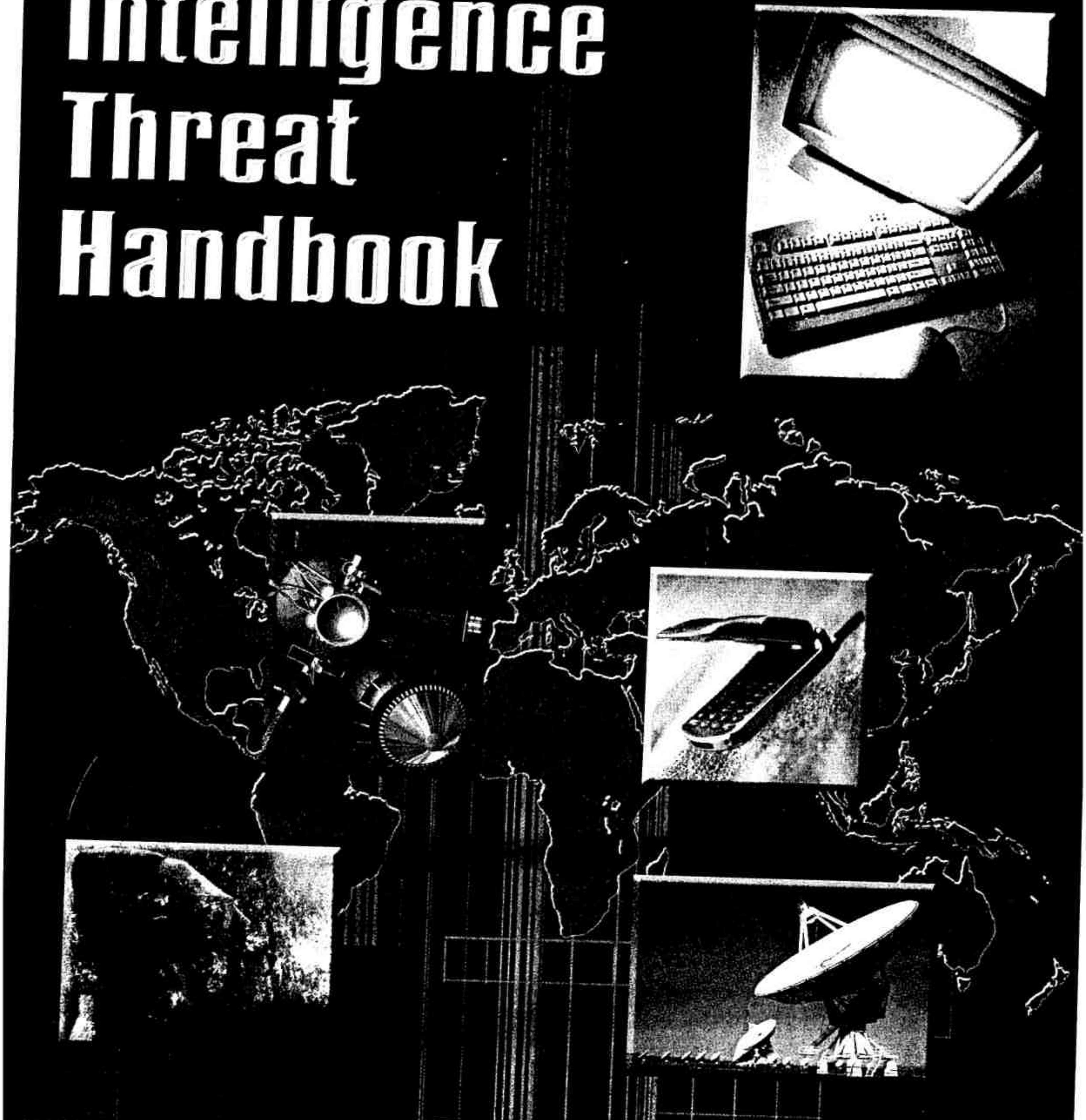
Intelligence Threat Handbook



INTERAGENCY OPSEC SUPPORT STAFF

Operations Security Information Series

The **Interagency OPSEC Support Staff (IOSS)** was created to support the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products and presenting conferences for the defense, security, intelligence, research and development, acquisition and public safety communities. Its mission is to help government organizations develop their own, self-sufficient OPSEC programs in order to protect U.S. programs and activities.

Our **Vision** is secure and effective operations for all National Security Mission activities.

Our **Mission** is to promote and maintain OPSEC principles worldwide by assisting our customers in establishing OPSEC programs, providing OPSEC training and conducting OPSEC surveys.

Our **Goal** is to be recognized as the leader and preferred provider of value-added OPSEC products and services.

PURPLE DRAGON:

In the early days of the Vietnam War, the U.S. lost an alarming number of pilots and aircraft. To reverse that trend, a team was assigned to analyze U.S. military operations. The team, "Purple Dragon," discovered that crucial planning information was being disclosed through routine patterns of behavior. Countermeasures were quickly initiated. Purple Dragon's analytic process, called **OPerations SECurity or OPSEC**, was used by the military for the next 20 years. In 1988, President Reagan formalized its use throughout the government and created the IOSS to provide training and guidance to the national security community.

The Intelligence Threat Handbook was researched, written and designed for IOSS by the Centre for Counterintelligence and Security Studies, cicentre.com.

Table of Contents

(U) Overview

(U) The purpose of this handbook is to provide unclassified threat reference information for Operations Security (OPSEC) personnel and managers. This handbook explains the categories of intelligence threat, provides an overview of worldwide threats in each category, and identifies available additional resources for obtaining threat information and outside assistance. The information presented has been drawn entirely from open-source reference material and, therefore, may be disseminated to the largest possible audience in order to increase the awareness of intelligence threats targeting U.S. government and industry.

(U) OPSEC is a set of procedures and methodologies that provides a way for program, project, or facility managers to implement cost-effective measures to protect their programs and staff from exploitation by adversaries. The key to effective OPSEC is to determine both what critical information most needs to be protected and how a potential adversary would most likely attempt to exploit weaknesses to obtain that information. An organization's OPSEC officer must understand the range of threats that confront the organization. Although many categories of threat that may be considered, most OPSEC activities focus initially on the intelligence collection threat.[1]

(U) While U.S. organizations and their staff are the targets of a large number of intelligence collectors worldwide, the specific collection methodologies deployed against U.S. targets are limited. Moreover, intelligence methodologies tend to change only slowly and are intended to be used against many targets. The starting point for the OPSEC manager is to become familiar with the intelligence procedures and methodologies used by adversaries, to determine how an intelligence attack on his facility would most likely be carried out. In the wake of the 11 September 2001 terrorist attack on the United States, attention to intelligence procedures and methodologies has become even more critical, because experience indicates that every successful terrorist attack has been preceded by at least one successful intelligence attack to gather information about the intended target.

Every successful terrorist attack has been preceded by at least one successful intelligence attack to gather information about the intended target.

(U) This handbook will provide OPSEC officers with information on how intelligence collection programs most often target and collect against individuals and institutions of interest. To simplify study of the different ways in which U.S. critical information is targeted by foreign collection programs, this handbook focuses on the collection mechanisms, strategies, and capabilities of the Russian Federation and the People's Republic of China. Although often targeting the same information, Russia and China approach their collection operations from very different intelligence perspectives.[2] This complicates the OPSEC process of determining threat, risk, and effective countermeasures.

(U) More details on specific intelligence organizations of other U.S. intelligence adversaries are included in Appendix A. Information about available U.S. Government resources is provided in Appendix B.

(U) Nature of the Threat

(U) Intelligence threat, as it applies to OPSEC, is defined as the intention and capability of any adversary to acquire and exploit critical information. The purpose of the acquisition is to gain a competitive edge or diminish the success of a particular U.S. program, operation, or industrial activity.[3]

(U) Changing Nature of the OPSEC Challenge

(U) While the end of the Cold War caused a dramatic drop in the military threat to U.S. security interests, it also gave rise to a significant increase in the OPSEC threat. Although there has been an easing of political and military tensions since the collapse of Soviet-style communism, there has not been a corresponding reduction in the level of espionage and other activities threatening the United States. In fact, foreign intelligence activities have grown in diversity and complexity over the last several years. OPSEC must become more diverse in order to confront the evolving threat environment. That environment now also includes a large number of terrorist organizations.

(U) Changing Nature of the Intelligence Environment

(U) *More Exchange Programs*

(U) A natural byproduct of less antagonistic relations with former military adversaries has been an increase in exchange programs. Because of this, U.S. facilities have been flooded with large numbers of foreign students, research scholars, and commercial delegations. Such exchanges, in turn, create increased opportunities for knowledgeable staff members of U.S. facilities to travel overseas on reciprocal visits—far from U.S. security and counterintelligence capabilities.

(U) Several other factors have combined to create significant changes in the overall OPSEC environment. Now, in addition to individual-country threats, there are transnational groups, such as terrorists, organized criminals, and economic competitors that engage in traditional intelligence collection activities.[4] This has been made possible by the fall of the Soviet Union, an event which threw many professional intelligence officers out of work, with little but their intelligence skills to fall back on.

(U) *A KGB Intelligence Training Connection*

(U) With the emergence of many newly independent states in Africa and Asia in the 1960s, the KGB founded the Foreign Intelligence Training Center in Moscow to provide special courses for the intelligence services of the new countries. This training was of a lesser quality than that provided to Soviet intelligence personnel or intelligence officers from former Bloc countries.[5]

(U) The fall of communism turned the training situation topsy-turvy. There now was very little demand for large-scale specialized training for former Soviet citizens, and no such interest at all from the Bloc. Intelligence instructors became more available for third-world students, and the those nations in turn became more interested in the training, since it no longer came with a strong dose of communist indoctrination and potential Soviet political interference. The KGB Training Center quickly evolved into a commercial entity.[6]

(U) One current Training Center intelligence professor put it this way to a former colleague:

> (U) *"Now we are after money, not ideology. In 1991, of course, if a foreign entity like the Cali Cartel openly asked us to train their personnel, we would refuse. If, however, the Cartel was smart enough to use a cover such as calling themselves personnel security officers from a Colombian or international bank, then we didn't mind training them. After all, in 1991, the government destroyed our jobs and threw us on the streets. We have to take care of ourselves. International crime is not our problem; for us, the name of the game is survival."*[7]

(U) Russian intelligence professors are available on a pay-as-you-go basis to teach the following courses to all who are interested: international security threats; agent networks; recruitment strategy and tactics; agent handling; countersurveillance theory and practice; signals intelligence and eavesdropping operations; and counterintelligence strategy, tactics, and practices.[8]

(U) *More Joint Ventures*

(U) In the United States, many facilities formerly dependent on defense contracts have found themselves in search of continued sources of funding. They have commonly responded to this challenge by instituting commercial joint ventures with private concerns. This has increased opportunities for information to flow outward and created direct economic incentives for sharing as much information as possible. The realities of joint-venture economics opens a de facto official umbrella for establishing and nurturing close relationships with those potential collectors of intelligence who also have a commercial dimension. In some cases, the same resources that were formerly dedicated to defense technical research and production are now designated for joint-venture technical commercial projects with entities representing former U.S. military adversaries.

(U) *The Internet*

(U) The current information explosion via computers and the Internet has also changed the OPSEC environment. Computers are constantly growing faster and more powerful while becoming smaller. In the past, just locating a possible source of desired information was a considerable stumbling block in the path of U.S. intelligence adversaries. With rise of the Internet and vast increases in data-storage capabilities, this is no longer the case. Many American businesses, including the military, use computers to communicate and store most information. Most have their computers internally networked to facilitate better and faster communication (Intranet or LAN). They also have external access to the Internet, and advertise their wares and capabilities on websites.

(U) While the Internet is a superb vehicle for advertising and informing the population at large, many businesses have not yet found the correct, and often delicate, balance for posting information on the Internet-thereby creating a virtual OPSEC nightmare. This E-business explosion, and often unchecked posting of information on websites, has made it much easier for foreign countries, non-government entities, and even motivated individuals to locate and focus on specific targets and feast on the information given away so freely.

(U) For example, Russia's Center for Automated Data Exchanges (once subordinated to the KGB and now believed to play a central role in the computer intelligence collection activities of its successor agency, the SVR) is a client of several on-line databases such as those provided by the Library of Congress, LEXIS/NEXIS, U.S. National Technical Information Service, and the International Atomic Energy Agency, and has direct access to data networks in the U.S., Canada, France, Germany and the United Kingdom. The Russians also have established accounts with multiple Internet service providers such as America Online, CompuServe, and the European

Union's EuNet.[9] Russia is only one country of many to have these capabilities; there are at least 20 others considered "critical countries" on various U.S. government lists at any given time.[10]

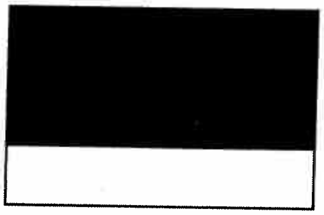
(U) Collectors around the world dedicated to the Internet collection effort no longer have to leave their homes to gather information; they can access it from the comfort of their armchairs in seconds rather than traveling for days and spending vast amounts of money to locate a source that may or may not have the morsel of information they seek.

Many businesses have not yet found the correct, and often delicate, balance for posting information on the Internet thereby creating a virtual OPSEC nightmare.

(U) Foreign Espionage

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

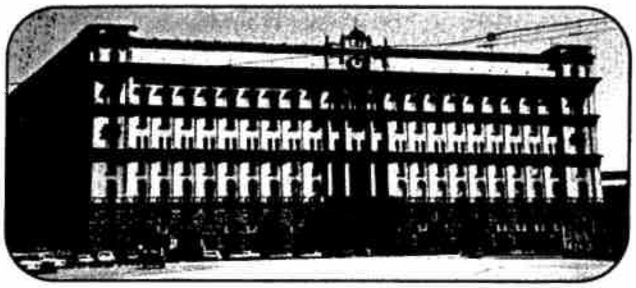
(U) *Russian Federation*



(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 declarations 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]

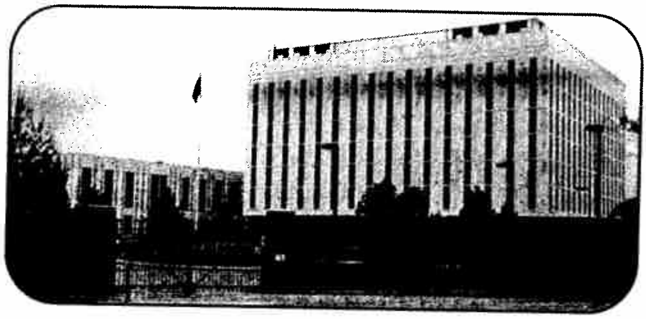
(U) The Soviet or Soviet-trained approach to intelligence collection poses two main problems for OPSEC managers: determining the activities of the adversary's intelligence officers, and monitoring the activities of employees to see if they are in contact with the intelligence officers. Further, because 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-

The Gusev Incident

(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.

(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:

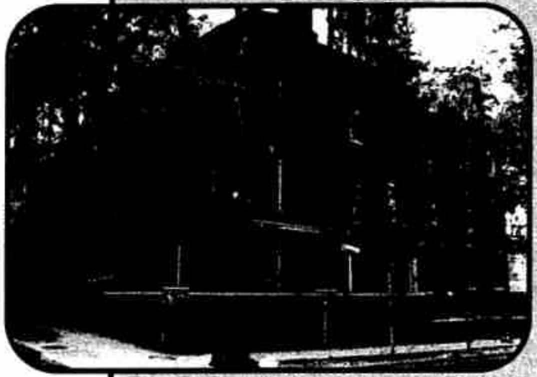
> (U) *"Once the FSB or SVR officer targets a Russian émigré for recruitment, they approach them, usually at their place of residence, and make an effort to reach an understanding. If he or she*

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]

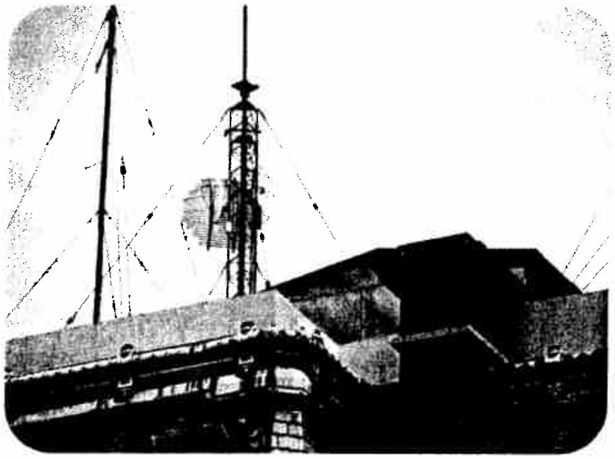
(U) Even after the failure of August 1991 attempted coup, the number of HUMINT operations conducted by the SVR and KGB targeting the United States and the West continues to rise. This is due to a number of factors. First, as a result of arms control treaties, joint business opportunities, and cultural 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]



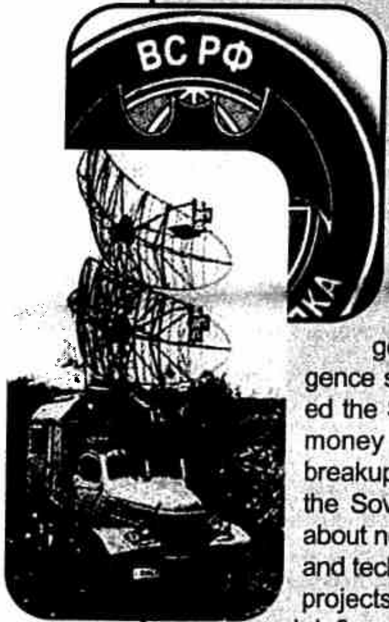
(U) The former Soviet Union also used a variety of other means to collect signals intelligence, and it is believed that Russia continues these activities in the United States. The locations of a number of Russian diplomatic facilities in the United States facilitate SIGINT access to sensitive information. 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.

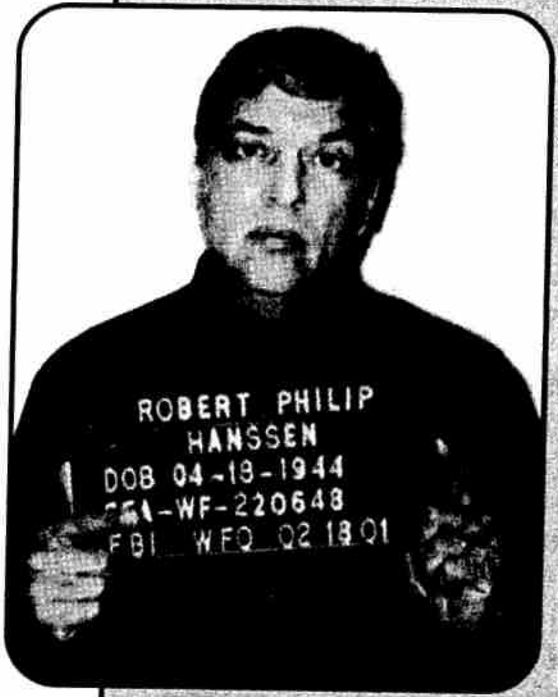
(U) In late 1985, Robert Hanssen was on the verge of leaving a job at FBI Headquarters in which he supervised a group of analysts studying Soviet intelligence techniques. In that position he had also acquired a reputation as someone who could understand and succinctly explain the technical aspects of 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,



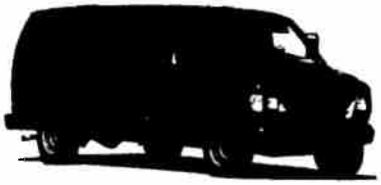
Hanssen broke off communications with the KGB, for security reasons. In 1999, however, Hanssen contacted the SVR, one of the Russian successor agencies to the KGB, and resumed passing intelligence, this time because of college expenses for his children and the desire to remodel his kitchen.

(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

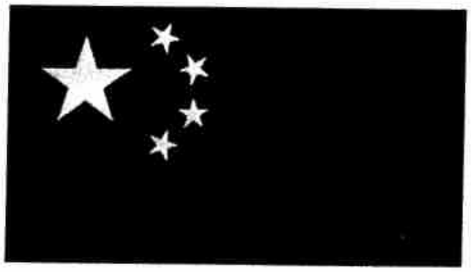
(U) Russia is likely to continue aggressive use of its intelligence services to gain information concerning the United States, with increased emphasis on obtaining commercial or dual-use technology. Defectors and former intelligence officers from the former Soviet and Russian intelligence services predict 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]

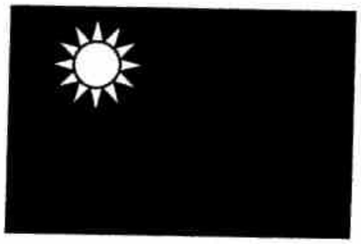
(U) As might be expected, MSS officers may occupy cover positions in virtually any PRC ministry, trading corporation, or private enterprise within China. They also use undercover slots abroad as diplomats, officials, businessmen, and students. In addition, it is very easy for MSS officers to join almost 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]

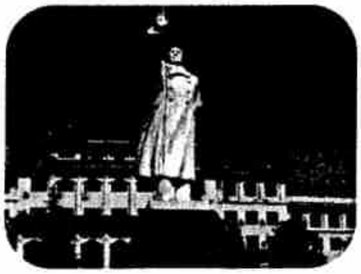
The crux of the PRC's approach is not to try to exploit a perceived vulnerability but to appeal to an individual's desire to help China out in some way.

(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]

(U) Economic Espionage

> "Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor... the companies are training the armies and the unemployed are the casualties."
>
> BERNARD ESAMBERT

(U) Economic espionage has always been a factor in relations between competitor nations. For example, in 1811 an American merchant, Francis Cabot Lowell, toured Scotland and England, ostensibly for "reasons of health," and in the process either memorized or purloined enough information concerning British textile mills to return to Boston and build a copy of the Cartwright loom. That particular tightly guarded device had revolutionized British textile production, and it subsequently helped Lowell build a complex of mills that propelled the U.S. into its own industrial revolution.[72]

(U) As the 21st Century begins, the lines of espionage are becoming less and less clearly defined. Because nations are now linking their national security with economic security, the spy of today may not be after the composition of a new warhead, because that is no longer a lucrative market. He may instead be collecting the scientific and technological data that goes into making a computer chip for a high-tech automobile, or the formula of a new cancer drug. In the words of Bernard Esambert, President of France's Pasteur Institute, "Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor...the companies are training the armies and the unemployed are the casualties."[73]

(U) Economic espionage often is not targeted at the "crown jewels" of U.S. technological supremacy. Instead, much of the sought-after information and technology is dated military-related or infrastructure-supportive material that is no longer classified but has both military and civilian applications. Although unclassified, information of interest usually is subject to control through government regulations.[74]

(U) Costs of Economic Espionage

(U) There has been a growing recognition of the cost of economic espionage. For example, in a 1999 American Society for Industrial Security survey of 1,000 U.S. companies, there were 579 reported losses of proprietary information. Loss of intellectual property totaled $45 billion. By 2001, this figure had risen to an estimated $59 billion. The average company responding reported 2.45 incidents, with the average loss per incident at over $500,000. Most of the incidents took place in high technology or service companies, with reported losses of intellectual property up sharply in 2001. Manufacturers reported fewer incidents—a total of 96—but suffered an average loss of nearly $50 million per incident.[75] According to a 1998 report to Congress on espionage, the actual figure may go as high as $300 billion.[76] The U.S. Chamber of Commerce estimates that losses today continue at roughly $2 billion a month.[77] Most U.S. companies do not have effective mechanisms for safeguarding their proprietary information, nor do they have consistent and effective mechanisms for determining the value of such information.

(U) These figures look less abstract if one applies what is known as the "economic loss model," developed by the Pacific Northwest National Laboratory. This model, applied to a single FBI case of economic espionage showed these results:

- (U) The foreign competitor captured the market
- (U) The U.S. business lost $600 million in sales
- (U) 2,600 full-time were jobs lost
- (U) 9,542 jobs were lost to the U.S. economy as a whole over 14 years
- (U) U.S. trade balance was negatively impacted by (U) $714 million
- (U) Lost tax revenues amounted to $129 million[78]

(U) Emerging Policy

(U) Although economic espionage has always been a part of the commercial landscape, it is only recently that it has been identified as a national problem at which U.S. intelligence resources should be deployed. This policy shift has taken place because over the past 40 years the U.S. has undergone a gradual paradigm shift concerning the general intelligence threat to the country. Prior to 1980, for example, the FBI defined the intelligence threat to the United States in terms of "the presence of hostile intelligence services and their diplomatic establishments in the United States." A country was deemed to be "hostile" if it met certain classified national-security criteria.[79]

(U) All this changed in 1981, however, when the French government provided U.S. authorities information from a Soviet source code-named "FAREWELL." In reality, FAREWELL was Vladimir Vetrov, a KGB intelligence officer with a senior analytical post in Directorate T, which was responsible for collecting strategic, military, and industrial technology from the West. Vetrov eventually provided the French with more than 3,000 documents detailing Soviet operations, which were more successful and much larger in scope than anyone had suspected.[80] Vetrov's reporting provided important documentation of the following:

Vetrov eventually provided the French with more than 3,000 documents detailing Soviet operations, which were more successful and much larger in scope than anyone had suspected.

- (U) The State Committee on Science and Technology determined what information must be collected and developed tasking for Line X, the operational unit which carried out the bulk of the collection objectives. Line X, however, was not the only entity to receive tasking from this committee. The GRU, the Soviet Academy of Sciences, and the State Committee for External Relations were assigned this collection mission, as well.[81]
- (U) It was not intelligence operatives trained to act like scientists who carried out the collection objectives; rather, it was the task of actual scientists who had been trained as collectors to gather the information. This meant that actual scientists could evaluate and decide on the spot if the information they had access to bore any relevance to the collection objectives with which they were tasked, and also if the information was worth the collection effort.[82]
- (U) The U.S. foreign policy of engagement with the Soviet Union provided broad access for these collectors and opened many new avenues for exploitation, few of which escaped Soviet intelligence. Beginning in 1972, delegations of Soviet specialists arrived in the U.S. in droves to visit companies and laboratories around the country.[83] Further, the Soviet Union was quickly acquiring information for about 1% the cost of what the West spent in developing it over many years.[84]

(U) Vetrov's reporting later was confirmed and amplified by Vasili Mitrokhin, a former KGB officer who, over more than a decade, hand-copied and archived a wealth of information from Soviet intelligence files. According to Mitrokhin, during the mid-1970s, the KGB made unprecedented use of the Soviet scientific community in intelligence operations. For example, the KGB's Directorate T succeeded in developing approximately 90 agent-recruiters, 900 agents, and 350 trusted contacts among the ranks of Soviet scientists. Of these, 77 agents and 44 trusted contacts reported on Western high technology. The intelligence role of the Soviet scientists was to talent-spot Western scientists in areas of intelligence interest, approach them on a personal or institutional level for cooperation, and collect information from them.[85]

(U) The intelligence treasure trove from FAREWELL was a factor in the FBI's 1985 shift in its view of the intelligence threat to the United States away from intelligence-service presence to a definition that focused on activities directed by intelligence services against the U.S., regardless of where those activities occurred or what country initiated them.[86]

(U) In the early 1990s, the winding down of the Cold War caused the FBI to again reassess the overall intelligence threat to the U.S. This time, the FBI developed a strategy that focused on the targets of intelligence activities, such as proprietary technology, data, and employees.[87] This shift took place at about the same time that the extensive direct involvement of France's intelligence services in economic espionage against the U.S. became public knowledge.

(U) In October 1996, the Economic Espionage and Protection of Proprietary Economic Information Act was signed. The new law had two primary elements not previously covered by U.S. law.

- (U) First, it allowed U.S. national intelligence resources to be used on more foreign intelligence organization activities, and not only when they targeted classified government information and programs. In particular, the Economic Espionage Act allowed U.S. agencies to investigate cases where a foreign intelligence service, applying traditional methodologies, mounted an intelligence attack against a U.S. company to gather proprietary information to support the commercial interests of a foreign company.
- (U) Second, the law extended the definition of "goods, wares or merchandise" protected by Federal anti-theft statutes to include the "proprietary economic information" of a company. This permitted Federal investigation and prosecution in the event that the information was used in interstate commerce.

(U) The Outsider Threat

(U) Most organizations conceptualize the main threat to their operations security as coming from outside the organization. In the realm of economic espionage, the main "outsider" threats come from company-to-company attacks launched by economic competitors, attempts to purloin critical intelligence through duping unwitting employees of the organization, and even through the direct involvement of foreign intelligence services.

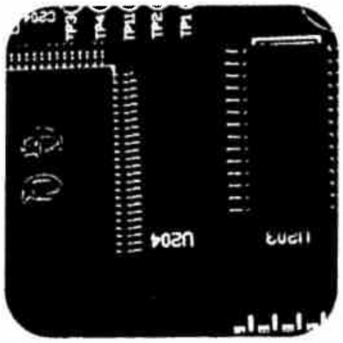
(U) Foreign or Domestic Competitors

(U) Competitor companies have been responsible for many instances of economic espionage against their U.S. counterparts. A frequent scenario is one in which an employee leaves his company and goes to work for the competitor, taking proprietary information with him. The following is a representative sample of competitor-company economic espionage against a variety of U.S. technologies:

(U) *Automotive Glass Manufacturing Process*

(U) In late 1973, John Akfirat, a research engineer in the Glass Division of Ford Motor Company was discovered to be in negotiation with a Portuguese automotive glass manufacturer in competition with Ford. Akfirat was to be paid $250,000 for delivering the proprietary information, and he would also be hired by the company at a good salary. Ford had licensed the revolutionary glassmaking process from its British inventor for $1.25 million and substantial royalties. The Portuguese competitor could have used the critical information to capture the European auto glass market from Ford, which calculated its potential loss at $2.79 million. Akfirat was convicted and received 60 days in jail and a $10,000 fine. Shortly after his release from jail in 1974, Akfirat got a job at another glass company, and he and his new boss began to travel frequently to Romania to talk with officials there about the proprietary glass manufacturing process. By 1978, he and his boss had exported specialized glass-manufacturing equipment to Romania, in the process making false statements in the export documents required. In 1983, Akfirat was again arrested for ongoing fraud against Ford. He admitted to meeting with Romanian officials as part of a scheme for constructing a plant there which would use the process Akfirat had learned from Ford and to providing the Romanians with computer hardware and software. This time Akfirat was convicted and sentenced to four months of community service, two years probation, and a $1,000 fine. His boss was not prosecuted, but the company did have to pay monetary damages both to Ford and the British company that invented the manufacturing process.[88]

(U) *Computer Chip Designs*



(U) In 1979, PRC nationals opened a computer chip manufacturing plant in California named Chipex, Inc. Chipex supposedly was a joint venture with a Hong Kong firm, but in actuality the Hong Kong company was itself a subsidiary of a PRC electronics company. The ostensible purpose of the plant was to manufacture chips from designs provided by U.S. companies, while at the same time training PRC nationals on how to use the manufacturing equipment. In reality, however, Chipex also was illegally copying its customers' proprietary designs and sending them to its parent corporation in China. U.S. Customs Service and the Commerce Department raided Chipex in 1982 and shut it down. The subsequent investigation determined that the PRC's San Francisco Consulate provided support and guidance to Chipex's operations, and several PRC students were used in duplicating the proprietary U.S. designs.[89]

(U) *Microwave Tube Design Drawings*

(U) In 1989, Ssangyong, a large South Korean conglomerate, purchased a U.S. microwave technology company, M Square Microtec, Inc. M Square was participating in a microwave technology joint venture with Litton Systems, which held U.S. defense contracts. Litton soon discovered that M Square had stolen some of its proprietary radar and microwave tube design drawings and passed them on to Ssangyong. Litton notified the FBI about the situation, but the intangible nature of its loss precluded criminal investigation. Litton Systems pursued the matter through civil litigation, and in the process, uncovered Ssangyong documents detailing its strategy to undercut Litton's prices, which had to reflect research costs. In 1995, Litton Systems was awarded a summary judgment of $65 million against Ssangyong.[90]

(U) *Organic Fertilizer*

(U) In late 1994, three representatives of a South Korean firm visiting the laboratory of Rubicon/Pacific Trading Group to view a sales presentation of its new organic fertilizer were observed dipping their ties in a solution of the product. The three visitors then pulled out cameras and fanned out in different directions, photographing everything in sight. Rubicon's new fertilizer was more productive, environmentally friendlier, and cheaper than its main alternative and had a potentially huge market, especially in Asia. Rubicon later had problems trying to interest South Korean farmers' associations in using the fertilizer.[91]

(U) *Cancer Drugs*

(U) In June 1997, Hsu Kai-lo and Chester H. Ho (naturalized U.S. citizens) were arrested by the FBI for attempting to steal the formula for Taxol, a cancer drug patented and licensed by the Bristol-Myers Squibb Company. Hsu and Ho were employees of

Adhesives Formulas

(U) An employee of FIELCO Industries received a phone call from a Mexican national offering the employee up to $10,000 for information on the formulas for his company's state-of-the-art adhesives. The employee notified his supervisors of the approach, and they called in U.S. law enforcement authorities. The caller subsequently mailed the employee $2,000 in cash and asked to be faxed some of the information. The facsimile number provided matched that of one of FIELCO's customer companies in Mexico. When the caller flew to the U.S. to pay the employee the balance of the bribe money, he was arrested. FIELCO estimated that the formula information would have cost the company $1 million annually in sales.[241]

the Yuen Foong Paper Manufacturing Company of Taiwan. Jessica Chou, a Taiwan citizen actively involved in the attempted theft, was also indicted. Taiwan publicly stated that it would not help the U.S. extradite Chou for trial in the U.S. If the Taiwan firm had obtained the synthetic Taxol formula, Bristol-Myers Squibb would have lost approximately $200 million a year in revenue from the world market.[92]

(U) *Coal Mining Technology*

(U) In mid-1997, John Fulton, a former employee of Joy Mining Machinery, Inc., and at the time the operator of a Joy competitor, United Mining Cable, approached a Joy employee in an attempt to purchase schematics for part of the coal-shearing system used by Joy. Joy Mining Machinery is a global coal mining company that manufactures and repairs technical components of equipment that mechanically shears coal from the face of an underground coal wall. The Joy employee became a cooperating witness in the case and participated in consensually monitored conversations. Fulton offered to pay any amount of money for information pertaining to the chock interface unit of the coal-shearing technology. In November 1997, Fulton paid the cooperating witness $1,500 for blueprints and a technical binder, both of which were Joy proprietary items. Fulton was arrested by the FBI after the exchange and was charged with unlawfully attempting to obtain trade secrets.[93]

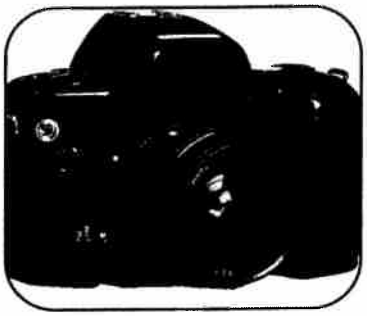
(U) **Through Unwitting Accomplices**

(U) Sometimes collectors of economic intelligence try to brazen their way into opportunities in which they can collect critical information. Another ploy is to create situations in which the employees of a targeted facility can be induced to give their proprietary information away, in the mistaken belief that the individuals requesting the information have been properly authorized to receive it. Examples of this type include the following:

- (U) A Japanese collector called the president of a major U.S. biotechnology firm, knowing the president was out of town. The Japanese businessman assured the secretary he spoke to that the company president had already given his approval for her to provide several sheets of data on a technical compound.

The secretary refused to provide the information, and her boss later confirmed that he had not given authorization for anyone to receive the data. [94]

- (U) A Japanese TV crew requested and obtained permission to visit a U.S. firm to film a documentary on cancer research. While filming the video, the crew asked many questions, collected information, and sought access to sensitive areas. Before long it became apparent the visitors had much more technical understanding of the industry than would be expected from a professional television crew. Company officials had the visitors escorted from the facility.[95]



- (U) Japanese scientific visitors to one facility wandered into restricted areas and began taking pictures. When confronted, they apologized profusely and blamed their lack of English language skills for not being able to read the posted signs denying them access. At later social gatherings, however, the Japanese scientists were observed conversing with their counterparts in fluent English.[96]

- (U) French engineers, with the support of the French Embassy in Washington, misrepresented themselves as customers of Dow Corning and sought to obtain information regarding the coating used in the stealth aircraft to evade radar detection.[97]

- (U) A business education professor from India who taught a night class at a Maryland college required each of her students to write a term paper on the company where they worked. One student advised the FBI that her paper had been returned by the professor three times, with the professor on each occasion asking for more detailed information. Eventually, the professor's interest in the student's company extended to directing her to provide sensitive, possibly proprietary data.[98]

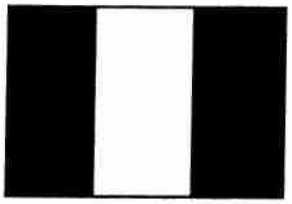
(U) From Foreign Intelligence Services

(U) Intelligence services are, by definition, specialists in the techniques of collecting "secret" information. When they apply their specialized skills against individual commercial targets, they can provide a potent combination of resources and special skills. It has been extensively documented that France has used this approach against the U.S. for many years.

(U) First, the memoirs of Count Alexandre de Marenches, director of France's external intelligence service from 1970-1981, recount that an agent in the U.S. Government provided information about an upcoming currency devaluation that allowed the Bank of France to reap enormous profits in international currency markets. De Marenches's successor, Pierre Marion, admitted in news interviews that he initiated an economic espionage program against U.S. businesses to keep France internationally competitive. Marion mentioned that IBM, Corning Glass, and Texas Instruments had been specific targets of the French intelligence service. Marion explained that, "It would not be normal for us to spy on the United States in political matters or military matters, but in the economic and technical spheres we are competitors; we are not allies." Marion was succeeded by Charles Silberzahn, who also confirmed publicly that economic espionage had replaced political intelligence as a priority for France, and that theft of information about large corporations was a long-term French government policy. In a 1996 interview on a German television program, Silberzahn observed that in France "the state is not just responsible for lawmaking, it is in business as well."[99]

> **"It would not be normal for us to spy on the United States in political matters or military matters, but in the economic and technical spheres we are competitors; we are not allies."**
>
> **Pierre Marion, Former Director of France's Eternal Intelligence Service**

(U) Examples of economic espionage operations against the U.S. directed and controlled by foreign intelligence services or other foreign government entities include the following:



- (U) Beginning in 1969, the French intelligence service recruited several French nationals in the France-based offices of IBM, Corning Glass, and Texas Instruments. These agents were tasked to collect information on marketing plans, product specifications, and travel itineraries of executives. French intelligence passed the information along to competing companies in France, including Machines Bull. In 1993, when Bull sued Texas Instruments over patent infringement on a computer chip, Texas Instruments discovered that Bull had originally stolen the design from them through an agent who worked for Texas Instruments for 13 years. After two years of litigation, the two companies settled out of court, on undisclosed terms.[100]

- (U) In 1973, ranking scientists and managers of the Soviet computer and electronics industries obtained a visa for the specific purpose of visiting the Uranus Liquid Crystal Watch Company of Minneola, Long Island. This was definitely a very odd choice

Well-Dressed Trashmen

(U) In May 1991, a private security guard in an exclusive residential area of Houston, Texas, noticed two well-dressed men tossing into their van plastic bags of garbage taken from behind the home of an executive for a U.S. defense contractor. The guard notified the FBI, and investigation later identified the van as belonging to the French consul general in Houston. When FBI agents quizzed the French diplomat about his actions, he claimed that he had been looking for bags of grass clippings to fill in a hole dug in his back yard.[242]

of destination for such a delegation, but three days before the delegation's arrival the Soviets requested an expansion of the itinerary to include nearly all leading U.S. computer and semiconductor firms. The reason for the abrupt change in plans was that the Soviets had studied U.S. regulations and procedures and discovered that, if they made a last-minute change of itinerary, the U.S. Defense Department would not have time to object. This allowed the delegation to observe the latest critical technology.

- (U) In 1985, a U.S. aerospace company bidding to sell jet fighter aircraft to India lost a $2 billion contract to a French aerospace company after the French intelligence service became aware of the U.S. company's best and final offer during negotiations and then passed the information along to a French competitor.

- (U) In the spring of 1986, Recon Optical was in the midst of a $45 million contract with Israel to manufacture advanced airborne photographic surveillance equipment. The terms of the contract allowed three Israeli Air Force officers to be stationed at Recon to monitor progress of the project. After a lengthy dispute with Israel over the financial terms of the contract, Recon decided to close work down and asked the three Israeli officers to leave. The officers attempted to leave the premises with boxes of Recon data labeled as their personal belongings. These were confiscated, and examination of their contents revealed that the

officers had for months been sending proprietary Recon information to a competitor company back in Israel. Recon sued the government of Israel, and an arbitrator awarded the American company $3 million in damages.[101]

(U) The Insider Threat

(U) Most people visualize espionage as a secret agent managing to sneak into a facility, defeat its guards and locks, and then spirit away secret documents or equipment. In reality, the most common threat comes from an employee inside the facility who approaches an outsider to sell his organization's secrets. Three surveys conducted between 1988 and 1994 by the American Society for Industrial Security determined that approximately 75 percent of all reported incidents of economic espionage were attributable to employees or former employees with access to sensitive information. The figure for losses attributable to vendors, consultants, joint venture partners, and subcontractors was at that time just 15 percent, but by 1999 a similar survey identified on-site contractor employees and original equipment manufacturers as the main source of concern for U.S. companies.[102]

Seventy-five percent of all reported incidents of economic espionage were attributable to employees or former employees with access to sensitive information.

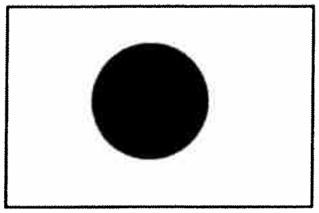
(U) In cases involving national security, between 1975 and 2000 the United States charged 140 individuals with espionage. Of these, 80 were U.S. citizens with a security clearance, 35 were U.S. citizens or resident aliens with no security clearance, and the remaining 25 were foreign nationals. By a more than three-to-one margin, the cases involved one person acting without co-conspirators. In about two thirds of the cases, the arrests were made only after there had been damage to U.S. national security.[103]

(U) Moles and espionage entrepreneurs are two types of insiders who can wreak havoc through economic espionage. These cases are particularly difficult for OPSEC managers, since an insider with access to his organization's critical information would also know the critical needs of competitors or adversaries. Moreover, he is likely to be familiar with his organization's security systems and safeguards and be in a good position to defeat or circumvent them.

(U) Moles

(U) A "mole" is an employee sent by an outside entity to work for a competitor or recruited after he already is inside the targeted organization. The mole tunnels his way into a position of access to the organization's critical information, and then passes the data back to his outside clients.

- (U) From 1977 to 1986, agents operating from the Japanese consulate in San Francisco obtained vast amounts of information from a middle-level researcher at Fairchild Semiconductors,



Inc. The employee provided them computer disks containing as many as 160,000 pages of confidential research results and corporate plans. The Fairchild mole was never conclusively identified and was apparently able to leave Fairchild with enough extra money to retire soon thereafter. Fairchild was so weakened by the mole's efforts that, in 1986, it required government assistance to fight off a Fujitsu Corporation bid to purchase 80 percent of the company.[104]

- (U) In 1981, a French software engineer was convicted on two counts of felony theft involving the intellectual property of his employer, Renaissance Software Systems, Inc. At the time, he was receiving a stipend from the French government for reporting on his work at Renaissance.[105]

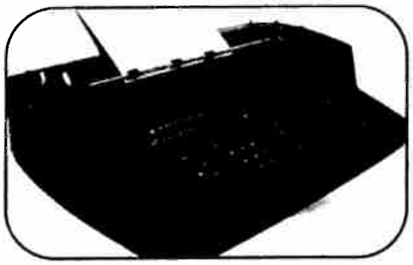
- (U) In 1994, Yao Mindong, a PRC national in a five-month engineer training program at a Motorola Company facility in Albuquerque, New Mexico, made a sudden, unannounced departure from the workplace several days early. Just before his departure, Yao visited the plant's computer facility and printed out some materials to take back with him. Motorola officials had no way of determining what data Yao printed out, but they were concerned because it had taken the company 50 man-years to develop the project Yao had been working on. Motorola valued its potential loss from the incident at $5 million.[106]

Avery-Dennison Case

(U) In September 1997, Dr. Ten Hong Lee, Pin Yen Yang, and his daughter Sally Hwei Chen Yang were arrested for theft of trade secrets from the Avery-Dennison Corporation, Pasadena, California. Four Pillars Enterprises, Ltd, which has offices in Texas and Taiwan, was also charged. Lee, a Taiwan native and U.S. citizen, had been an Avery-Dennison employee since 1986 at the company's Concord, Ohio, facility. Over a period of approximately eight years, he received between $150,000 and $160,000 for providing Four Pillars and the Yangs with secrets about adhesives used in products such as self-stick postage stamps, name labels, diaper tape and battery labels. Both Yangs were fined, and Pin Yen Yang was also sentenced to home confinement. Four Pillars was assessed the maximum statutory fine, $5 million. The estimated damage to Avery-Dennison was $50-60 million.[243]

(U) Espionage Entrepreneurs

(U) An "espionage entrepreneur" is an employee who obtains access to critical information and then tries to use the information as an inducement to a competitor company to hire him for a better job or simply tries to sell his secrets outright to one or more buyers. They are most commonly discovered when an approach is reported by one of the potential buyers of the critical information. Here are some examples of critical intelligence compromised by information entrepreneurs:



(U) *Electronic Typewriter Trade Secrets*

(U) In the summer of 1979, Orion Briel, a disgruntled employee at Exxon's QYX division, resigned his job and sent a letter to a vice president of IBM's Office Products Division, offering to steal proprietary Exxon documents, including designs for new products, research and development plans, and marketing strategies. QYX at the time had captured nearly 25 percent of the computerized typewriter market, a field once dominated by IBM. Briel asked for $100,000. IBM reported the approach to the FBI. The potential loss to Exxon was $500 million.[107]

(U) *Telecommunications Computer Applications*

(U) In 1986, Ronald Hoffman, a U.S. scientist working on space technology computer research for Science Applications International Corporation (SAIC) attempted to persuade SAIC to sell information to Japan developed for the Strategic Defense Initiative but with commercial telecommunications and weather-satellite applications. Japan was years behind the U.S. in this area, but SAIC declined to pursue the matter, since the information was both classified and restricted from export. Hoffman thereupon formed his own research and export company, Plume Technology, as a sideline activity and contacted various Japanese firms to offer his services. Over the next four years, he sold SAIC technology to four Japanese companies. Ronald Hoffman was arrested in 1990 and convicted of selling classified information. No legal action was taken against his Japanese customers, who subsequently gained a significant competitive advantage in the space industry.[108]

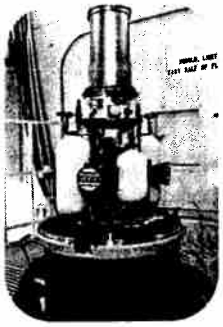
(U) *Genetically Engineered Pharmaceuticals*

(U) In early 1990, a former research scientist with Merck and Company and Schering-Plough Company and an accomplice who ran a research laboratory let it be known that they had some extremely valuable pharmaceutical trade secrets to sell. Their offer was to provide details of the manufacturing process for two genetically engineered pharmaceuticals: Ivermectin, a leading antiparasitic drug with worldwide livestock usage, and Interferon, which is used as an anticancer and antiviral drug. Their offer attracted the attention of the FBI, and later that year both were arrested immediately after selling their critical information on one of the drug fermentation processes to an undercover agent, who paid the two $1.5 million in cash and bonds. The companies involved advised that over $750 million had been spent developing the two drugs. Since there was no Economic Espionage Act at the time, the case was prosecuted under applicable fraud statutes.[109]

(U) *Tomahawk Missile Bid Information*

(U) In 1993, the U.S. Navy decided to have a sole vendor, either Hughes Aircraft or McDonnell-Douglas Missile Systems Company, manufacture its Tomahawk cruise missiles; and this caused an intense competition between the two companies. In November of that year, a former Hughes employee approached a senior manager at McDonnell-Douglas and offered to sell the specifics of the Hughes bid and pricing information for $70,000. The manager alerted the FBI. A month later, the espionage entrepreneur and the current Hughes employee who was the source of his information were arrested by the FBI and the Naval Criminal Investigative Service after they agreed to sell the proprietary information to undercover agents.[110]

(U) *Copier Technology*



(U) In late 1996, Harold Worden, a 28-year employee of Eastman Kodak Corporation, retired and established his own consulting firm. Worden thereupon hired many former Kodak employees and stole a considerable amount of Kodak trade secret and proprietary information that he later attempted to sell to Kodak rivals, including corporations in China. Worden's illegal activities were documented in an investigation using a double-agent operation, and he was arrested and pled guilty. Worden was sentenced to one-year imprisonment and a $30,000 fine.[111]

(U) *Voice-Mail Intelligence*

(U) In November 1996, John Hebel was arrested and charged with wire fraud. Hebel had been employed by Standard Duplicating Machines Corporation as a field sales manager from 1990 to 1992, when he was terminated. Hebel subsequently found employment at the U.S. affiliate of Duplo Manufacturing Corporation of Japan. Through an unsolicited phone call from a customer, Standard discovered that, while employed at Duplo, Hebel had accessed Standard's electronic phone messaging system and used the information to Duplo's benefit to compete against Standard. In March 1997, Hebel was sentenced to two years' probation. In addition, a civil suit was brought against Duplo by Standard, with a final settlement close to $1 million.[112]

(U) *Glass Technology*

(U) In December 1996, Patrick Worthing and his brother, Daniel, were arrested by the FBI, after agreeing to sell PPG Industries (Pittsburgh Plate Glass) information for $1,000 to an FBI special agent posing as a representative of Owens-Corning, a primary PPG competitor. Patrick Worthing had misappropriated diskettes, blueprints and other types of confidential research information from PPG, which he tried to sell to Owens-Corning. However, Owens-Corning alerted PPG, who subsequently informed the FBI that an individual was attempting to sell company trade secrets to representatives of Owens-Corning Corporation.[113]

(U) *Razor Blade Design Information*

(U) In February and March 1997, Steven Louis Davis stole and disclosed trade secrets concerning a new shaving system developed by the Gillette Company. Davis was a process control engineer employed by a subcontractor of Gillette Company. Using several pseudonyms, Davis sent facsimiles and electronic mail containing confidential technical drawings to Gillette's competitors Warner-Lambert Co., Bic, and American Safety Razor Co. Davis, in soliciting further interest, claimed that he had 600 megabytes of Gillette's product drawings, equipment drawings, and assembly drawings relating to Gillette's next generation of razor systems. Davis was arrested in October 1997. Subsequent FBI investigation was not able to establish to what extent he had disseminated trade secrets overseas. After pleading guilty, he was sentenced to two years and three months in Federal prison and $1.2 million in restitution.[114]

(U) *Computer source code*

(U) In a recent case, Cadence Design Systems, Inc., was attempting to recover $1.2 billion from former employees alleged to have stolen intellectual property to build up the product line of a competitor. Evidence collected during the execution of a search warrant included electronic footprints which show that one employee E-mailed six megabytes of computer source code to a private account before quitting Cadence and joining the rival company. Before long, the competitor company began marketing a product similar to Cadence's, and theirs contained the same source code, including the same typographical errors as in the Cadence product. In the words of a senior vice president of Cadence, "That source code is the central nervous system for every other product and service we put out. It took hundreds and hundreds of engineering hours and years to develop." A criminal case is pending against the rival company.[115]

(U) Developing a Countermeasures Strategy

(U) One of the problems that U.S. companies who have been the victims of economic espionage face is that they often feel constrained to keep their losses secret. In fact, the General Accounting Office-the investigative arm of the U.S. Congress-had to abandon its plan to study the extent and impact of foreign government spying on U.S. companies when it became clear that firms had little desire to discuss the matter.

(U) U.S. firms have been reluctant to speak out about their experiences with economic espionage for a number of practical reasons. For one thing, if a firm makes its loss known, it may suffer public embarrassment and become known as a company that can't keep its secrets. Some companies that have reported successful attacks on their critical information have seen their stock prices drop, their employee morale plummet, and their corporate partners pull out of deals for fear their own critical information may be compromised. Also, when the economic espionage has come from a foreign country, the U.S. company that names names runs the additional risk of losing future contracts there. Finally, criminal and civil penalties imposed on individuals and organizations engaged in economic espionage are small compared to the potentially huge gains possible.

(U) The case of Recon Optical is an instructive example of some of the problems that U.S. companies can face, even after they have "successfully" fended off an economic espionage operation. Although Recon was awarded a reported $3 million by an arbitration panel, the figure did not cover the company's legal expenses in waging a four-year lawsuit against Israel. The Israeli contract had been the company's largest, and its management was tied down in the legal process. The action depleted all the company's cash, and when it tried to bid for contracts in two huge new Pentagon reconnaissance programs, its prices had to reflect its low cash reserves and thus could be beat by competitors. The company's sales dropped 40 percent, and it was forced to lay off 800 of its 1,100-member workforce. Only the emergency military needs of the Gulf War kept Recon Optical from going under completely.[116]

Recon's sales dropped 40 percent, and it was forced to lay off 800 of its 1,100-member workforce.

(U) Economic Espionage Indicators

(U) Given the realities that U.S. organizations face, many may try to handle OPSEC requirements without outside assistance. The following is a partial list and discussion of indicators that a given company may be under economic espionage attack.

(U) Outsider Threat Indicators

(U) *Unsolicited requests for information*

(U) Such requests frequently involve faxing, mailing, E-mailing, or phoning to individuals rather than corporate marketing departments. The requests may involve surveys or questionnaires and are frequently sent over the Internet. Marketing surveys can elicit sensitive technological and business information. With this method, it is important to consider who is the end user of the information and who is completing the survey. Increasing use of the Internet provides a method of bypassing organizational security systems for collection purposes. Internet access to a company's bulletin board, homepage, and employees provides a collector many avenues to broaden collection efforts. Additional indicators include communications in which the recipient has never met the sender; the requestor identifies himself as a consultant or student; the requestor insinuates the company he works for is "classified;" and the requester advises the recipient not to worry about security concerns.[117]

(U) *Inappropriate Conduct During Visit*

(U) Visitors are an obvious vector for loss of critical information. One economic espionage indicator is an attempt to arrange an alternative mechanism such as proposing a commercial visit shortly after an official visit has been denied by the host organization. Another situation involves foreign visitors accompanied by a diplomat who attempts to conceal the visitors' identities or official positions during the visit. Yet another is the existence of hidden agendas: the visitors arrive to discuss program "X" but do everything to discuss and meet with personnel who work with program "Y." Last-minute and unannounced persons being added to the visiting party is also a reason for heightened concern. The questions asked by the visitors also may be an indicator of an economic espionage interest on their part, especially if they ask them during a briefing outside the scope of the approved visit, hoping to get a courteous or spontaneous response.[118]

(U) *Suspicious Work Offers*

(U) Sometimes foreign scientists and engineers will offer their services to research facilities, academic institutions, and defense contractors. This may be an attempt to place a foreign national inside the facility as a "mole" to collect on a desired technology. There are further reasons for concern if the foreign applicant has a scientific background in a specialty for which his country has been identified as having a collection requirement, if the technology the prospective employee wants to work with is proprietary or export-controlled, if the applicant's salary and expenses are to be paid by a foreign government or a corporation associated with the government, or if the prospective employee offers to work under a knowledgeable individual for a lengthy time for free. Another tactic is for one side to overstaff a joint-venture operation, using its excess employees to gather loose information from their business partners.[119]

(U) *Invitations to International Exhibitions, Conventions, and Seminars*

(U) It is not necessary for critical information collectors to devise ways to get into a

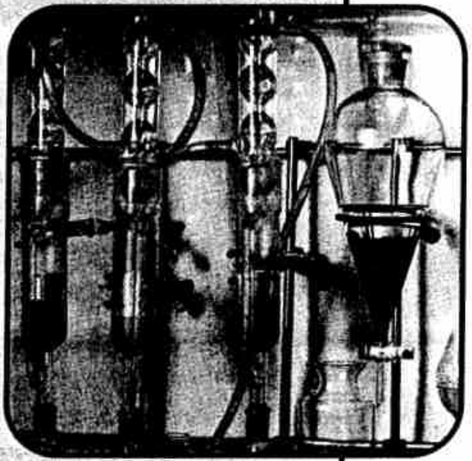
(U//FOUO) Here are the steps a security consultant recently used to compromise the current research projects of a large chemicals company.

1. (U//FOUO) The consultant used the Internet and newspaper files to familiarize himself with news reports of current projects and with past incidents of "industrial espionage" against the company. He wanted to find out what had worked and what had not.

2. (U//FOUO) Hired as a temporary employee in a low-level position, the insider went to a nearby restaurant that had a fishbowl with business cards in it for a weekly free lunch drawing and fished out a company card. He had a local print shop duplicate the card in his name, with the title, "Supervisor of Information Security."

3. (U//FOUO) Noting that the company used a passcard for some computer systems, the employee forged his supervisor's name to a memo ordering a special access card for himself in his assumed information-security role.

4. (U//FOUO) The insider called on a senior researcher on one of the projects he had read about in the newspaper and gave her his new business card. He interviewed the researcher about what information in the project could be considered sensitive and asked for suggestions on how to improve security. The researcher suggested he contact the team leader, which he did, mentioning the referral from the researcher. The team leader identified the portion of the project considered most valuable and gave the insider the names of all the people working on the project, so he could interview them about data-storage security. Using the same technique, the insider interviewed several other employees until he found one who admitted he had not backed up his key files. Under the guise of "walking through" the backup process with the employee, the insider had the employee mark his files as "shared." Later he downloaded the files from his own office computer.



5. (U//FOUO) Looking for a critical document on the project, the insider accessed an unprotected computer file with research meeting minutes on it. One document identified the location of the document and the User ID and password needed to open it. Using the same password, the insider accessed several other summary documents with details of two other critical projects the company was working on.

(U//FOUO) Had he chosen to, the security consultant could have left at the end of the day and not returned. He had compromised three projects of potential multi-million dollar value to the company's competitors.[245]

U.S. facility if they can induce the facility to send its knowledgeable staff members to locations and situations where there is little or no protection for them. This is a particular OPSEC problem for organizations in which foreign travel is highly prized by staff members. If the invitation is to send representatives for a specific topic, whom the organization selects to attend may itself identify future targets for foreign collectors and economic competitors. Indicators that economic espionage may be involved in such situations are: if the organizing country or organization has tried unsuccessfully to visit the invited facility, if the travel or accommodations are offered expense-paid, if a summary of the conference speaking topic is requested far in advance of the foreign meeting, if attendees wear false or incomplete conference name tags, or if there is excessive or suspicious filming or photography at the conference.[120]

(U) *Proposals for Joint Ventures or Joint Research Projects*

(U) It is not necessary for a foreign collector or an economic competitor to steal critical intelligence from an organization if the organization can be persuaded to give the information away. Proposals for mutually profitable cooperative enterprises are one means of collecting critical information that would otherwise be difficult to obtain. Requests for unrestricted access to the organization's local area network or its physical plant may be indicators of economic espionage. Sometimes companies are induced to provide large amounts of technical data as part of the bidding process, only to have the contract canceled, or the proposed technology sharing agreements may be one-sided. Other indicators of the impending loss of critical information are the venture partner's sending more people than necessary to staff the project, or the venture partner's staff members singling out individual employees to provide information outside the scope of the agreement.[121]

(U) Insider Threat Indicators

(U) *Hiring Ex-Employees*

(U) An ex-employee who now works for a competitor can be a good source of critical company intelligence for the competitor, not just because of the intellectual property the ex-employee may already know, but also because of the ex-employee's ability to find out recent information. In this regard, it can be critical to keep track of which former employees now work for competitor companies and which former employees still maintain social or professional contact with current staff members. Of particular concern is the employee who has a job history of alternating working between one company and one of its competitors.[122]

(U) *Foreign Ethnic Targeting of Employees*

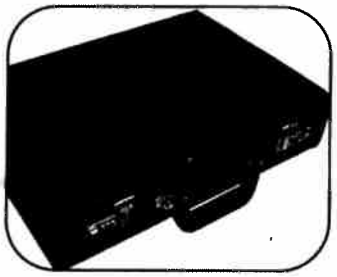
(U//FOUO) Sometimes, foreign countries and their commercial entities attempt to exploit cultural ties with company employees to exploit them for collection of critical information. Sometimes, an employee will receive unsolicited mailings or greeting cards from foreign embassy personnel. In other cases, an employee may be invited to travel to the country of his ancestry to give a lecture or receive an award. This may be an especially ominous development if the travel is also to be expense-paid. Alternatively, foreign delegations may arrive without an interpreter and ask the company to provide an employee who speaks their language. The visitors may then single out the employee for extra socializing and may invite him to pay a reciprocal visit to their country.[123]

(U) *A "Too-Good" Employee*

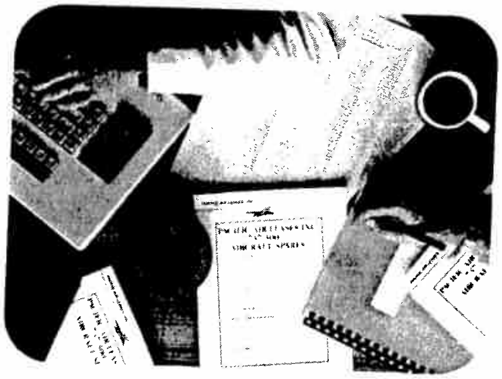
(U) Sometimes individual characteristics that are most valued in an employee may, taken together, give reason to fear possible economic espionage from him. These indicators include extra initiative, such as volunteering for special work or project assignments offering different or higher access; repeatedly volunteering to work nights or weekends, especially when few other employees are present; refusing promotion to a higher-paying job with less access to proprietary information; etc.

(U) **Work Assignments and Access Indicators**

- (U) Any attempt to obtain classified, sensitive, or trade secret information without a genuine "need to know" that information
- (U) Unauthorized removal of classified, sensitive, or trade secret information from a work area
- (U) Placing classified, sensitive, or trade secret information in desks or briefcases for no apparent reason
- (U) Unusual use of, requests for, classified, sensitive, or trade secret information
- (U) Using a copier machine in other offices to reproduce classified, sensitive, or trade secret information when a copier machine is available in that person's office



- (U) Repeated or unusual or unnecessary overtime
- (U) Sudden deterioration in work performance or a change in attitude of a person with access to classified, sensitive, or trade secret information
- (U) Borrowing or making notes of classified, sensitive, or trade secret information not associated with assigned work
- (U) Attempting to obtain witness signatures on a classified or sensitive



document destruction form where the destruction was not actually observed by the witness

- (U) Bringing a camera or recording device into an area where classified, sensitive, or trade secret information is used, especially new cellular phones with digital imaging and transmission capability
- (U) Excessive unauthorized use of a classified or sensitive computer system at work.[131]

(U) Financial Indicators

- (U) Sudden purchase of high-value items such as real estate, automobiles or vacations for which no logical source of income exists
- (U) Flashing of expensive purchases or large sums of cash, especially after returning from leave
- (U) Extensive or regular gambling losses or financial indebtedness
- (U) Sudden repayment of large loans
- (U) Purchase of expensive miniature cameras and related equipment
- (U) Purchase of quality international or ham radio-band communications equipment by other than a known hobbyist[124]

(U) Leave and Travel Indicators

- (U) Short domestic or overseas trips for no apparent purpose

- (U) Recurring or quick weekend trips not associated with recreation or family
- (U) Trips that cost out of proportion to the short time spent at the locations
- (U) Upon return, the traveler has a hard time describing the location visited
- (U) Personal or family travel to current or former Communist countries

- (U) Inquiries about passport or visa requirements for current or former Communist countries
- (U) Travel on current or former Communist Bloc aircraft or cruise liners
- (U) Mention of problems with border-crossing, visa or police in former or current Communist countries[125]

(U) Social and Family Indicators

- (U) Relatives or friends live in or maintain connections to current or former Communist countries
- (U) Relatives or friends visit from current or former Communist countries
- (U) Relatives or friends in current or former Communist countries request assistance
- (U) Use of illegal drugs[126]

(U) Computers and the Internet

(U) Background

(U) Advances in telecommunications and in computer technology have caused an information revolution in the United States and worldwide, the impact of which may be as profound as that of the industrial revolution of the 19th century. Developments such as fiber optic cable have occurred when computer processor speeds have doubled and redoubled and computer memory has trebled and sextupled. A seemingly instantaneous evolution of telephone, cable, satellite and computer networks and software, combined with technological breakthroughs in computer processing have made this latest revolution possible.

[redacted]

(U) Apart from the rapid evolution of personal computers (PCs), the computing environment today allows for a sophisticated and complex interconnection of PCs, networks and hosts. Many organizations now have PCs connected to different networks with the additional capability of accessing a mainframe. Laptops and notebook computers add to the risk factor by providing the ability to easily remove sensitive information from the workplace. The loss of sensitive information, whether deliberate or inadvertent, can carry a price tag far beyond the cost of platform hardware.

(U) Since networks of computers allow users to share vast amounts of data very efficiently, networked computer environments are used every day by the majority of corporations and organizations. Corporate networks are not always designed and implemented with security in mind, merely functionality and efficiency. Although this is good from a business standpoint in the short-term, security problems arise later, which cost millions to solve in larger environments.

(U) The most obvious example of both the prevalence and power of computer networking today is the Internet. The Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways, including gateways, routers, dial-up connections, and Internet service providers. The Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day.

Corporate networks are not always designed and implemented with security in mind, merely functionality and efficiency.

(U) The only equipment required for Internet access is a computer with a modem and a telephone line, and even these requirements are being superseded by services that offer high-speed connection through cable TV lines or directly through a combination computer-television set. As more people get connected, the attractiveness of the Internet as a convenient, cheap, quick and intriguing way of communicating increases. With more participants, the amount of available information (news groups, program and data files, graphic and multimedia documents, and government and industry documents) increases and attracts even more users.

(U) The Internet strives to be a seamless web of networks; therefore, it is often impossible to distinguish where one network ends and another begins. Local, state, and Federal government networks are connected to commercial networks, which in turn are connected to military networks, financial networks, utilities networks, etc.

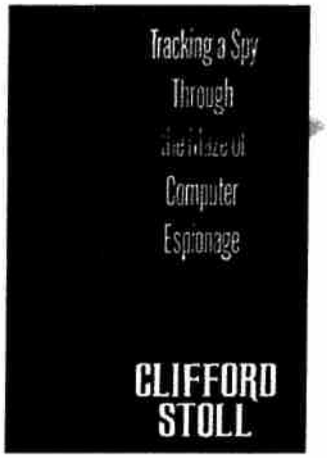
(U) History of Internet Security

(U) The Internet began in 1969 as the ARPANET, a project funded by the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. One of the original goals of the project was to create a network that would continue to function even if major sections of the network failed or were attacked. The ARPANET was designed to reroute network traffic automatically around problems in connecting systems or in passing along the necessary information to keep the network functioning.[127]

(U) As more sites joined the ARPANET, the usefulness of the network grew. The ARPANET consisted primarily of university and government computers, and the applications supported on this network were simple: electronic mail (E-mail); electronic news groups; and remote connection to other computers. By 1971, the Internet linked about two dozen research and government sites, and researchers began to use it to exchange information not directly related to the ARPANET itself. The network was becoming an important tool for collaborative research.[128]

(U) The ARPANET protocols (the rules of syntax that enable computers to communicate on a network) were originally designed for openness and flexibility, not for security. The ARPA researchers needed to share information easily, so everyone needed to be an unrestricted "insider" on the network. During these years, researchers also played "practical jokes" on each other, using the ARPANET. These jokes usually involved humorous messages, annoying messages, and other minor security violations. It was rare that a connection from a remote system was considered an attack, however, because ARPANET users comprised a small group of people who generally knew and trusted each other.[129]

(U) In 1986, the first well-publicized international computer-network security incident was identified. A university scientist noticed a simple accounting error in the computer records of systems connected to the ARPANET, and this discrepancy led him to uncover an international effort, using the network, to connect to computers in the United States and copy information from them. These U.S. computers were not only at universities, but at military and government sites all over the country. This incident raised awareness that the ARPANET could also be used for destructive purposes.[130]



(U) In 1988, the ARPANET had its first automated network security incident. A student at Cornell University, Robert T. Morris, wrote a program, now called a "worm," that would connect to another computer, find and use one of several vulnerabilities to copy itself to that second computer, and begin to run the copy of itself at the new location. Both the original code and the copy would then repeat these actions in an infinite loop to other computers on the ARPANET. This "self-replicating automated network attack tool" caused a geometric explosion of copies to be started at computers all around the ARPANET. The worm used so many system resources that the attacked computers could no longer function. As a result, 10% of the U.S. computers connected to the ARPANET effectively stopped at about the same time.[131]

(U) By that time, the ARPANET had grown to more than 88,000 computers and was the primary means of communication among network security experts. With the ARPANET effectively down, it was difficult to coordinate a response to the worm. Many sites removed themselves from the ARPANET altogether, further hampering communication and the transmission of the solution that would stop Morris's worm.[132]

(U) The Morris worm prompted the Defense Advanced Research Projects Agency (DARPA, the new name for ARPA) to fund a computer emergency response team, now the CERT Coordination Center at Carnegie-Mellon University, to give experts a central point for coordinating responses to network emergencies. Other teams quickly sprang up to address computer security incidents in specific organizations or geographic regions. Within a year of their formation, these incident response teams created an informal organization now known as the Forum of Incident Response and Security Teams (FIRST). These teams and the FIRST organization exist to coordinate responses to computer security incidents, assist sites in handling attacks, and educate network users about computer security threats and preventive practices.[133]

(U) In 1989, the ARPANET officially became the Internet and moved from a government research project to an operational network; by then it had grown to more than 100,000 computers. Security problems continued, with both aggressive and defensive technologies becoming more sophisticated. Among the major security incidents were the 1989 WANK/OILZ worm, an automated attack on one type of system attached to the Internet, and exploitation of vulnerabilities in widely distributed programs such as the "sendmail" program, a complicated set of instructions commonly used for sending and receiving electronic mail.[134]

(U) In 1994, intruder tools were created to "sniff" packets from the network easily, resulting in the widespread disclosure of user names and password information. A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text.[135]

(U) In 1995, the method that Internet computers use to name and authenticate each other was exploited by a new set of attack tools that allowed widespread Internet attacks on computers that have "trust relationships" with any other computer, even one in the same room. Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.[136]

(U) Although the Internet was originally conceived of and designed as a research and education network, usage patterns have radically changed. The Internet has become a home for private and commercial communication, and it is still expanding into important areas of commerce, medicine, and public service. Increased reliance on the Internet is expected over the next five years, along with increased attention to its security.[137]

(U) Threats to Computer Network Security

(U) Three basic security concepts important to information on computer networks are confidentiality, integrity, and availability. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality.

Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need.[138]

(U) Concepts relating to the people who use network information are authentication, authorization, and nonrepudiation. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication is proving that a user is who he or she claims to be. That proof may involve something the user knows, such as a password; something the user has, such as an electronic passcard; or something about the user that proves his identity, such as a fingerprint. Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is considered to be strong when the means of authentication cannot later be refuted – the user cannot later deny that he or she performed the activity. This is known as nonrepudiation.[139]

(U) Just as with other types of threats, it is useful for OPSEC managers to conceptualize computer network security in terms of the risk of loss of critical information or other damage caused by outsiders versus the risks posed by the actions of insiders. While the potential for attack may come from a variety and potentially large number of individuals, computer attacks themselves tend, just like other areas of OPSEC concern, to use a relatively small number of methodologies to compromise the organization's security systems.[140]

(U) Website Content and OPSEC

(U) It is not necessary for an intelligence adversary, a terrorist, an economic competitor, a mischief-maker, or any other potential security threat to an organization to devise novel and clever methods to steal the organization's critical information, if that information is already being given away on the organization's website or a series of sites. While the World Wide Web provides any organization a new and powerful tool for conveying information quickly and efficiently on a broad range of topics, it also increases the risk to the organization. The particular problem posed by today's technology is that Internet connectivity provides a single user with new levels of understanding from unclassified sources.[141]

(U) While analysts have always employed "data mining" techniques to collect small pieces of information from a number of different sources and compile them into a product which contains critical information, it was hard for them to produce a timely product. Their problem was that the sources of information they required might be very widely scattered, and gaining physical access to them imposed real constraints on the process. With today's interconnected networks, however, geography is no longer a factor in information retrieval. Time is now the most critical factor, but increasingly sophisticated computer search engines and information compilation algorithms have automated many steps in the research process and vastly reduced the time necessary to collect comprehensive amounts of information.[142]

Information posted on the organization's website may pose more risk than information about the organization available through other means.

(U) For OPSEC managers, this means that information posted on the organization's website may pose more risk than information about the organization available through other means. For example, one website might identify the officers of a given military unit, and a page on the site might provide names of immediate family members. Using this information, an analyst might be able to locate another website that provides support and advice to military families. Noting the type of support offered, in particular anything under a "what's new" banner, an analyst might be able to derive indicators that the unit will deploy in the near future or indicators of where the unit will deploy. Both of these items of intelligence might be considered critical to the unit's ability to carry out its mission. Using conventional information-gathering techniques, it might take days or even weeks to gather such information; on the Internet, it could take only hours—or even minutes.

(U) Because of the increased risk that someone will be able to make a coherent mosaic of small pieces of information, small items of information posted on a publicly available website are of increased OPSEC significance. Further, it may be possible for an intelligence adversary, or other collector, to put together a public item from one site, and an item from an unrelated site, and derive critical information from the combination. An OPSEC manager, can no longer simply review the organization's website for items that may be targets for an adversary, since there is no sure way of specifically identifying which items in conjunction with information from other sites or sources may become a critical indicator.

(U) The OPSEC solution to this apparent security dilemma is to adopt a zero-based approach to website content. Decide which items, combined with other information, would be critical to an outside collector. Use OPSEC procedures to determine what information is necessary to post on websites to fulfill the mission. These are the most important considerations in zero-based website security:

- (U) **Assess the benefits to be gained by posting specific types of information on a website.** Identify a target audience for each type of information and why their need for the information is important to the organization's mission. A careful examination of the potential consequences of placing information on the website is necessary.[143]

- (U) **Post only information for which the organization is responsible.** Since any organization knows its own critical information best, it can reduce the vulnerability of other organizations by letting them post their own information.[144]

- (U) **Do not post public links to more sensitive sites.** These links identify the existence and location of potential targets for a collector who may previously been unaware of them. If it is necessary to link to other sites, the link should pass through an intermediate site, which can screen visitors through passwords or other criteria.[145]

(U) Roots of Network Vulnerability

(U) Many early network protocols that now form part of the Internet infrastructure were not designed with security in mind. Without a fundamentally secure infrastructure, network defense becomes more difficult. Furthermore, the Internet is an extremely dynamic environment. Its software changes constantly, and this makes it difficult for security systems to catch up with current and newly discovered security holes.[146]

(U) Because of the inherent openness of the Internet, and the original design of its protocols, Internet attacks are quick, easy, inexpensive, and may be hard to detect or trace. An attacker does not have to be physically present to carry out the attack. Many attacks can be launched readily from anywhere in the world—and the location of the attacker can easily be hidden. It is not always necessary to "break in" to a site (i.e., gain privileges on it) to compromise the confidentiality, integrity, or availability of its information or service.[147]

(U) Many sites place unwarranted trust in the Internet. It is common for operators of sites to be unaware of the risks or unconcerned about the amount of trust they place in the Internet. They may not be aware of what can happen to their information and systems. They may believe that their site will not be a target or that precautions they have taken are sufficient. The technology is constantly changing and intruders are constantly developing new tools and techniques, therefore solutions do not remain effective indefinitely.[148]

(U) Since much of the traffic on the Internet is not encrypted, confidentiality and integrity are difficult to achieve. This situation undermines not only applications (such as financial applications that are network-based) but also more fundamental mechanisms such as authentication and nonrepudiation. As a result, sites may be affected by a security compromise at another site over which they have no control. An example of this is a packet sniffer that is installed at one site but allows the intruder to gather information about other sites, possibly in other countries.[149]

(U) Another factor that contributes to the vulnerability of the Internet is the rapid growth and use of the network, accompanied by rapid deployment of network services involving complex applications. Often, these services are not designed, configured, or maintained securely. In the rush to get new products to market, developers do not adequately ensure that they do not repeat previous mistakes or introduce new vulnerabilities.[150]

Operating system security is rarely a purchase criterion.

(U) Compounding the problem is that operating system security is rarely a purchase criterion. Commercial operating system vendors often report that sales are driven by customer demand for performance, price, ease of use, maintenance, and support. As a result, off-the-shelf operating systems are shipped in an easy-to-use but insecure configuration that allows sites to use the system soon after installation. These hosts/sites are often not fully configured from a security perspective before connecting. This lack of secure configuration makes them vulnerable to attacks, which sometimes occur within minutes of connection.[151]

(U) Finally, the explosive growth of the Internet has expanded the need for well-trained and experienced people to engineer and manage the network in a secure manner. Because the need for network security experts far exceeds the supply, inexperienced people are called upon to secure systems, opening still more windows of opportunity for the intruder community.[152]

(U) Outsider Attack Techniques

(U) The typical outsider threatening the computer security of an organization with critical information in its network is a computer "hacker." Once used as a slang term for a computer enthusiast, "hacker" is now largely used to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing or corrupting data. A typical hacker is male, between 16 and 25 years old. Hackers usually become interested in breaking into machines and networks in order to improve their computer skills, or to use network resources for their own purposes. Most hackers are quite persistent in their attacks, possibly because of the amount of spare time the average hacker has.[153]

(U) In addition, there are as many as 1,000 professional hackers worldwide. According to the managing director of the Centre for Infrastructural Warfare Studies, "These are people with hard-core skills. They know exactly what they're doing .... these are highly trained professionals and are way out of the age bracket of the teenage hacker. These people are very difficult to stop. They'll come at you in 10 different ways, not just trying to get through a firewall. They'll steal a password, they'll put 'honey pots' [i.e., very attractive sub-sites] out there to trap passwords, they'll do anything."[154]

(U) A typical hacker attack pattern consists of gaining access to a network user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites or areas of the network. It is possible to accomplish all these steps manually in as little as 45 seconds; with automated software hacking tools, the time can decrease further.[155] Hackers tend to use the following ways to penetrate or damage an organization's computer network:

- (U) **Probing:** A probe is a search initiated at a remote site with the intent of determining potential weaknesses in systems for later exploitation. They are characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry.[156]

- (U) **Scanning:** A scan is simply a large number of probes done using an automated tool. Such tools are available for download at hacker websites on the Internet. Scanning is often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.[157]

[redacted]

- (U) **Compromising an account:** An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving privileges a system administrator or network manager has. An account compromise might expose the victim to serious data loss, data theft, or theft of services. The damage can usually be contained, but a user-level account is often an entry point for greater access to the system.[158]

- (U) **Compromising a root directory:** A root compromise is similar to an account compromise, except a compromised account has special privileges on the system. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs, change how the system works, and hide traces of their intrusion.[159]

- (U) **Packet sniffing:** A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise.[160]

- (U) **Launching a denial-of-service attack:** The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume all of the channels used to connect with the targeted site. Sometimes an attack is used in conjunction with an intrusion attempt. For example, a denial-of-service attack may be launched against a website, effectively shutting it down or keeping it too busy to communicate with other sites. While the first site is busy defending itself, the hacker sends a message to another site, misrepresenting it as a communication from the disabled site, which may be fully trusted by the other site. The hacker uses this trust to penetrate the targeted site.[161]

The cost of security measures to protect against network weaknesses is normally a small fraction of the cost of having to handle a successful outside attack against an organization.

- (U) **Exploiting Trust:** Computers on networks often have "trust relationships" with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.[162]

- (U) **Malicious Code:** Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Trojan horses are programs that hide inside other programs and then execute commands, like ordering a copy of all passwords typed in by the user to be copied stored in a new directory. Viruses are self-replicating programs usually designed to become a nuisance by replicating themselves endlessly until they crowd all available memory out. They usually require action on the part of the user to spread inadvertently to other programs or systems, normally inserting an "infected" diskette into an uninfected machine. Worms are self-replicating programs that are constructed with a built-in strategy to spread themselves to other computers with no human intervention after they are started. These programs can lead to serious data loss, downtime, denial of service, and other security incidents.[163]

(U)The Outsider Target: Network Weaknesses

(U) Most network security incidents exploited by attackers from the outside are made possible by a relatively small number of problems. Most problems can be prevented if adequate defenses are established against these weaknesses. The cost of security measures to protect against network weaknesses is normally a small fraction of the cost of having to handle a successful outside attack against an organization. The following weaknesses are the perennial targets of outside attack:

- (U) **Easy network passwords.** Passwords are the single most important weakness in computer network security. Doing everything else correctly is almost of no value if password security is low. The biggest such problem is an account where the username is the same as the password. This makes the password both easy to remember and easy to guess. The most common occurrences of this problem is the initial password that the system administrators set for an account, with the expectation the user will change it promptly. Often enough, the user doesn't know how to change it or never logs in at all.[164]

- (U) **Duplicate passwords on different machines.** Many years ago, it was reasonable to request that a person to use a different password on each machine or set of machines. With a modern workstation environment, however, it is no longer practical to expect this from a user, and a user is unlikely to comply if asked. At a minimum, users with computer access at another facility should use a different password for their accounts on machines at those facilities. Otherwise, a compromise of a computer at a remote facility could compromise all the computer systems the user has access to. The worst offenders of the "shared password problem" are network maintenance people and teams. Often they want an account on every local area net that they service, each with the same password. That way they can examine network problems and such without having to look up hundreds of passwords.[165]

- (U) **Readable password files.** A readable password file is an accident waiting to happen. It is vital to prevent any user from making and removing a copy of the organization's password file, and it is important to make it as difficult as possible for a user to see the encrypted version of his individual password. A related password problem can arise if there is a game or other lower-level computer application on the network that identifies and stores the records for individual users by allowing them to choose their own passwords. Usually applications do not encrypt the user's password, and there will always be some people who choose their network password as their game password.[166]

- (U) **Old password files.** When a system is backed up or upgraded, several copies of the password file may be created and left in a completely readable state in a forgotten corner of the storage system. Looking for these files is a favorite technique of any hacker who manages to get past the outermost layer of system security.[167]

- (U) **Managers.** Managers, center directors, and other respected people are often given privileged accounts on a variety of machines. They are given these privileges as a sign of respect. Unfortunately, they often are not as familiar with the systems as the programmers and system maintainers themselves. As a result, they often are the targets of attack. Often they are so busy, they do not take the security precautions that others would, and do not have the same level of technical knowledge. They often ignore instructions to change passwords or file protections. Managers should have separate privileged accounts and normal user accounts, with a different password for each.[168]

- (U) **Secretaries to managers.** Managers are often so busy or out of the office so frequently that they reveal their passwords to their secretaries, who may make an electronic note of it and inadvertently leave it within easy electronic reach of a hacker. The risk involved can escalate when the manager has a single password that gives him special user privileges.[169]

- (U) **System administrators.** System programmers often add their own security problems. They sometimes create privileged programs that are needed and then forgotten about without being disabled. To make the situation worse, their files and user accounts sometimes are excluded from security audits because they are thought to know better than to create computer security vulnerabilities.[170]

- (U) **Demonstrators.** The one case where it is especially important to have separate accounts or passwords for a single individual is for an employee who travels to give demonstrations. Such an employee may inadvertently reveal his password if he experiences equipment failure while on the road.[171]

- (U) **Well-known security holes.** There are a very small number of security holes in most large systems that are exploited by hackers over and over. Hacker websites publish information about such entry points, and security manager websites in turn post patches and upgrades that patch the holes.[172]

(U) Examples of Attacks by Hackers

(U) In September 1996, Russian hackers apparently succeeded in siphoning about $10 million into foreign bank accounts, but bungled their attempts to extract cash from these electronic, fraudulent deposits. All but $400,000 of the stolen funds was recovered.[173]

(U) In February 2000, the FBI reportedly was investigating a total of 17 distributed denial of service intrusions. The number of reported attacks had quadrupled from the beginning of the month. Four investigations centered on the placing of denial of service tools, known as daemons, on ambushed computers that were later remotely ordered to attack a victim site. Planting daemons on unwitting host computers is a

(U) In March 1997, a juvenile computer hacker disabled a Worcester, Massachusetts, airport control tower and other airport facilities for six hours and disrupted phone service in a neighboring town. The juvenile also hacked into a Worcester pharmacy computer and stole prescription details from a local pharmacist. Both attacks occurred after computer systems were made accessible through the Internet so that system administrators could work remotely.[244]

key step in mounting such an attack. The tools to accomplish these attacks can be downloaded free from Internet websites.[174]

(U) Insider Attack Techniques

(U) For most organizations, the major threat to computers remains internal. Not only is there the possibility that a disgruntled employee will attempt to disrupt the organization's computer files for malice or steal information for personal gain, there is also the possibility that a skilled outsider employed by a competitor may gain employment with the organization and thus become an insider. Inside access, even if as a temporary employee, puts such a person in position to supplement his computer network hacking with HUMINT operations, called "social engineering" by some.

Employees will at times take some actions or fail to take others and will make an otherwise secure system suddenly completely vulnerable.

(U) It is axiomatic that in technical systems humans usually are the weakest link. From an OPSEC standpoint, employees will at times take some actions or fail to take others and will make an otherwise secure system suddenly completely vulnerable. For example, sometimes employees will unwittingly facilitate a hacker's efforts by using their organization's Internet portal to visit freeware sites and download games or screen savers. Some of these programs contain Trojan-horse programs that will become active every time the infected machine is booted up and will perform actions to facilitate the covert entry of the hacker. A Trojan-horse program hidden inside a game downloaded from a user's favorite newsgroup might contain instructions to E-mail all the user's files anywhere in the world.[175]

(U) Countermeasures

(U) A high percentage of computer hackers are opportunists. They tend to operate on either the Internet or on telephone networks. Because they do not have many resources, they tend to bypass organizations that have even a low level of rigorously-enforced security in favor of attacking targets that are "softer."[176]

(U) Web servers are not usually attacked by hackers who want to break through into corporate records systems, unless the "firewall,"—the collection of hardware and software designed to examine a stream of network traffic and service requests—between the systems has been improperly configured. Hackers instead prefer to attack corporate mail servers, which must have access to Internet mail servers in order to deliver mail properly to the corporate clients. Instead of looking for a possible hole in the firewall, they try to widen and exploit existing paths in the mail servers.[177]

(U) Most hacker probes and scans occur during evening hours, when the outsider is more certain to be able to operate without worrying about the presence of systems administrators. Hackers tend to have most of their spare time on the weekends, and their intrusion attacks are usually made then.[178]

(U) While there is not much that the OPSEC manager can do on her own to protect her computer system from extremely technical attacks, there are many things that she can do to protect her network from an attack that is based on HUMINT security lapses or on a combination of computer hacking and "social engineering."

(U) OPSEC managers and personnel can take the following steps to help reduce the risk of damage to their organizations through computer security incidents:

- (U) **Secure all access points between an internal network and the outside world.** Hackers will find and attack the weakest and most easily exploitable point of a network. Usually this is the initial point of contact within the company, its computer network. One way to prevent corporate information from "leaking out" is to ensure that Internet terminals are completely separated from the company's other computer systems. Without a direct link to the company's operating systems, a potential hacker will only get into the company's Internet computer and not its core computer system. When risk is assessed as too high, the only safe connection to the Internet is none at all.[179]

- (U) **Develop a security policy for each system.** Users must know what is allowed and what is not, which applications may be run and which not, and who is allowed access and who is not. The basis for this should be an OPSEC risk analysis that identifies the organization's assets, the threats that exist against those assets, and the costs of asset loss. This policy should also cover contingencies such as guidelines for reacting to a site compromise (e.g., how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system).[180]

Hackers will find and attack the weakest and most easily exploitable point of a network.

- (U) **Ensure all user accounts have a password.** Also, the passwords should not be easy to guess. There is software available to analyze the security of a network's passwords.[181]

- (U) **Regularly check the integrity of system software.** There are a number of software tools available at Internet computer security websites with the latest version of system-integrity analysis programs. OPSEC managers should also check security archives periodically for security alerts and technical advice.[182]

- (U) **Keep network systems up to date with upgrades and patches.** Each major operating system has its own characteristic security weaknesses. Hackers regularly confer to trade information on these as they are identified. System programmers also issue upgrades to fix problems as they are identified.[183]

- (U) **Audit systems and networks, and regularly check user logs.** Information resources should be as comprehensive as practicable. Many organizations victimized by hackers or insiders later find that they have kept insufficient track of the activities of their users and are unable to completely understand how they were victimized.[184]

(U) Intelligence Collection Disciplines

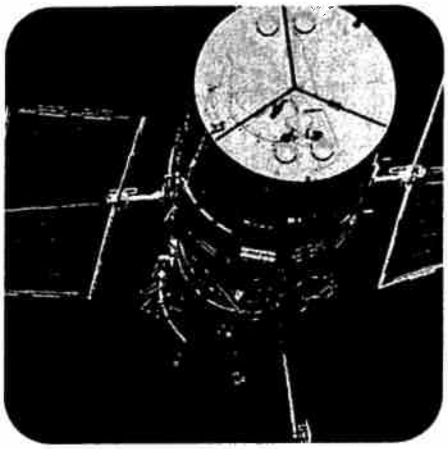
(U) There are five general collection platforms that countries use to gather intelligence regarding U.S. activities:

(U//FOUO) **HUMINT**, or Human Intelligence, is the use of human beings to obtain or confirm information. Collection of information via humans includes overt, covert and clandestine methodologies.

(U//FOUO) **SIGINT**, or Signals Intelligence, which can be performed from a variety of remote locations on the ground or via plane or satellite, is an umbrella term for intelligence derived from the intercept and exploitation of signals. There are three SIGINT subdisciplines:-

- (U//FOUO) **COMINT**, or Communications Intelligence, is the collection and exploitation of communications signals, which can include voice communication, fax and printer, pagers and beepers, and myriad computer-to-computer transmissions.
- (U//FOUO) **ELINT**, or Electronic Intelligence, includes the interception and analysis of non-communications transmissions, most often associated with civil and military radars.

- (U//FOUO) **FISINT**, or Foreign Instrumentation Signals Intelligence, includes interception and exploitation of performance and tracking data (usually telemetry) during tests or operations of weapons systems and space vehicles.



(U//FOUO) **IMINT**, or Imagery Intelligence, is intelligence derived from visual photography, infrared sensors, lasers, electro-optics, and radar sensors. The last includes synthetic aperture radar (SAR), wherein images of objects are reproduced optically and electronically on film, electronic display devices, or other media. This category also includes imagery gathered via satellites.

(U//FOUO) **MASINT**, or Measurement and Signatures Intelligence, is the analysis of equipment emanations. This includes radar intelligence (RADINT); infrared intelligence (IRINT); telemetry intelligence (TELINT); acoustic intelligence (ACOUSTINT); and nuclear intelligence (NUCINT). MASINT operates in different parts of the electromagnetic spectrum and is used to detect information patterns not previously exploited by other systems. The information gathered by MASINT often is not protected by countermeasures.

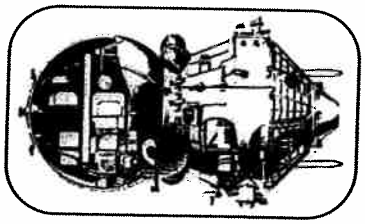
(U) **OSINT**, or Open-Source Intelligence, is intelligence derived from sources available to the public, especially from the news media, and more recently the Internet. More than 90 percent of all information a typical foreign intelligence effort gathers about the U.S. and its activities is derived from open sources.

(U) Selected Supplemental Intelligence Service Information

(U) Russian Federation

(U) Russia has the ability to use IMINT and MASINT to supplement its other intelligence-collection methodologies and develop all-source intelligence products for Russian political leaders, military planners, and industrial concerns.

(U) IMINT



(U) **Satellite imagery systems are Russia's primary source of IMINT.** The first Soviet reconnaissance satellite was launched in 1962. During the next 30 years, the Soviets launched over 850 photoreconnaissance satellites. On average, the Soviets, and now the Russians, have been able to maintain two photoreconnaissance satellites in orbit each year, with an average of 780 mission-days per year. It is believed that Russian imagery systems are able to obtain resolutions of better than one-third of a meter. The Russians currently use three types of imagery satellites, depending on the imagery requirement.[185]

(U) The third-generation photoreconnaissance satellite is a medium resolution system (1 to 3 meters) used for wide area surveillance missions. The satellite flies in low earth orbits at altitudes ranging from 235 to 245 kilometers. It is designed for a mission of 2- to 3-week duration and requires that the satellite be deorbited for return of film canisters. During Operation Desert Storm, the former Soviet Union launched three of these spacecraft to fly repetitive ground tracks over the Persian Gulf region. The capability to quickly launch and recover these satellites allowed the Soviets to respond to the intelligence requirements of Soviet political and military leaders by doubling the coverage of that area. The Russians appear to be phasing the 3rd-generation satellite out of operation in favor of follow-on systems.[186]

(U) The 4th-generation photoreconnaissance satellite provides the Russians with increased operational capabilities. The spacecraft flies elliptical orbits at altitudes of 170 kilometers, which improves resolution. The principal improvements in the systems are the ability to return film canisters without deorbiting the spacecraft and, consequently, the extension of orbital lifetime. The productive lifetime of the 4th-generation satellite now averages 60 days per mission. During the last 5 years, the Russians have launched 6 high-resolution satellites and 1 topographic mapper annually. During the Persian Gulf War, the former Soviets launched 4 fourth-generation satellites in a period of less than 90 days, illustrating the ability of the Russians to surge reconnaissance systems in times of crisis or international tension. The ground track of these satellites was aligned with the Persian Gulf region to provide additional coverage during daylight hours.[187]

The Russians have been able to maintain a constellation of 160 satellites in simultaneous orbits, the same level as during the existence of the Soviet Union, despite a 35 percent reduction in launches.

(U) The 5th-generation satellite is an EO imaging system that provides the Russians with near real-time imagery. The 5th-generation imagery satellite greatly improves the reconnaissance capabilities of the Russian Federation. It provides quicker return of intelligence data and ends the restrictions posed by the limited amount of film that can be carried by a photoreconnaissance satellite. In general, the 5th-generation satellite is used for global reconnaissance and the 3rd- and 4th-generation satellites are used for coverage of particularly sensitive areas.[188]

(U) Overall, the Russians have continued to maintain a robust space reconnaissance program, despite predictions that the program would wane after the demise of the Soviet Union. The Russians have been able to maintain a constellation of 160 satellites in simultaneous orbits, the same level as during the existence of the Soviet Union, despite a 35 percent reduction in launches. The one major problem faced by the Russians is the lack of an all-weather, day-night imaging system. Both EO and photographic systems require daylight and clear weather in order to get an image of an area. In the 1980s, the Soviets attempted to develop a SAR system to provide all-weather and night coverage. This program failed to develop a militarily acceptable product, and the resulting Almaz spacecraft was converted into a commercial mapping system. No comparable SAR system is currently known to be under development.[189]

(U) MASINT

(U) The Russians have programs that can provide MASINT data, such as the Prognoz satellite program that has infrared detection capabilities similar to those provided by the United States Defense Support Program (DSP) satellite system. The Prognoz can be used to conduct a variety of missions in support of Infrared Intelligence. Other MASINT-related systems include a wide variety of sophisticated radar systems that can be used for Radar Intelligence, a well-developed Acoustic Intelligence program for antisubmarine warfare, and a highly developed Nuclear Intelligence program that collects samples from nuclear testing.[190]

(U) Peoples Republic of China

(U) Ministry of State Security

(U) The MSS is divided into several different subsections or divisions. Each division relates to one of two specific types of skills; regional or organizational. Regional divisions are responsible for conducting operations in their specific geographic locale. Organizational divisions are responsible for the bureaucratic functions of the MSS, such as accounting or training.

(U) **Domestic Bureau.** The Domestic Bureau, also known as the First Bureau, recruits people with overseas connections to work for the Ministry of State Security. The Domestic Bureau can expedite exit document application procedures for travelers. The Bureau is also responsible for receiving Chinese secret agents from abroad who return to China every few years for holidays, or meetings. To conceal the identity of its agents, the Domestic Bureau may require its agents to enter China through a third country. The MSS has special guesthouses in the suburbs of Beijing to provide accommodation for returning agents. These guesthouses have many small compounds, and offer substantial privacy and security.[191]

(U) **Overseas Bureau.** The Overseas Bureau, also known as the Second Bureau, is responsible for operations abroad. It provides tasking, and receives, analyzes and reports to higher levels intelligence collected by its operatives and agents. The Overseas Bureau is responsible for sending clandestine agents abroad using covers such as cadres posted to foreign trade companies, banks, insurance companies, ocean shipping companies, etc. The Overseas Bureau also recruits agents abroad. Some of these agents have worked for the Bureau for decades, while others are long-time hidden agents who are not normally assigned duties and are only activated as needed.[192]

(U) **Hong Kong, Macao, and Taiwan Bureau.** The Hong Kong, Macao, and Taiwan Bureau, also known as the Third Bureau, has geographical intelligence responsibility for operations in these areas. The main activities of the Bureau include agent operations and recruitment of PRC nationals with Hong Kong, Macao and Taiwan connections. The Bureau receives agents when they return to the mainland for reporting, tasking or holidays. Only a small number of the postings are permanent, and most agents are replaced once every few years. The Ministry of State Security increased its activities in Hong Kong following the reversion of the territory in 1997, where it can now operate without foreign interference against pro-democracy elements in the territory.[193]

(U) **Technical Bureau.** The Technical Bureau, also known as the Fourth Bureau, studies and develops intelligence gathering and counterintelligence tradecraft. This includes surveillance, wiretapping, photography, recording, communications, and intelligence transmission gadgetry. Due to the technical nature of this field, postgraduates in virtually every discipline have been recruited to the work of the Bureau.[194]

(U) **Local Intelligence Bureau.** The MSS Fifth Bureau, the Local Intelligence Bureau, is responsible for directing and coordinating the work of local departments and bureaus of the Ministry at the provincial and municipal levels.[195]

(U) **Counterintelligence Bureau.** The Sixth Bureau is the MSS's Counterintelligence Bureau. The primary task of Chinese counterintelligence activity is to work against overseas Chinese prodemocracy organizations. Its investigative priorities have included Western consortia investing in China, which were suspected of involvement in attempts to bring about "peaceful evolution" to democracy in China. Overseas Chinese prodemocracy organizations also have been investigated under suspicions that they were sending "investors" to China who were actually engaged in anti-communist activities. Much of the Counterintelligence Bureau's work is focused on surveillance of individuals of interest and on conducting security awareness education briefings for local authorities to encourage them to report suspicious people and activities.[196]

(U) **Reports Bureau.** Also known as the Seventh Bureau, the Reports Bureau checks, verifies, prepares, and writes intelligence reports and special classified reports based on all-source intelligence. Ordinary reports are prepared for other government departments, while the special reports go to the top Chinese hierarchy. Work at the Seventh Bureau is the most boring and difficult of all the MSS units, and low morale is a continuing problem.[197]

(U) **Institute of Contemporary International Relations (ICIR).** The Eighth Bureau of the MSS has no operational intelligence function. Instead, it is one of the world's largest institutes for research on international relations, with a staff that at one time numbered over 500 research fellows. The Bureau is divided into 10 research offices, specializing in general international relations, global economy, the United States, Russia, Eastern Europe, Western Europe, the Middle East, Japan, Asia, Africa, and Latin America. One of its main objectives is to collect open-source information. The institute is also responsible for providing every foreign affairs secretary of each

Political Bureau Standing Committee member with subscriptions to major English-language newspapers as well as major Hong Kong and Taiwan newspapers and magazines. Another mission of the institute is the preparation of publications for units at the provincial, army, and ministerial levels. ICIR's recurring publications include:

- (U) **Studies in International Relations** (guoji guanxi yanjiu), published every 10 days, on world political and economic trends and events, and policies toward China.
- (U) **Summaries of Books and Newspapers** (shubao jianxun), a news bulletin published every three to four days with excerpts of works by the world's public figures, documents issued by other governments, editorials from major papers, and articles by noted reporters.
- (U) **Contemporary International Relations** (xiandai guoji guanxi), a journal issued quarterly.[198]

(U) **Counterespionage Bureau.** The Counterespionage Bureau, also known as the Ninth Bureau, is responsible for countering efforts by foreign intelligence services to recruit personnel of the MSS and among cadres of other Chinese institutions abroad. It also counters surveillance, wiretapping and infiltration by foreign intelligence services against Chinese embassies and consulates. The Counterespionage Bureau includes an overseas students section, which specializes in "anti-defection" work among Chinese students abroad, including both preventing their recruitment by foreign intelligence services as well as investigating student participation in overseas Chinese prodemocracy organizations.[199]

(U) **Science and Technology Bureau.** Also known as the Tenth Bureau, the MSS's Science and Technology Bureau is charged with collecting economic, scientific and technological intelligence. This represents a significant shift in emphasis from work under the former Central Investigation Department, which was mainly concerned with political intelligence. There have been few reported instances of successful covert collection by this bureau, however.[200]

(U) **Computer Support Bureau.** The Eleventh Bureau, the Computer Support Bureau, is responsible for analyzing intelligence gathered with electronic computers, and also operating the computer network of the Ministry of State Security. It also collects information on advanced electronic systems from the West and protects the information systems of Chinese intelligence services from attacks by foreign intelligence agencies.[201]

(U) Military Intelligence Department

(U) The Military Intelligence Department (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). [202]

(U) The MID is organized into numerous divisions and bureaus, including military-based collection and analysis groups. These groups exist within the PLA's Navy and Air Force, its ground army. Each division of the MID is responsible for determining its own intelligence requirements and conducting operations within its own Military Region. In addition to the individual service intelligence divisions within the MID, there are a number of functional bureaus responsible for collection, analysis, science and technology, records and archives, classified materials, general resource management, and OPSEC:[203]

(U) **The First Bureau** is primarily engaged in the collection of military intelligence and has these responsibilities divided into regional sections. In the regions that share a border with another state, the regional offices collect information on that state. However, the Nanjing region of the MID is responsible for collecting information about the United States.[204]

Two of the bureau's favorite sources of information are Congressional reports and RAND Corporation documents.

(U) **The Western Nations Analysis Bureau, or Fifth Bureau**, primarily relies on OSINT collection, focusing on the United States. Two of the bureau's favorite sources of information are congressional reports and RAND Corporation documents.[205]

(U) **The Bureau of Science and Technology, or Seventh Bureau,** controls two electronics factories, the Sea Gull Electrical Equipment Factory and the Beijing Electronic Factory; two computer centers, the Science and Technology Bureau Computer Center and the Northern Transportation University Computer Center; and two research institutes, the No. 57 and No. 58 Institutes. The Seventh Bureau is completely independent from its civilian counterparts in the MSS.[206]

(U) **The Beijing Institute for International Studies** 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 suspected that the institute 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.[207]

(U) **The PLA Institute for International Studies**, formerly known as the Nanjing Foreign Affairs Institute, is responsible for teaching MID personnel specialized techniques and methodology used in intelligence operations.[208]

(U) **The 8341 Unit.** The Beijing-based Central Security Regiment, also known as the 8341 Unit, was an important PLA law enforcement element. It was responsible over the years for the personal security of Mao Zedong and other party and state leaders. More than a bodyguard force, it also operated a nationwide intelligence network to uncover plots against Mao or any incipient threat to the leadership. The unit reportedly was deeply involved in undercover activities, discovering electronic listening devices in Mao's office and performing surveillance of his rivals. The 8341 Unit participated in the late 1976 arrest of the leadership of the ultra-left wing of the Chinese Communist Party, marking the official end of the Cultural Revolution; but the unit reportedly was deactivated soon after that event.[209]

(U) Technical Department

(U) The Technical Department (TD), also called the Third Department, is responsible for Chinese SIGINT operations. The TD was founded in the 1950s with equipment supplied by the Soviet Union, originally under the guise of being a meteorological bureau. Although the TD currently maintains the most extensive SIGINT capability in the Asia-Pacific region, only fragmentary information concerning its organization and activities have become public knowledge.[210]

(U) The Technical Department provides the PRC with a wide range of SIGINT capabilities. The Chinese maintain, by far, the most extensive SIGINT capability of any nation in the Asia-Pacific region. The Chinese operate several dozen SIGINT ground stations deployed throughout China. There they monitor signals from Russia, Taiwan, Japan, South Korea, India, and Southeast Asia. Signals from U.S. military units located in the region are of significant interest to these monitoring stations, and a large SIGINT facility at Hainan Island is principally concerned with monitoring U.S. naval activities in the South China Sea. Additionally, the Chinese have developed a series of SIGINT collection vessels that monitor U.S. military operations and exercises in the Asia-Pacific region.[211]

The Chinese actively monitor international communications satellites from SATCOM intercept facilities on Hainan Island and outside Beijing.

(U) The Chinese also actively monitor international communications satellites from SATCOM intercept facilities on Hainan Island and outside Beijing. The Hainan SIGINT complex was significantly upgraded in 1995.[212]

(U) The PRC has been conducting space-based imaging of the earth since 1975, when it became the third country in the world to retrieve high-resolution photographs of the planet shot from space. The Chinese currently 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 present a substantial intelligence collection threat to U.S. forces in the region. By mid-1999 a total of 17 FSW-class spacecraft had been orbited, with 15 successful recoveries. The FSW-1 model was introduced in September 1987. FSW-1 satellites have carried imaging payloads with high-resolution (10-15 m) cameras for film development on Earth and with 50-m resolution camera systems for near-real-time images. Unlike Russian photo reconnaissance satellites, FSW-1 spacecraft do not perform orbital maneuvers to adjust their groundtracks for prolonged observations over areas of high interest. FSW satellites are normally flown only once each year and usually in the August-October period.[213]

(U) The Chinese appear to be developing a spaceborne ELINT system that is mounted on their photoreconnaissance and communications satellites. There is no indication at this point that this capability presents a significant threat to U.S. forces in the region.[214]

(U) New China News Agency (NCNA)

(U) The NCNA was founded in 1931 as the Red China News Agency. It is currently China's primary source of foreign and domestic news and deploys hundreds of journalists who are assigned to collect and disseminate foreign news, publish documents, and disseminate information throughout the PRC. However, the NCNA primarily engages in open-source collection. It has a staff of more than 5,000 employees operating out of over 90 bureaus and 300 offices in China and abroad; monitoring newspapers, magazines, and broadcasts from around the world; and conducting open-source analysis for the Chinese leadership. Given its global network and journalistic credentials, it often provides cover to Chinese intelligence operatives from other agencies. In the past, only People's Daily and NCNA were used to provide journalist cover for MSS intelligence officers. However, this practice has recently extended to most major newspapers, including Guangming Daily, Economic Daily, China Youth News, and Workers' Daily, which have correspondents in the United States, Japan, Europe and other countries.[215]

China's news agency has a staff of more than 5,000 employees operating out of over 90 bureaus and 300 offices in China and abroad; monitoring newspapers, magazines, and broadcasts from around the world.

(U) Cuba

(U) The principal intelligence collection arms of the Cuban government are the Directorate General of Intelligence (DGI) of Ministry of the Interior and the Military Counterintelligence Department of the Ministry of Revolutionary Armed Forces. Both have been closely associated with the Soviet and Russian intelligence services. Based upon the military cooperation agreement between Russia and Cuba of June 1993, the relationship between these services is likely to continue.[216]

(U) Military Counterintelligence Department

(U) The Military Counterintelligence Department is responsible for conducting counterintelligence, SIGINT, and electronic warfare activities against the United States.[218]

(U) Directorate of General Intelligence

(U) The DGI is responsible for Cuba's foreign intelligence collection and has six divisions divided into two categories of roughly equal size: the operational divisions and the support divisions.

(U) The DGI's operational divisions include the Political/Economic Intelligence Division, the External Counterintelligence Division, and the Military Intelligence Division. The Political/Economic Intelligence Division consists of four sections: Eastern Europe, North America, Western Europe, and Africa-Asia-Latin America. The External Counterintelligence Division is responsible for penetrating foreign intelligence services and the surveillance of exiles. The Military Intelligence Department focuses on collecting information on the United States Armed Forces and coordinating SIGINT operations with the Russians at Lourdes.[219]

(U) The support divisions include the Technical Support Division, the Information Division, and the Preparation Division. The Technical Support Division is responsible for production of false documents, communications systems supporting clandestine operations, and development of clandestine message capabilities. The Information and Preparation Divisions are responsible for intelligence analysis functions.[220]

(U) Despite the economic failure of the Castro regime, Cuban intelligence-in particular, the DGI-remains a viable threat to the United States. The Cuban mission to the UN is the third largest UN delegation, and it has been alleged that almost half the personnel assigned to the mission are DGI officers. The DGI actively recruits HUMINT agents within the Cuban émigré community and has used refugee flows into the United States to place agents in this country.[221]

(U) In February 2000, FBI agents arrested Mariano Faget, a Cuban-born supervisor in the Miami office of the U.S. Immigration and Naturalization Service for spying for the Cuban government. Faget was accused of handing over U.S. secrets to a Cuban citizen and lying about contacts with Cuban government officials.[222] At his trial, prosecutors revealed that FBI agents were wiretapping Faget as he told a business acquaintance with ties to Cuban intelligence that a Cuban security officer who had been based in Washington was going to defect to the United States. The information was false and had been fed to Faget to see what he would do with it. A jury convicted Faget of disclosing classified information and other offenses, but in June 2001 the trial judge sentenced him to only five years' imprisonment, citing his "exemplary work record" and the failure of the prosecution to demonstrate that the information Faget had compromised to Cuba damaged U.S. interests.[223]

(U) The DGI collects political, economic, and military information within the United States. The DGI also conducts operations to collect information about technologies needed to improve the Cuban economy.[224] The United States considers Cuba to be a sponsor of international terrorism, one that has worked closely with Puerto Rican separatist and Latin American terrorist groups. Much of this activity is handled through the DGI.[225]

(U) America Department

(U) Some analysts say that a third intelligence component, the America Department (DA), is the most powerful branch of Cuba's security apparatus.[226] The DA has control over covert Cuban activities for supporting national liberation movements and the efforts of regimes such as those of Nicaragua and Grenada. The DA may be responsible for planning and coordinating Cuba's secret guerrilla and terrorist train-

The Ana Belen Montes Case

(U) In September 2001, Ana Belen Montes, the Defense Intelligence Agency's (DIA's) senior analyst for Cuban matters, was arrested for spying for Cuba. Montes, single and 44 years old, had begun working for DIA in 1985 and become a Cuban analyst in 1992. At about the same time, she began spying for Cuba because she believed it was not being treated fairly by the United States. She provided information about U.S. intelligence-gathering programs concerning Cuba and also the identities of some U.S. officers working undercover against the Cubans.

(U) Montes would receive coded radio transmissions from the Cubans, decode them with a program on her home computer, and then go to a public telephone to use prepaid telephone cards provided to her by the Cubans to call telephone pager numbers also provided to her. She would leave a message on the pager by entering digits that corresponded to a special list of messages she had been given on special water-soluble paper, so that it could be disposed of quickly in an emergency. U.S. authorities were able to recover details of her activities over a number of years by recovering files she had deleted on a laptop computer she purchased. Other than reimbursement for some travel expenses, Montes did not accept money for her espionage activities.

(U) After pleading guilty to espionage in October 2002, Montes addressed the court: "I engaged in the activity that brought me before you because I obeyed my conscience rather than the law. I believe our government's policy towards Cuba is cruel and unfair... My way of responding to our Cuba policy may have been morally wrong... I can only say that I did what I thought right to counter a grave injustice." Ana Belen Montes was sentenced to 25 years in prison.

ing camps, networks for the covert movement of personnel and material from Cuba, and a propaganda apparatus. DA personnel regard themselves as the elite of the various Cuban security agencies. Covers used by DA staff include diplomatic posts; Cuba's Prensa Latina news agency; Cubana Airlines, the Institute for Friendship With the People (ICAP); and Cuban front companies. In 1983, the DA had between 200 and 300 members.[227]

(U) North Korea

(U) HUMINT is North Korea's primary source of intelligence collection against South Korea and other intelligence targets. Additionally, North Korea continues to expand its SIGINT capabilities and currently possesses the capability of monitoring many South Korean and U.S. communications in the region. The North Koreans have a limited HUMINT capability in the United States, and what they have is primarily directed at acquiring nuclear weapons technology. The primary threat posed by North Korean intelligence operations is directed against U.S. forces stationed in South Korea.

The primary threat posed by North Korean intelligence operations is directed against U.S. forces stationed in South Korea.

(U) The North Korean intelligence community is in a dynamic environment. It changes structure and organization as power shifts within the Communist Party of the Peoples Democratic Republic of Korea (DPRK). At present, the majority of DPRK intelligence agencies are within the Cabinet General Intelligence Bureau (CGIB) of the Korean Worker's Party (KWP) Central Committee and are directly responsible to the president of the country. The CGIB is primarily responsible for coordinating and implementing the intelligence directives among five departments actively involved in intelligence collection operations.[228]

(U) Liaison Department

(U) The oldest of these departments is the Liaison Department. The Liaison Department was founded in the late 1940s and, until the early 1980s, was the premiere intelligence agency in North Korea. The Liaison Department was initially responsible for the collection of intelligence on South Korea, but this evolved into the role of conducting collection and covert operations overseas, especially in Japan. [229]

(U) Reconnaissance Bureau

(U) The Reconnaissance Bureau is responsible for collecting strategic, operational, and tactical intelligence for the Ministry of the People's Armed Forces. It also exercises operational control over agents engaged in collecting military intelligence and in the training and dispatch of unconventional warfare teams to South Korea. The primary methods of infiltration have been through tunnels under the Demilitarized Zone and seaborne operations involving submarine and high-speed patrol boats as insertion vehicles. In the 1970s, in support of overland insertion, North Korea began clandestine tunneling operations along the entire DMZ, with two tunnels per forward division. By 1990, four tunnels dug on historical invasion routes from the north had been discovered by South Korean and United States tunnel neutralization teams: 3 in the mid-1970s and the 4th in March 1990. The South Koreans suspect there were as many as 25 tunnels in the early 1990s, but the level of ongoing tunneling is unknown.[230]

(U) State Security Department

(U) Since 1973, the State Security Department has been responsible for North Korea's defensive and offensive counterintelligence programs. It carries out a wide range of counterintelligence and internal security functions normally associated with "secret police." It is charged with searching out anti-state criminals-a general category that includes those accused of antigovernment and dissident activities, economic crimes, and slander of the political leadership. Camps for political prisoners are under its jurisdiction. To support its counterintelligence responsibilities at home and abroad, the Security Department runs overseas intelligence collection operations. It also monitors political attitudes and maintains surveillance of returnees.[231]

(U) Ministry of Public Security

(U) The Ministry of Public Security, responsible for internal security, social control, and basic police functions, is one of the most powerful organizations in North Korea and controls an estimated 144,000 public security personnel. It maintains law and order; investigates common criminal cases; manages the criminal prison system and traffic control; monitors citizens' political attitudes; conducts background investigations, census, and civil registrations; controls individual travel; manages the government's classified documents; protects government and party officials; and patrols government buildings and some government and party construction activities. Ministry of Public Security personnel escort high-ranking officials traveling abroad. The Ministry also guards national borders and monitors international entry points. The Border Guards are the paramilitary force of the Ministry of Public Security. They are primarily concerned with monitoring the border and with internal security. The latter activities include physical protection of government buildings and facilities. During a conflict, they would probably be used in border and rear area security missions.[232]

(U) The Chosen Soren

(U) Chosen Soren (the General Association of Korean Residents in Japan—Zainichi Chosenjin Sorengokai), is North Korea's de facto diplomatic presence in Japan. The association currently has 200,000 members. Nearly one-third of the Japanese pachinko [pinball] industry is controlled by Chosen affiliates or supporters.[233] Chosen members each year remit an estimated $100-$600 million in hard currency to Pyongyang for family members in North Korea. A wing of the Chosen Soren supports intelligence operations in Japan, assists in the infiltration of agents into South Korea, collects open source information, and diverts advanced technology for use by North Korea.[224]

A wing of the Chosen Soren supports intelligence operations in Japan, assists in the infiltration of agents into South Korea, collects open source information, and diverts advanced technology for use by North Korea.

(U) In February 2003, Los Angeles Korean-American businessman John Joungwoon Yai was arrested by the FBI for failing to register as a foreign agent for North Korea and not disclosing that he had received at least $18,000 from North Korean officials for a variety of low-level intelligence services over a seven-year period. In late 2003, Yai entered a guilty plea to the charge and was expected to be sentenced to up to two years' imprisonment.[235]

(U) The Economic Espionage Act of 1996

(U) In October 1996, the Economic Espionage Act was signed into law. The purpose of the new statute was to provide new tools, weapons, and sanctions to use against industrial espionage. The main provisions of the new legislation are as follows:

(U) **Scope.** The Economic Espionage Act outlaws economic espionage where:

1. (U) The conduct occurs in the U.S.
2. (U) The conduct occurs outside the U.S. and either:
    a. (U) An Act in furtherance of the offense was committed in the U.S.
    b. (U) The offender is a U.S. person or organization.

(U) **Confidentiality.** The court must issue orders necessary to protect the confidentiality of trade secrets consistent with Federal Rules of Procedure and the Constitution. Also, the prosecution is permitted to immediately appeal any order authorizing or directing disclosure of a trade secret.

(U) **Criminal Penalties.** Imposes up to a:

1. (U) 15 year prison term and/or maximum $500,000.00 fine on any person and a $10 million fine on any organization who steals or destroys a trade secret of value with intent to benefit any foreign power.
2. (U) 10 year prison term and/or a maximum $250,000.00 fine on any person and a $5 million fine on any organization who knowingly steals or destroys any trade secret with intent to:
    a. (U) Economically benefit anyone other than the owner; and
    b. (U) Injure the owner of the trade secret (Title 18 USC 1832).

(U) **Forfeiture.** Requires the forfeiture to the U.S. Government of proceeds or property derived from economic espionage and may require forfeiture of property used to commit economic espionage. The victim can apply to the U.S. for restitution.

(U) **Civil Relief.** The Government can apply for injunctive relief to prevent trade secret crimes.

(U) Definition of Terms

(U) "**Owner**," with respect to trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

(U) "**Trade Secret**" means all forms and types of financial, business, scientific, technical, engineering or economic information, including patterns, plans, compilations, programs devices, procedures, methods, techniques, codes, processes, or programs, whether or how stored, complied memorialized physically, electronically, graphically, photographically, or in writing if—

1. (U) The owner thereof has taken reasonable measures to keep such information secret; and
2. (U) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

(U) **Corporate Responsibility**. To take reasonable measures to keep trade secret information secret.

(U) Economic Espionage Act of 1996 Text

(U) *1831. Economic Espionage*

(a) (U) IN GENERAL.-Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) (U) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) (U) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) (U) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) (U) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) (U) conspires with one or more others persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) (U) ORGANIZATIONS.-Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

(U) *1832. Theft of trade secrets*

(a) (U) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate of foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) (U) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) (U) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) (U) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) (U) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) (U) conspires with one or more others persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) (U) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

(U) *1833. Exceptions to prohibitions*

(U) This chapter does not prohibit—

(1) (U) any otherwise lawful activity conducted by a government entity of the United States, a State, or a political subdivision of a State; or

(2) (U) the reporting of a suspected violation of law to any government entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

(U) *1834. Criminal forfeiture*

(a) (U) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentenced imposed, that the person forfeit to the United States—

(1) (U) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(2) (U) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

(b) (U) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceedings in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this section.

(U) *1835. Orders to preserve confidentiality*

(U) In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the federal rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

(U) *1836. Civil proceedings to enjoin violations*

(a) (U) The Attorney general may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

(b) (U) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

(U) *1837. Applicability to conduct outside the United States*

(U) This chapter also applies to conduct occurring outside the United States if-

(1) (U) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

(2) (U) an act in furtherance of the offense was committed in the United States.

(U) *1838. Construction with other laws*

(U) This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful, disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

(U) *1839. Definitions*

(U) As used in this chapter—

(1) (U) the term **'foreign instrumentality'** means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

(2) (U) the term **'foreign agent'** means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

(3) (U) the term **'trade secret'** means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing if—

(A) (U) the owner thereof has taken reasonable measures to keep such information secret; and

(B) (U) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

(4) (U) the term **"owner,"** with respect to a trade secret, means the person or entity in which or in which rightful legal or equitable title to, or license in, the trade secret is reposed." ❖

(U) Finding Information and Assistance

Any potential adversary is interested in virtually anything about U.S. military capability, law enforcement capabilities and intentions, political and economic policies, and diplomatic initiatives.

(U) Threat information about a particular operation can be postulated first by employing some common sense concerning who might be interested in critical information about the operation, why they would need the information, and how they might go about collecting it. We should assume that any potential adversary is interested in virtually anything about U.S. military capability, law enforcement capabilities and intentions, political and economic policies, and diplomatic initiatives and that any competitor is interested in anything dealing with economic, trade, and commercial endeavors.

(U) Although threat summaries and intelligence reports can provide an overall picture of the threat, this picture should be tailored to each specific operation or activity. Tailoring the threat picture involves examining both national intelligence sources as well as local sources. Threat information can be obtained through a number of the U.S. government sources, such as the Federal Bureau of Investigation, the Department of Homeland Security, the Defense Intelligence Agency, the Defense Security Service, the Department of Defense Security Institute (DODSI), the Department of Energy (DOE), the Department of State (DOS), and the National Counterintelligence Executive (NCIX). These agencies are responsible for protecting U.S. government and commercial activities, as well as executing counterintelligence programs, security education, and/or threat analysis.

(U) Federal Bureau of Investigation

(U) www.fbi.gov

(U) The FBI has primary responsibility for counterintelligence investigations within the United States and can provide a variety of support services and classified analytical products to government agencies. An integral part of the FBI's counterintelligence efforts is the Awareness of National Security Issues and Response (ANSIR) program. It is the "public voice" of the FBI for espionage, counterintelligence, counterterrorism, economic espionage, cyber and physical infrastructure protection, and all national security issues. The program is designed to provide unclassified national security threat and warning information to U.S. corporate security directors and executives, law enforcement, and other government agencies. Information is disseminated nationwide via the ANSIR-Email and ANSIR-FAX networks. Each of the FBI's field offices has an ANSIR coordinator and is equipped to provide national security threat and awareness information on a regular basis to corporate recipients within their jurisdiction.

(U) Department of Homeland Security (DHS)

(U) www.dhs.gov

(U) One primary reason for the establishment of the Department of Homeland Security was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure the United States. DHS carries out its mission by focusing on the following elements:

- (U) **Awareness**—Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.
- (U) **Prevention**—Detect, deter and mitigate threats to our homeland.
- (U) **Protection**—Safeguard our people and their freedoms, critical infrastructure, property and the economy of our Nation from acts of terrorism, natural disasters, or other emergencies.
- (U) **Response**—Lead, manage and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.
- (U) **Recovery**—Lead national, state, local and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.

(U) Defense Intelligence Agency

(U) www.dia.mil

(U) DIA is a combat support agency and the senior military component in the United States Intelligence Community. It provides intelligence in support of joint military operations in peacetime, crisis, contingency, and combat; service weapons systems acquisition; and defense policy making. DIA prepares counterintelligence (CI) risk assessments for the DOD and conducts a variety of assessments and studies on the foreign intelligence collection threat. DIA also assesses the threat posed by illegal transfers of high-tech military capabilities to adversaries of the United States.

(U) Defense Security Service

(U) www.dss.mil

(U) DSS provides security services to the Department of Defense through the integration of personnel security, industrial security, information systems security, and counterintelligence. Through the integration of security services, combined with intelligence threat data, DSS is uniquely able to facilitate the application of threat-appropriate security countermeasures. A counterintelligence element in DSS is responsible for providing threat data from the intelligence and counterintelligence communities to industry. As the partnership has matured, industry routinely reports security incidents to DSS for joint resolution with management officials. As an added benefit, DSS is able to share this information in a sanitized form in order to enhance the security awareness and training programs for defense industry at large. DSS refers significant incidents involving both industrial and personnel security to the FBI and the military counterintelligence elements if a counterintelligence investigation is believed to be warranted.

(U) Department of Defense Security Institute

(U) www.dss.mil

(U) DODSI was disestablished at the end of fiscal year 1998, and its functions were assumed by the DSS Training Office. In December 1998, DODSI became a part of the DSS. As such, it continues to develop and present courses on DOD security countermeasure programs. DODSI conducts instructional courses on industrial, personnel, and information security. Discussion of intelligence collection threats is an inherent part of the training provided by DODSI. They also publish unclassified security awareness publications. The best known of these publications is the Security Awareness Bulletin, which is distributed to 25,000 customers in government and industry. Articles often highlight foreign economic and industrial intelligence efforts, as well as methods to protect against such activities.

(U) Department of Energy Counterintelligence Division

(U) The DOE Counterintelligence Division is responsible for analyzing foreign intelligence collection threats, providing awareness training, and disseminating threat assessments to government and contract organizations. The CI Division publishes classified and unclassified threat assessments, and distributes bulletins and newsletters concerning foreign intelligence threats to DOE activities and facilities. This data can be provided to U.S. government agencies and corporations that have entered Cooperative Research and Development Agreements (CRADAs) with DOE. The DOE Counterintelligence Division can be contacted at (202) 586-5901.

(U) Department of State Bureau of Diplomatic Security

(U) **www.travel.state.gov**

(U) The Bureau of Diplomatic Security (DS) is responsible for protecting the Secretary of State and other senior leaders in the department; ensuring the security of diplomatic facilities overseas and department activities within the United States, conducting counterterrorism and antiterrorism activities; and investigating violations of U.S. passport laws. In support of its mission, DS conducts threat assessments and provides U.S. government and private entities overseas with threat assessment support through its regional security officers. DOS's Overseas Advisory Council (OSAC) is a joint DS and industry venture that cooperates on overseas security problems of mutual concern. An area of growing concern for OSAC is the intelligence collection threat faced by U.S. businesses overseas. OSAC gathers and disseminates threat information to member businesses. To exchange threat information as expeditiously as possible, the OSAC Electronic Bulletin Board (EBB) has been implemented. The EBB provides a means for businesses to exchange information among themselves and with the Department. It also provides a means for the Bureau of Diplomatic Security's Office of Intelligence and Threat Analysis to disseminate threat information. Travel advisories and other pertinent State Department security information is available on their website.

(U) National Counterintelligence Executive (NCIX)

(U) **www.ncix.gov**

(U) The NCIX was established in accordance with Presidential Decision Directive 24, United States Counterintelligence Effectiveness, issued in May 1994. The NCIX coordinates the U.S. government's efforts to identify and counter foreign intelligence threats to U.S. national and economic security. The NCIX conducts analyses of emerging collection threats, and identifies and broadly disseminates information on HUMINT and technical collection methods. As appropriate, the NCIX provides analytical products to private firms, depending on classification and dissemination caveats.

(U) Department of Commerce Bureau of Export Administration

(U) The Bureau of Export Administration has three offices available to counsel businesses and individuals on their obligations under the Export Administration Regulations and assist in determining their licensing requirements. The Bureau of Export Administration also maintains a list of firms and individuals who have been denied export and reexport privileges.

(U) **Exporter Counseling Division (Washington, DC)**
Room 2705 (for mail)
Room 1099 (for visitors)
14th Street and Pennsylvania Ave., N.W.
U.S. Department of Commerce
Washington DC 20230
Phone: (202) 482-4811 Fax: (202) 482-3617

(U) **Western Regional Office (Newport Beach, CA)**
3300 Irvine Avenue, Suite 345
Newport Beach, CA 92660
Phone: (949) 660-0144 Fax: (949) 660-9347

(U) **Western Regional Office (San Jose, CA)**
101 Park Center Plaza, Suite 1001
San Jose, CA 95113
Phone: (408) 998-7402 Fax: (408)998-7470

(U) The Interagency OPSEC Support Staff

(U) **www.ioss.gov**

(U) The Interagency OPSEC Support Staff (IOSS) was established in January 1989 to carry out national-level, interagency OPSEC training for executives, program and project managers, and OPSEC specialists; to act as a consultant to the executive departments and agencies in connection with the establishment of OPSEC programs and the conduct of OPSEC surveys; to perform OPSEC-related analyses; and to provide an OPSEC technical staff to the National Security Council. IOSS also conducts the Defensive Information to Counter Espionage (DICE) program to disseminate threat information to DOD contractors. DICE provides current threat information through training programs and briefings provided to DOD contractors and the presentation of threat briefings at selected classified conferences. The IOSS can provide government agencies and their supporting contractors with assistance in the following areas:

- (U) OPSEC training courses
- (U) OPSEC program development
- (U) OPSEC survey support
- (U) OPSEC publications and training materials development

The Brian Regan Case

(U) Brian Regan, a 40-year-old married father of four, owed nearly $117,000 on his credit cards when he wrote a letter in 2001 to Iraqi leader Saddam Hussein offering to sell satellite intelligence that could help Iraq hide anti-aircraft missiles. His asking price was $13 million. The letter was found on a computer at Regan's home. The computer contained a nearly identical letter to Libyan leader Moammar Gadhafi. Regan worked at the National Reconnaissance Office (NRO), which operates the government's spy satellites, first for the Air Force and then as a civilian employee for TRW, a defense contractor.

(U) Using his access to a classified government computer network, Regan looked up numerous top-secret documents, including satellite photos of Iraqi missile sites and confidential documents about Libya's biological warfare program. He printed approximately 20,000 pages of this secret material and then buried portions of the information in a series of caches in state parks in Virginia and Maryland. Regan's idea was to sell the exact location of the sites to a foreign country and let its officials or agents dig up the buried intelligence treasure, thus insulating himself from the danger of being caught while delivering the documents.

(U) Regan was arrested in August 2001 at Dulles International Airport outside Washington while boarding a flight for Zurich, Switzerland. Regan was carrying information with the coded coordinates of Iraqi and Chinese missile sites, the missiles that were stored there, and the date the information was obtained. He also had the addresses of the Chinese and Iraqi embassies in Switzerland and Austria in his wallet and tucked into his right shoe.

(U) Prosecutors sought the death penalty for Regan; but although a jury convicted him in February 2003 of espionage, it decided his crimes did not merit execution. In exchange for Regan's cooperation in debriefing, the government dropped possible charges against his wife and allowed her to collect a portion of his pension. Brian Regan was sentenced to life in prison in March 2003. Although he protested that his sentence was too harsh and that his actions were undertaken just "to protect my wife and children," the judge immediately rejected Regan's plea, observing, **"You have betrayed your nation's trust...You have joined the list of infamous spies."**

(U) Selected Readings

Adams, James. **The New Spies: Exploring the Frontiers of Espionage**. Pimlico, 1995.

Andrew, Christopher, and Oleg Gordievsky. **KGB: The Inside Story**. Hodder & Stoughton, 1990.

Andrew, Christopher and Vasili Mitrokhin. **The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB**. Basic Books, 1999.

Choate, Pat. **Agents of Influence: How Japan Manipulates America's Political & Economic System**. Simon and Schuster, 1990.

De Borchgrave, Arnaud and Robert Moss. **The Spike**. Crown Publishers, Inc., 1980.

Dziak, John J. **Chekisty: A History of the KGB**. Lexington Books, 1988.

Eftimiades, Nicholas. **Chinese Intelligence Operations**. Naval Institute Press, 1994..

Faligot, Roger and Remi Kauffer. **The Chinese Secret Service: Kang Sheng and the Shadow Government in Red China**. William Morrow and Company, Inc., 1987.

Fialka, John. **War By Other Means: Economic Espionage in America**. W.G. Norton and Co., 1997.

Hansen, James H. **Japanese Intelligence: The Competitive Edge**. National Intelligence Book Center Press, 1996.

Kalugin, Oleg with Fen Montaigne. **The First Directorate: My 32 Years in Intelligence and Espionage Against the West**. St. Martin's Press, 1994.

Lamphere, Robert J., and Tom Shachtman. **The FBI-KGB War: A Special Agent's Story**. Random House Inc., 1986.

Lunev, Stanislav with Ira Winkler. **Through the Eyes of the Enemy**. Regnery Publishing Inc., 1998.

Metcalfe, Robyn Shortwell. **The New Wizard War**. Tempus Books, 1988.

Polmar, Norman, and Thomas B. Allen. **Spy Book: The Encyclopedia of Espionage.** Random House, Inc., 1997.

Richelson, Jeffrey T. **A Century of Spies: Intelligence in the Twentieth Century.** Oxford University Press, 1995.

Schweizer, Peter. **Friendly Spies**. Atlantic Monthly Press, 1993.

Slatalla, Michelle and Joshua Quittner. **Masters of Deception: The Gang that Ruled Cyberspace**. Harper-Collins, 1995.

Stoll, Clifford. **The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.** Mass Market Paperbacks, 1995.

Timperlake, Edward and William C. Triplett II. **Red Dragon Rising**. Regnery Publishing, Inc. 1999.

Volkman, Ernest. Espionage: **The Greatest Spy Operations of the Twentieth Century**. John Wiley & Sons Inc., 1995.

Weinstein, Allen and Alexander Vassiliev. **The Haunted Wood**. Random House, 1999.

Winkler, Ira. **Corporate Espionage**. Prima, 1997.

(U) Footnotes

[1] Interagency OPSEC Support Staff, OPSEC Fundamentals: Computer Based Training Series (Greenbelt, MD: IOSS, 2002).

[2] Paul D. Moore, "Spies of a Different Stripe," The Washington Post (May 31, 1999), A-23.

[3] Interagency OPSEC Support Staff, OPSEC Fundamentals Computer Based Training Series (Greenbelt, MD: IOSS, 2002).

[4] Peter A Lupsha, "Transnational Organized Crime versus the Nation-State," Transnational Organized Crime 2, no. 1 (spring 1996): 21.

[5] Valentin Aksilenko, "The KGB's Foreign Intelligence Training Center," unpublished notes for the Centre for Counterintelligence and Security Studies, (McLean, VA: January, 2000).

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Wayne Madsen, "Intelligence Agency Threats to Computer Security," International Journal of Intelligence and Counterintelligence 6, no. 4 (winter 1993): 419-420.

[10] Peter Schweizer, Friendly Spies, (New York: Atlantic Monthly Press, 1993), 11-31.

[11] Jeffrey T. Richelson, Sword and Shield: The Soviet Intelligence and Security Apparatus (Cambridge, Mass.: Ballinger, 1986); and United States House of Representatives Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, FBI Oversight and Authorization Request, Hearings before the Subcommittee on Civil and Constitutional Rights, 101st Congress, 2nd Sess., 1990, 281.

[12] Sander Thoenes and Alan Cooperman, "Yeltsin's Eyes and Ears," U.S. News and World Report 119, no. 6 (7 August 1995): 36-39; and Victor Yasmann, "Security Services Reorganized: All Power to the Russian President?" Radio Free Europe/Radio Liberty Reports 3, no. 6 (11 February 1994): 7-14.

[13] Ibid.

[14] Victor Yasmann, "Security Services Reorganized: All Power to the Russian President?" Radio Free Europe/Radio Liberty Reports 3, no. 6 (11 February 1994): 7-14

[15] James Sherr, "Change and Continuity in the Former KGB," Jane's Intelligence Review (March 1993): 110-112; and Adam Zagorin, "Still Spying After All These Years," Time (29 June 1992): 58-59.

[16] Carey Schofield, "Interview with the Head of Russian Military Intelligence," Jane's Intelligence Review (March 1993): 112-116.

[17] Jeffrey T. Richelson, Sword and Shield: The Soviet Intelligence and Security Apparatus (Cambridge, Mass.: Ballinger, 1986), 34-38.

[18] Victor Yasmann, "Security Services Reorganized: All Power to the Russian President?" Radio Free Europe/Radio Liberty Reports 3, no. 6 (11 February 1994): 7-14.

[19] Victor Yasmann, "Security Services Reorganized: All Power to the Russian President?" Radio Free Europe/Radio Liberty Reports 3, no. 6 (11 February 1994): 7-14; and James Sherr, "Change and Continuity in the Former KGB," Jane's Intelligence Review (March 1993): 110-112.

[20] Jeffrey T. Richelson, Sword and Shield: The Soviet Intelligence and Security Apparatus (Cambridge, Mass.: Ballinger, 1986), 34-38

[21] Jane's Intelligence Digest, http://www.janes.com/regional_news/ europe/news/jid/jid021203_1_n.shtml

[22] Victor Yasmann, "Security Services Reorganized: All Power to the Russian President?" Radio Free Europe/Radio Liberty Reports 3, no. 6 (11 February 1994): 7-14; and James Sherr, "Change and Continuity in the Former KGB," Jane's Intelligence Review (March 1993): 110-112.

[23] Desmond Ball, Soviet Signals Intelligence (SIGINT): Intercepting Satellite Communications, Strategic and Defence Studies Centre (Canberra: Australian National University, 1989), 62-63.

[24] "Current and Projected National Security Threats to the United States and Its Interests Abroad," (U.S. Congress: Senate Select Committee on Intelligence, 1996) 213.

[25] Christopher Andrew and Oleg Gordievsky, KGB: The Inside Story (New York: Harper Collins, 1990), 609.

[26] Desmond Ball, "Soviet Signals Intelligence: Vehicular Systems and Operations," Intelligence and National Security 4, no. 1 (January 1989): 5-23.

[27] Ibid.

[28] Christopher Andrew and Oleg Gordievsky, KGB: The Inside Story (New York: Harper Collins, 1990), 608-610; and Craig Covault, "Russian Space Program Advances Despite Crisis," Aviation Week and Space Technology (16 January 1995): 22-24.

[29] Wayne Madsen, "Intelligence Agency Threats to Computer Security," International Journal of Intelligence and Counterintelligence 6, no. 4 (winter 1993): 419-420.

[30] United States House of Representatives Subcommittee on Economic and Commercial Law, Committee on the Director FBI, Hearings before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, 102nd Congress, 2nd Sess., 1992, 42.

[31] Adam Zagorin, "Still Spying After All These Years," Time (29 June 1992): 58-59.

[32] James Adams, Sellout: Aldrich Ames and the Corruption of the CIA (New York: Viking, 1995), 43-45; and Wayne Madsen, "Intelligence Agency Threats to Computer Security," International Journal of Intelligence and Counterintelligence (winter 1993): 418, 420, and 422.

[33] Paul D. Moore, "Spies of a Different Stripe," The Washington Post (May 31, 1999), A-23.

[34] Paul D. Moore, "How China Plays the Ethnic Card," Los Angeles Times, (June 24, 1999), B-9.

[35] "Report to Congress on Chinese Espionage Activities Against the United States by the Director of Central Intelligence and the Director of the Federal Bureau of Investigation," (December 12, 1999).

[36] Ibid.

[37] Paul D. Moore, "China's Subtle Spying," New York Times, (September 2, 1999) A-21.

[38] Ibid.

[39] "Report to Congress on Chinese Espionage Activities Against the United States by the Director of Central Intelligence and the Director of the Federal Bureau of Investigation," (December 12, 1999), and Paul D. Moore, "China's Subtle Spying," New York Times, (September 2, 1999) A-21.

[40] Jeffrey T. Richelson, Foreign Intelligence Organizations (Cambridge, Mass.: Ballinger, 1988), 295, and Desmond Ball, "Signals Intelligence in China," Jane's Intelligence Review 7, no. 8 (1 August 1995): 365.

[41] Nicholas Eftimiades, Chinese Intelligence Operations (Annapolis: Naval Institute Press, 1994), 17-19.

[42] Ibid., 18-20.

[43] Paul D. Moore, "Chinese Recruitment Techniques," Centre for Counterintelligence and Security Studies, (January, 2000 unpublished class notes).

[44] "Report to Congress on Chinese Espionage Activities Against the United States by the Director of Central Intelligence and the Director of the Federal Bureau of Investigation," (December 12, 1999).

[45] "China Boosts Spy Presence in U.S., CIA, FBI Report," Washington Times (March 9, 2000).

[46] Paul D. Moore, "How China Plays the Ethnic Card," Los Angeles Times, (June 24, 1999), B-9.

[47] Paul D. Moore, "China's Subtle Spying," New York Times, (September 2, 1999) A-21, and Paul D. Moore, "Spies of a Different Stripe," The Washington Post (May 31, 1999), A-23.

[48] Ibid.

[49] Nicholas Eftimiades, Chinese Intelligence Operations (Annapolis: Naval Institute Press, 1994), 78-89.

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] Desmond Ball, "Signals Intelligence in China," Jane's Intelligence Review 7, no. 8 (1 August 1995): 365.

[54] Ibid.

[55] "Report to Congress on Chinese Espionage Activities Against the United States by the Director of Central Intelligence and the Director of the Federal Bureau of Investigation," (December 12, 1999).

[56] Nicholas Eftimiades, Chinese Intelligence Operations (Annapolis: Naval Institute Press, 1994), 113-116.

[57] Paul D. Moore, "Spies of a Different Stripe," The Washington Post (May 31, 1999), A-23, and Paul D. Moore, "China's Subtle Spying," New York Times, (September 2, 1999) A-21.

[58] Paul D. Moore, "Chinese Recruitment Techniques," Centre for Counterintelligence and Security Studies, (January, 2000 unpublished class notes).

[59] "An Earlier China Spy Case Points Up Post-Cold War Ambiguities," New York Times, (March 13, 1999).

[60] Ibid.

[61] "Reports Show Scientist Gave U.S. Radar Secrets to Chinese," New York Times, (May 10, 1999).

[62] Ibid.

[63] Ibid.

[64] "In China, Physicist Learns, He Tripped Between Useful Exchange and Security Breach," New York Times, (August 1, 1999).

[65] Ibid.

[66] Ibid.

[67] Desmond Ball, "Signals Intelligence in China," Jane's Intelligence Review 7, no. 8 (1 August 1995): 365-368; and Desmond Ball, "Signals Intelligence in Hong Kong," Intelligence and National Security 11, no. 3 (July 1996): 474-495.

[68] Desmond Ball, "Signals Intelligence in China," Jane's Intelligence Review 7, no. 8 (1 August 1995): 367.

[69] Jeffrey T. Richelson, "The Future of Space Reconnaissance," Scientific American 264, no. 1 (January 1991): 38-44.

[70] Paul D. Moore, "Spies of a Different Stripe," The Washington Post (May 31, 1999), A-23, and Paul D. Moore, "China's Subtle Spying," New York Times, (September 2, 1999) A-21.

[71] "Report to Congress on Chinese Espionage Activities Against the United States by the Director of Central Intelligence and the Director of the Federal Bureau of Investigation," (December 12, 1999).

[72] John Fialka, War By Other Means, (New York: Norton, 1997), xi-xiv.

[73] Canadian Security Intelligence Service, "Economic Security," www.csis-scrc.gc.ca/eng/operat/es2e.html, (January, 2000).

[74] National Counterintelligence Center "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage - 2002," vii.

[75] American Society for Industrial Security, "Trends in Proprietary Information Loss," (Pricewaterhouse Coopers, 1999), 6-24.
[76] 1999 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, "Foreign Economic and Industrial Espionage Remains a Threat in 1999," (GPO: 1999).
[77] 1998 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, "The Cost of Economic Espionage," (GPO: 1998).
[78] Ibid.
[79] Rusty Capps, "The Spy Who Came to Work," Security Management, (February, 1997), 47.
[80] John Fialka, War By Other Means, (New York: Norton, 1997), 66-76.
[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] Christopher Andrew and Vasili Mitrokhin, The Sword and the Shield, (New York: Basic, 1999), 474-475.
[86] Rusty Capps, "The Spy Who Came to Work," Security Management, (February, 1997), 47.
[87] Ibid.
[88] Federal Bureau of Investigation, "Economic Espionage Case Summaries," (1995), 12-13.
[89] Ibid., 1.
[90] Ibid., 5.
[91] "Dirty Work: Fertilizer, Frustration, and Industrial Espionage," Far Eastern Economic Review, (February 9, 1995), 50-51.
[92] "Taiwan Men Held for Trying to Steal Bristol-Myers Drug," Dow Jones News Service, (June, 1997); and "Corporate-Spy Case Rebounds on Bristol," The Wall Street Journal, (February 2, 1998).
[93] "Man Admits to Economic Espionage," Pittsburgh Post-Gazette, (April 20, 1998); and "Man Sentenced in Theft," Pittsburgh Post-Gazette, (November 14, 1998).
[94] Rusty Capps, "The Spy Who Came to Work," Security Management, (February, 1997), 48.
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Ibid., 49.
[99] Federal Bureau of Investigation, "Economic Espionage Case Summaries," (1995), 6.
[100] Ibid., 7.
[101] "Inquiring Eyes: an Israeli Contract with a U.S. Company Leads to Espionage," The Wall Street Journal, (January 17, 1992), A-1; and Rusty Capps, "The Spy Who Came to Work," Security Management, (February, 1997), 54-55.
[102] Rusty Capps, "The Spy Who Came to Work," Security Management, (February, 1997), 48.
[103] David G. Major, "Espionage Realities," Centre for Counterintelligence and Security Studies, (January, 2000 unpublished class notes).
[104] Peter Schweizer, Friendly Spies, (New York: Atlantic Monthly Press, 1993), 38-39.
[105] Rusty Capps, "The Spy Who Came to Work," Security Management, (February, 1997), 48.
[106] Federal Bureau of Investigation, "Economic Espionage Case Summaries," (1995), 11.
[107] "Former Exxon Employee Charged with Offering Secrets to IBM," Dow Jones News Service, (August 8, 1980).
[108] Federal Bureau of Investigation, "Economic Espionage Case Summaries," (1995), 3-4.
[109] Ibid., 9.
[110] Ibid., 8.
[111] "Testing the Limits of Trade Secrets," The Washington Post, (December 9, 1997), C-1.
[112] "Voice Mail Theft Scheme May Land Man in Jail," Boston Herald, (November 26, 1996); and "As Computer Technology Thrives, Lawbreaking Is a Keystroke Away," Boston Globe, December 4, 1996.
[113] "Firm Stops Apparent Espionage Try," Greensboro News & Record, (December 12, 1996);

and "Five Years Prison in Espionage Case," York Daily Record, (April 19, 1997).

[114] "Engineer Indicted on Charges He Stole Trade Secrets on Gillette Shaving System," The Wall Street Journal, (September 26, 1997); and "Former Gillette Associate Pleads Guilty to Stealing Trade Secrets," Dow Jones Online News, (January 27, 1998).

[115] "Cadence Suit on Trade-Secret Theft Pending," Dow Jones News Service, (March 18, 1997); and "Avant! Loses Lawsuit by Cadence Design over Trade Secrets," The Wall Street Journal, (September 24, 1997).

[116] "Inquiring Eyes: an Israeli Contract with a U.S. Company Leads to Espionage," The Wall Street Journal, (January 17, 1992), A-1; and Rusty Capps, "The Spy Who Came to Work," Security Management, (February, 1997), 54-55.

[117] "Report of the Special Senate Committee on Security and Intelligence," (Government of Canada: Canadian Security Intelligence Service, 1999).

[118] Ibid.

[119] Ibid.

[120] Ibid.

[121] Ibid.

[122] Ibid.

[123] Ibid.

[124] Ibid.

[125] Ibid.

[126] Ibid.

[127] Computer Emergency Response Team (CERT) Coordination Center, "Overview of Internet Security," Froelich/Kent Encyclopedia of Telecommunications, vol. 15, (1997).

[128] Ibid.

[129] Ibid.

[130] Ibid.

[131] Ibid.

[132] Ibid.

[133] Ibid.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] Ibid.

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] U.S. Department of Defense, "Web Site Administration Policies and Procedures," (November 25, 1998), 1.1.2.

[142] Ibid., 1.2.4

[143] Ibid., 3.1.

[144] Ibid., 2.3

[145] Ibid., 8.2.

[146] Russel L. Brand, Coping with the Threat of Computer Security Incidents, (June, 1980), 45.

[147] Ibid.

[148] Ibid.

[149] Ibid.

[150] Ibid.

[151] Ibid.

[152] Ibid.

[153] Ibid., 21.

[154] William Church, as quoted by John Borland, "Analyzing the Threat of Cyberterrorism," (TechWeb: September 23, 1998).

[155] Russel L. Brand, Coping with the Threat of Computer Security Incidents, (June, 1980), 39.

[156] Ibid., 39-41.

[157] Ibid.
[158] Ibid.
[159] Ibid.
[160] Ibid.
[161] Ibid.
[162] Ibid.
[163] Ibid.
[164] Ibid.
[165] Ibid.
[166] Ibid.
[167] Ibid.
[168] Ibid.
[169] Ibid.
[170] Ibid.
[171] Ibid., 6.
[172] Ibid., 13.
[173] "The Tale of the Russian Hacker," The Guardian, (December 5, 1996); Cyber-Space Is the New Battleground," Toronto Star, (August 10, 1997); and "Cyberterror Threat Draws Disorganized Response," USA Today, (October 21, 1997).
[174] "FBI Hacker Caseload Multiplies," Newsbytes, (February 22, 2000).
[175] Russel L. Brand, Coping with the Threat of Computer Security Incidents, (June, 1980), 15.
[176] Ibid., 21.
[177] Canadian Security Intelligence Service, "Computer Security: the Problem of Keeping Information Systems Secure," (CSIS Liaison/Awareness Program, 1999), 4.
[178] Russel L. Brand, Coping with the Threat of Computer Security Incidents, (June, 1980), 27.
[179] Canadian Security Intelligence Service, "Computer Security: the Problem of Keeping Information Systems Secure," (CSIS Liaison/Awareness Program, 1999), 4.
[180] Ibid.
[181] Russel L. Brand, Coping with the Threat of Computer Security Incidents, (June, 1980), 48.
[182] Ibid.
[183] Ibid.
[184] Ibid.
[185] Jeffrey T. Richelson, "The Future of Space Reconnaissance," Scientific American 264, no. 1 (January 1991): 38-44.
[186] Nicholas L. Johnson and David M. Rodvold, 1991-1992 Europe and Asia in Space, Technical Report DC-TR-2191.103-1 (Kirtland Air Force Base, N.Mex.: USAF Phillips Laboratory, 1992), 241-245.
[187] Ibid., 241-245.
[188] Ibid., 241-245; and Craig Covault, "Russian Space Program Advances Despite Crisis," Aviation Week and Space Technology (16 January 1995): 22-24.
[189] Ibid., 241-245; and Craig Covault, "Russian Space Program Advances Despite Crisis," Aviation Week and Space Technology (16 January 1995): 22-24.
[190] William B. Scott, "Russian Pitches Common Early Warning Network," Aviation Week and Space Technology 9 (January 1995): 46-47; and Jeffrey T. Richelson, Sword and Shield: The Soviet Intelligence and Security Apparatus (Cambridge, Mass.: Ballinger, 1986), 108-111.
[191] Tan Po, "Spy Headquarters Behind the Shrubs-Supplement to 'Secrets About CPC Spies'" Cheng Ming no. 233 (Hong Kong, March 1, 1997), 34-37.
[192] Ibid.
[193] Ibid.
[194] Ibid.
[195] Ibid.
[196] Ibid.
[197] Ibid.
[198] Ibid.

[199] Ibid.

[200] Ibid.

[201] Ibid.

[202] Ibid.; and Tan Po, "Communist China's Intelligence, External Affairs Research Organs,"Cheng Ming, no. 227, (Hong Kong: September 1, 1996), 28-31.

[203] Nicholas Eftimiades, Chinese Intelligence Operations (Annapolis: Naval Institute Press, 1994), 75-79.

[204] Ibid., 17.

[205] Ibid., 83.

[206] Ibid., 84.

[207] Ibid., 82.

[208] Ibid., 81.

[209] Tan Po, "Spy Headquarters Behind the Shrubs-Supplement to 'Secrets About CPC Spies'" Cheng Ming no. 233 (Hong Kong, March 1, 1997), 34-37.

[210] Desmond Ball, "Signals Intelligence in China," Jane's Intelligence Review 7, no. 8 (1 August 1995): 365.

[211] Ibid.; and Desmond Ball, "Signals Intelligence in Hong Kong," Intelligence and National Security 11, no. 3 (July 1996): 474-495.

[212] Federation of American Scientists, www.fas.org/intelligence/world agencies/China/facilities/Hainan. (January, 2000)

[213] H. Changchui, "The Development of Remote Sensing in China", Space Policy, February 1989, pp.65-74; J. Zhaogian and G. Lynwood-May, "China's Developing Space Program," Signal, (February, 1986) 27; "LM-2C Placed a Satellite Into LEO", press release, China Great Wall Industry Corporation, (October 28,1993); and Liu Ming, "The Use of Retrievable Satellites," Beijing Review, (July, 1997).

[214] Desmond Ball, "Signals Intelligence in China," Jane's Intelligence Review 7, no. 8 (1 August 1995): 365-368; and Desmond Ball, "Signals Intelligence in Hong Kong," Intelligence and National Security 11, no. 3 (July 1996): 474-495. See also Richard D. Fisher, "China's Arms Require Better U.S. Military Ties with Taiwan," Heritage Foundation backgrounder no. 1163, (March 11, 1998); and Lin Hau-bao and Min Gui-rong, "Aspects of the China's Recoverable Satellite Platform," Paper IAF-93-U.2.552, 44th Congress of the International Astronautical Federation, (October 1993).

[215] Jeffrey T. Richelson, Foreign Intelligence Organizations (Cambridge, Mass.: Ballinger, 1988), 295; and Nicholas Eftimiades, Chinese Intelligence Operations (Annapolis: Naval Institute Press, 1994), 21-23, 107.

[216] H. P. Klepak, "The Cuban Armed Forces," Jane's Intelligence ReviewYear Book (31 December 1994): 136-138; and Jeffrey T. Richelson, Sword and Shield: The Soviet Intelligence and Security Apparatus (Cambridge, Mass.: Ballinger, 1986), 210-212.

[217] Ibid.

[218] Ibid.

[219] Ibid.

[220] Ibid.

[221] Christopher Andrew and Oleg Gordievsky, KGB: The Inside Story, of its Foreign Operations from Lenin to Gorbachev (New York: Harper Collins, 1990), 561-563.

[222] "INS Officer Charged with Spying for Cuba," The Washington Post, (February 18, 2000), A-8; and "FBI Sting at INS Found an Unlikely Cuban Spy," The Washington Post, (February 19, 2000), A-1.

[223] "INS Official Gets 5 Years in Spy Sting," Miami Herald. (Miami, FL: June 30, 2001), p. A1.

[224] Calvin Sims, "Engineer Says He Stole Secrets of Chip Makers," New York Times, (May 22, 1995), A-1.

[225] Christopher Andrew and Oleg Gordievsky, KGB: The Inside Story, of its Foreign Operations from Lenin to Gorbachev (New York: Harper Collins, 1990), 561-563.

[226] Rex A. Hudson, Castro's America Department, The Cuban American National Foundation, 1988.

[227] Desmond Ball, "Signals Intelligence in North Korea," Jane's Intelligence Review 8, no. 1

(January 1996): b28.

[228] Ibid.

[229] Ibid., 29.

[230] Andrea Matles Sevada, ed., North Korea: A Country Study (Washington, D.C.: USGPO, 1993), 261-262; Joseph S. Bermudez, Jr., "North Korea's Intelligence Agencies and Infiltration Operations," Jane's Intelligence Review (June 1991): 269-271; and Kongdan Oh, North Korea in the 1990s: Implications for the Future of the United States-South Korean Security Alliance, RAND Note 3480 (Santa Monica: RAND, 1992).

[231] Ibid.

[232] Andrea Matles Sevada, ed., "North Korea-the Public Security Apparatus," North Korea: A Country Study (Washington, D.C.: USGPO, 1993).

[233] "Pachinko Players Underwrite North Korea," The Washington Post, (June 7, 1996), A-25.

[234] Tsutomu Nishioka, Chosen Soren Today and Its Future. (Monthly Modern Korea)

[235] "Man Enters Guilty Plea in Federal Probe" Los Angeles Times. (Los Angeles, CA: October 24, 2003.

[236] David Wise, "Tinker, Tailor, Soldier, Spy Hunter; If Caruso Has His Way, Foreign Agents in District Will Be Put Out in the Cold," The Washington Post (January 19, 2000), A-21.

[237] Ibid, p. A-21.

[238] David Major and Rusty Capps, U.S. Counterintelligence: The Foundation of Strategy and Espionage Realities, (Centre for Counterintelligence and Security Studies, 1999), 396.

[239] Robyn Shotwell Metcalfe, The New Wizard War, (Redmond, Washington: Tempus, 1988) 118-119.

[240] Ibid., 376.

[241] Federal Bureau of Investigation, "Economic Espionage Case Summaries," (1995), 10.

[242] "Trashy Caper in River Oaks; FBI Is Alerted after French Consul Grabs Garbage," Houston Chronicle, (June 5, 1991); "U.S. Firms Targeted by Foreign Intelligence," Asian Wall Street Journal, (June 25, 1991).

[243] "Two Convicted in Spying Case," New York Times, (April 30, 1999); and "Detention Given in Theft of Secrets," New York Times, (January 8, 2000).

[244] "Teenager Charged in Air Tower Hacking," Los Angeles Times, (March 19, 1998); "FBI Hacker Caseload Multiplies," Newsbytes, (February 22, 2000).

[245] Ira Winkler, Corporate Espionage, (Prima, 1997).