

Section 3

ADVERSARY FOREIGN INTELLIGENCE OPERATIONS

Introduction

This section focuses on the intelligence collection activities of five nations that traditionally have been considered hostile to our national interests and have used their intelligence services to harm the interests of the United States. The nations considered in this section are: **Russia, the Peoples' Republic of China (PRC), Cuba, North Korea, and Romania**. Despite the substantial political changes that have taken place in the world, these nations continue to expend significant resources to conduct intelligence operations against the United States. In the past, these efforts were centered on producing intelligence concerning U.S. military capabilities, other national security activities, and military research and development activities. The nations discussed in this section continue to collect this type of information, however, they have expanded their collection efforts to place additional emphasis on collecting scientific, technical, economic, and proprietary information. These collection efforts are designed to promote the national welfare of these nations and provide technologies required for the acquisition and maintenance of advanced military systems. In general, the national intelligence collection efforts of these nations have diminished little since the end of the Cold War.[1]

Each of the countries discussed in this section has the ability to collect intelligence on targeted U.S. activities using HUMINT, SIGINT, and the analysis of open source material. Intelligence collection activities initiated by these nations have targeted activities within the continental United States, and U.S. facilities and personnel in foreign nations. Some of these nations also have access to imagery products that can be used to produce IMINT. Only the Russian Federation, and the PRC to a very limited extent, however, have the ability to gather intelligence from spaceborne intelligence collection platforms. Russia continues to present the most serious intelligence collection threat to the United States and will be discussed in the next portion of this section.[2]

Russian Intelligence Collection Capabilities--An Overview

The Russian Federation has a significant intelligence capability that it inherited from the former Soviet Union. Much of this intelligence collection infrastructure continues to focus on collecting information concerning the United States. Russia has the ability to use IMINT, SIGINT, HUMINT, MASINT, and open source analysis to develop all source intelligence products for Russian political leaders, military planners, and industrial concerns. According to the Federal

Bureau of Investigation, Russian intelligence operations against the United States have increased in sophistication, scope, and number, and are likely to remain at a high level for the foreseeable future.[3]

Russia has three bodies with foreign intelligence functions designated by law: the Russian Foreign Intelligence Service (SVR), the Main Intelligence Directorate of the General Staff (GRU), and the Federal Agency for Government Communications and Information (FAPSI). After the dissolution of the Soviet Union, the Committee of State Security (KGB) was broken up into eight different agencies, the majority of which are responsible for internal security matters. The President of the Russian Federation directly controls the activities of the intelligence, law enforcement, and defense activities of the Russian government. Intelligence activities are overseen by the Russian National Security Council and coordinated through the Permanent Interbranch Commissions of the National Security Council and their Chairmen. In addition to the three foreign intelligence agencies, the 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 could be derived from declarations made to the Customs Service. 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.[4]

Russian Intelligence Organizations

The Russian Foreign Intelligence Service (SVR)

The SVR, the successor to the First Chief Directorate of the KGB, is responsible for collecting foreign intelligence. The SVR 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, and the KGB was broken up in retribution for these actions. 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, and relies on HUMINT, SIGINT, and open source analysis for producing intelligence.[5] The majority of SVR case officers operate under diplomatic cover from Russian embassies and consulates. Although the number of SVR personnel has allegedly been reduced by 30 percent, the agency continues active collection operations. It is also suspected that the SVR continues to be involved in conducting propaganda and influence operations.[6]

The Main Intelligence Directorate of the General Staff (GRU)

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 for the Russian armed forces. Principle missions include the collection of indications 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 SIGINT from various platforms (ships, aircraft, satellites and ground stations).[7]

Collection activities that threaten U.S. interests are those under the First Deputy Chief and the Space Intelligence Directorate.[8] The Space Intelligence Directorate manages the Russian space reconnaissance program in coordination with the Fleet Intelligence Direction of the Fifth Directorate. 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. The directorate is located at Votutinki, 50 kilometers southwest of Moscow. It operates its own cosmodromes, several research institutes, supporting mission ground centers, and a centralized computer processing facility.[9]

The Chief of Information is responsible for the analysis of information obtained through the intelligence collection operations managed by the First Deputy Chief. 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 Mnth Directorate, which acquires and assesses scientific and technical data for the military design bureaus. Of particular interest to the OPSEC manager is the Institute of Information, which operates separately from the directorates under the Chief of Information and is responsible for developing intelligence products based on the fusion of open source materials and classified information.[10]

The Federal Agency for Government Communications and Information (FAPSI)

The FAPSI was created in October 1991 by Presidential decree. It is the newest of the Russian intelligence agencies, and relatively little information is available on its organizational structure and activities. The FAPSI is responsible for both communications security for the Russian Federation, and SIGINT operations against targeted foreign activities. It has also been given responsibility 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 on the territory of other sovereign states, and to conduct foreign business activities. The access provided through such activities will allow FAPSI the opportunity to monitor communications systems in which it has an interest, and will permit the purchase 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. It appears that the Russians hope that the entrance of FAPSI into the commercial telecommunications market will end this isolation.[11]

Russian Intelligence Operations

HUMINT

Both the GRU, and the SVR as the successor to the KGB, conduct HUMINT operations that target the United States. The most recent example of a HUMINT operation conducted by Russia is the case of Aldrich Ames. Ames was a Central Intelligence Agency employee in the Directorate of Operations. In his work with the Directorate of Operations, Ames was able to obtain information pertaining to ongoing operations targeting the former Soviet Union and later Russia. Ames volunteered to work for the KGB in April 1985 as a walk-in to the Soviet Embassy in Washington and continued to work for the SVR after the fall of the Soviet Union. His espionage activities continued until his arrest on the morning of February 21, 1994. Upon his arrest, it was determined that Ames had been paid at least \$2.5 million for his services and that he had compromised, by his own admission, "virtually all Soviet agents of the CIA and other American and foreign services known to me." In addition, he stated that he provided the former Soviet Union and Russia with a huge quantity of information on U.S. foreign, defense, and security policies.[12]

It is very likely that the Russians will continue to place a significant emphasis on the development of HUMINT sources because of the quality of information they have received in the past.[13] Since the August 1991 coup, the number of HUMINT operations conducted by the SVR and KGB that target the United States and the West have risen rather than fallen. In March 1993, the FBI and German counterintelligence authorities reported that SVR/GRU activities in their respective countries had grown by over 12 percent from pre-coup levels.[14] This is due to a number of factors. First, as a result of arms control treaties, joint business opportunities, and numerous cultural and economic exchanges, the Russian intelligence services now have greater access to American society, government, and industry. Second, there has been a significant influx of Russian emigres into the United States. **The FBI estimates that over 105,000 Russians emigrated to the United States in the late 1980s.** The Russians have traditionally used emigres as a means to gather intelligence. Third, there has been a substantial influx of Russian students into the United States; many of these students are studying technical disciplines that are required by the Russians to improve both military and civil industries. Fourth, travel restrictions on Russian diplomatic and consular personnel in the United States have been lifted, making it easier to collect information on U.S. activities.[15]

SIGINT

Russia continues to maintain one of the most sophisticated SIGINT programs in the world. The GRU's Sixth Directorate uses over 20 different types of aircraft, a fleet of 60 SIGINT collection vessels, satellites, and ground stations to collect signals intelligence. Together with FAPSI, the GRU operates SIGINT collection facilities in over 60 diplomatically protected facilities throughout the world. These agencies also operate large ground collection facilities within the territory of the Commonwealth of Independent States, at Cam Rank Bay, Vietnam, and at Lourdes, Cuba. These activities provide the Russians with worldwide SIGINT collection capabilities.[16]

The SIGINT facility at **Lourdes** is among the most significant intelligence collection capabilities targeting the United States. This facility, less than 100 miles from Key West, is one of the largest and most sophisticated SIGINT collection facilities in the world. It is jointly operated by the GRU, FAPSI, and Cuba's intelligence services. The 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, together with a sister facility in Russia, allows the Russians to monitor all U. S. military and civilian geosynchronous communications satellites.[17] It has been alleged that the Lourdes facility monitors all White House communications activities, launch control communications and telemetry from NASA and Air Force facilities at Cape Canaveral, financial and commodity wire services, and military communications links. According to one source, Lourdes has a special collection and analysis facility that is responsible for **targeting financial and political information**. This activity is manned by specially selected personnel and appears to be highly successful in providing Russian leaders with political and economic intelligence.[18]

The former Soviet Union also used a variety of other means to collect signals intelligence. The Soviets operated SIGINT collection sites in over 60 countries from diplomatically protected embassies, consulates, trade legations, and residences. It is possible that these activities are continuing in the United States. The location of a number of Russian diplomatic facilities in the United States would provide Russian SIGINT collectors with access to sensitive information. Russian collection activities could derive sensitive information on Government policies from monitoring Government activities in the Washington, DC area, and sensitive financial and trade information using Russian facilities located in New York, San Francisco, and Seattle. The location of microwave towers and cellular communication repeaters in the vicinity of Russian diplomatic facilities in these cities increases the potential damage from collection activities. In the past, vans from the Soviet Mission to the United Nations were observed in the vicinity of the GE Americom satellite ground station in Vernon Valley, NJ, and vans from the San Francisco consulate were observed in the vicinity of AT&T microwave towers in Northern California. In both cases, the vans appeared to be conducting SIGINT monitoring at these facilities.[19]

The Russians have probably also continued the Soviet practice of using covert mobile collection platforms. During the Cold War, the Russians frequently used tractor-trailers, and other vehicles with concealed SIGINT collection equipment to gather intelligence in Western Europe. Western intelligence officials estimate that the Soviets conducted over **7,000 covert vehicular SIGINT** operations in NATO countries annually. During these operations, the Soviets gathered electronic order of battle (EOB) data, monitored exercise communications, conducted direction finding operations, and calibrated Soviet SIGINT satellites to determine geolocation accuracies. The Soviets also allegedly used clandestine collection vans located in Mexico to monitor activities at White Sands Missile Range in New Mexico and Vandenberg Air Force Base, California. Vans operating from Tijuana, Mexico reportedly were able to monitor all of Southern California and Western Arizona. There have also been reports that Aeroflot aircraft and clandestine collection vehicles have been used to collect SIGINT data inside the continental United States.[20]

The Russians also use satellites for collecting SIGINT. The first Soviet SIGINT satellite was the **Cosmos 189 ELINT satellite**, which was launched in 1967. Over the next 24 years, the Soviets placed over **200 SIGINT satellites into orbit**. The Russians continue to maintain a robust

presence in space. During 1994, the Russians conducted 48 spacecraft launches, 50 percent of which were military missions including advanced imagery systems, ocean reconnaissance, and electronic intelligence collection. In 1995, the Russians have programmed 45 space launches; again approximately 50 percent will be military missions.[21]

The GRU is tasked with operating Russian ELINT satellites. **ELINT satellites use active and passive techniques to detect specific targets.** They complement the data provided by imaging satellites and assist in developing a more complete picture of an adversary's forces or intentions. These satellites are designed to track and geolocate radio and radar emanations of ships at sea, mobile air defense radars, fixed strategic early warning radars, and other military emitters for the purpose of identification, location, and signals analysis. The data can then be used for targeting, offensive and defensive engagement planning, and countermeasure development.

Collection activities are managed by the Satellite Intelligence Directorate, and data analysis is performed by the Decrypting Service of the Sixth Directorate. Currently, there is no evidence of the existence of a Russian COMINT satellite, however, it is likely that the Russians could develop such a system if they wished.[22]

IMINT

The primary IMINT threat posed by Russia is represented by satellite imagery systems. The first Soviet reconnaissance satellite was launched in 1962. Over the next 30 years, the Soviets launched **over 850 photoreconnaissance satellites.** On average, the Soviets, and now the Russians, have been able to maintain 2 photoreconnaissance satellites in orbit each year with an average of 780 mission days per year. Russian imagery systems are assessed to be 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.**[23]

The third-generation photoreconnaissance satellite is a **medium resolution system (1.5 to 3 meters) that is 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 mission durations of **2 to 3 weeks, 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 double their coverage of the area in response to the intelligence requirements of Soviet political and military leaders. The Russians appear to be phasing the third-generation satellite out of operation in favor of follow-on systems.[24]

The fourth-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 the extension of orbital lifetime. The productive lifetime of the fourth-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 groundtrack of these satellites was aligned with the Persian Gulf region to provide additional coverage during daylight hours.[25]

The fifth-generation satellite is an electrooptic imaging system that provides the Russians with near real-time imagery. The fifth-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 fifth-generation satellite is used for global reconnaissance, and the third and fourth generation satellites are used for coverage of particularly sensitive areas.[26]

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 orbit simultaneously, the same level as under 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 electro-optic and photographic systems require daylight and clear weather to be able to image an area. In the 1980s, the Soviet attempted to develop a synthetic aperture radar (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.[27]

MASINT

The Russians have a number of programs that can provide MASINT data. The Russian Prognoz satellite has infrared detection capabilities similar to those provided by the U.S. Defense Support Program (DSP) satellite system. The Prognoz can be used to conduct a variety of missions in support of infrared intelligence (IRINT). Other MASINT-related systems include a wide variety of sophisticated radar systems that can be used for radar intelligence (RADINT), a well-developed acoustic intelligence (ACOUSTINT) program for antisubmarine warfare, and a highly developed nuclear intelligence (NUCINT) program that collects samples from nuclear testing. [28]

Russian Intelligence Collection Trends

Russia is likely to continue to aggressively use its intelligence services to gain information concerning the United States. They will retain the ability to develop all source intelligence and will use the information gained through these efforts to improve their standing in global political, economic, and security matters. Russia will continue to pursue intelligence concerning U.S. military capabilities, foreign policy initiatives, and the development of military technologies. There is likely to be an increased emphasis on obtaining commercial or dual use technology through intelligence operations.[29]

Defectors from the former Soviet and the Russian intelligence services have stated 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 joint U.S./Russian business ventures in an effort to legally obtain or steal desirable Western technologies. The Russians do not in many cases have the ability to pay for those items they need to improve economic growth so they are willing to steal them or obtain them through other illegitimate means. Additionally, the Russians still must contend with restrictions on certain technologies that they desire. Most of these technologies are dual use technologies that would play a significant role in the development of advanced weapons systems or improved Command, Control, Communications, and Intelligence (C3I) systems. In 1994, the United States denied a request by the Russian government to purchase advanced telecommunications systems from AT&T. The request was denied based on an assessment by the National Security Agency that the technology would be used in C3I systems. Based on past collection patterns, it should be assumed that the Russians are still targeting these technologies.[30]

Another likely trend is that, because of the reported reduction in the number of SVR intelligence officers, the Russians will place increasing emphasis on gaining information through technical intelligence disciplines, and open source analysis.[31] Although the opportunity to collect HUMINT has expanded as a result of the relaxation of security standards in 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 is likely to be more carefully targeted to gain information not readily available through technical intelligence collection or through open source exploitation. The Russians have always relied on open source information and will continue to obtain intelligence by analyzing public data in comparison with intelligence derived through classified sources. The Soviets used a variety of research and political institutes for the analysis of open source data. The majority of these institutes have been retained by the Russians and are likely performing the same roles as they did under the Soviet Union. The Russians will continue to use information gained through these research institutes and from the collection opportunities provided by joint trade, research, and educational activities.[32]

Chinese Intelligence Collection Capabilities--An Overview

The People's Republic of China (PRC) has a significant intelligence collection capability, much of which is focused on regional adversaries, in particular, Russia. The United States is a primary target of China because of its role as a global superpower, its substantial military, political, and economic presence in the Pacific Rim and Asia, and its role as a developer of advanced technology China requires for its economic growth. Intelligence functions in China are controlled through the Central Committee of the Communist Party and through the General Staff Department of the Central Military Commission. Intelligence operations are coordinated through the General Office of the Central Committee, and all intelligence reports must be reviewed by this office prior to presentation to the Chinese leadership. China has four intelligence organizations that conduct collection activities directed at the United States: the Ministry of State Security, the Military Intelligence Department, the Third or Technical Department of the Central Military Commission, and the New China New] Agency.[33]

Chinese Intelligence Collection Organizations

Ministry of State Security (MSS)

The MSS was created in June 1983 by the Central Committee to centralize foreign intelligence and counterintelligence functions. The MSS is headed by the Minister of State Security, who reports to the Central Committee. It conducts counterespionage operations within China, and HUMINT and limited SIGINT operations both inside and outside of the PRC. The MSS centers its collection operations on regional adversaries with which China has shared borders, including Russia, India, and Vietnam, and on nations that are militarily, politically, or economically important to China. The latter category includes the United States, Taiwan, South Korea, and Japan. Key intelligence collection objectives for the MSS include:

- Acquiring foreign military and civilian high technology
- Collecting information on adversary military planning, foreign policy, and foreign trade positions concerning China
- Monitoring Chinese dissident groups overseas.[34]

HUMINT is the primary discipline used by the MSS for intelligence collection in the United States and other targeted nations. The MSS may also have a limited covert SIGINT capability. The Chinese use both overt and clandestine HUMINT collection to gather information required by their leaders. Additionally, the MSS attempts to gain information on foreign targets through surveillance of foreigners visiting China.[35]

Military Intelligence Department (MID)

The MID is responsible for basic order-of-battle intelligence, studies of foreign weapons systems, and analyses of the capabilities of foreign military organizations. It obtains information through military attaches, review of open source literature, clandestine HUMINT operations, and joint business ventures. The MID is believed to play an integral role in obtaining advanced military technologies to bolster China's military capabilities and improve weapons systems vital to China's export arms business. The MID has also played a significant role in the development of clandestine relationships with Israel and other nations to gain expertise in the development of advanced weapons systems. Together with the Commission on Science, Technology and Industry for National Defense (COSTIND), the MID works to obtain military technologies for application to the Chinese military. Much of this technology is obtained through technological diversion and reverse engineering of products purchased from the West. The MID is also responsible, in concert with the COSTIND, for the development of China's space reconnaissance program.[36]

Technical Department

The Technical Department, or Third Department of the General Staff Department of the Central Military Commission, is the national agency responsible for managing China's strategic SIGINT program. The Department was established in the early 1950s with Soviet assistance to provide the Chinese General Staff with a limited SIGINT capability and strategic communications support.[37]

New China News Agency (NCNA)

The NCNA is the primary domestic and international news agency for the PRC. The NCNA has a staff of over 5,000 employees operating out of over 90 bureaus and 300 offices in China and abroad. NCNA has served as a cover for clandestine Chinese intelligence operations. The NCNA monitors newspapers, magazines, and broadcasts from around the world, and conducts open source analysis for the Chinese leadership.[38]

Chinese Intelligence Operations

HUMINT

The MSS is the primary Chinese HUMINT collection organization, although the MID is also involved in HUMINT collection. The MID is primarily involved in the overt collection of technical information through visits to trade shows, military exchange programs, and through the military attache program. The MSS is responsible for both overt and clandestine collection. It uses students, diplomats, businessmen, and scientists in its attempts to gain information. China has been extremely aggressive in its HUMINT collection activities in the United States. The PRC has more than 2,600 diplomatic and commercial officials in the United States. A substantial percentage of these personnel are actively involved in collecting intelligence. More than 40,000 students from the PRC also attend schools in the United States, and many of these students have been tasked to collect information by the Chinese government. In addition to these personnel, over 25,000 Chinese visit the United States each year as members of official delegations, and an additional 20,000 Chinese emigrate to the United States annually.[39]

The MSS has been able to obtain high- and mid-level technologies not cleared for export to the PRC through its activities. It has used three principal means to obtain such technology: first, recruiting agents in China and sending them abroad to acquire technology; second, acquiring American firms that produce a desired technology; and third, the use of MSS operated front companies in Hong Kong. The Chinese have used a number of different methods to gather HUMINT. They have used pressure to gain information from the Chinese immigrant community, especially on those Chinese that have access to high technology or military data. The MSS has also encouraged Chinese students to remain in the United States as long-term penetration agents. MSS personnel have acted as intelligence collectors using cover as NCNA reporters, trade office representatives, and accredited diplomats.

Scientific exchange programs have proven to be extremely useful means for the Chinese to gather information. The FBI has stated that virtually all Chinese allowed to leave the PRC for the United States are given some type of collection requirement to fulfill. Although the bulk of Chinese operations are not sophisticated operations, the large number of ongoing Chinese operations greatly increases the difficulty of countering their espionage activities. In recent years, the Chinese have been the subject of approximately half of all cases initiated by U.S. law enforcement agencies concerning the illegal diversion of technology from the United States.[40]

SIGINT

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. 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. A large SIGINT facility at Hainan Island is principally concerned with monitoring U.S. naval activities in the South China Sea. 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. The Chinese actively monitor international communications satellites from SATCOM intercept facilities on Hainan Island, and outside Beijing. Additionally, the Chinese have developed a series of SIGINT collection vessels that monitor U.S. military operations and exercises in the Asia/Pacific region.[41]

IMINT

The Chinese currently have a limited spaceborne photoreconnaissance capability that focuses on collecting imagery over the Russian border. The Chinese 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. U.S. intelligence agencies believe that China will likely develop a mid-resolution electro-optic imaging system in the future that will provide the Chinese with improved capabilities.[42]

Chinese Intelligence Collection Trends

The PRC will continue to use its intelligence services to gather information about the United States, and to obtain access to advanced technologies. An integral part of this effort will be the use of open source information gathered by students, scientific researchers, and the NCNA. China will likely improve both its SIGINT and IMINT capabilities, increasing the collection threat to the United States. The Chinese will continue to use intelligence collection to improve their economic position in the global economy.[43]

Cuban Intelligence Collection Capabilities An Overview

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. The relationship between these services is likely to continue based upon the June 14, 1993 agreement on military cooperation between Russia and Cuba. The DGI is responsible for foreign intelligence collection. The DGI has six divisions divided into two categories of roughly equal size: the Operational Divisions and the Support Divisions. The operational divisions include the Political/Economic Intelligence Division, the External Counterintelligence Division, and the Military Intelligence Division. 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. 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 is focused on collecting information on the U.S. Armed Forces and coordinates SIGINT operations with the Russians at Lourdes. The Military Counterintelligence Department is responsible for conducting counterintelligence, SIGINT, and electronic warfare activities against the United States.[44]

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 United Nations 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 within the Cuban emigre community and has used refugee flows into the United States to place agents. The DGI collects political, economic, and military information within the United States. More recently, the DGI has started to conduct operations to gain access to technologies required to improve the Cuban economy. Cuba is considered by the United States to be a sponsor of international terrorism and has worked closely with Puerto Rican separatist and Latin American terrorist groups. Much of this activity has been handled through the DGI.[45]

North Korean Intelligence Collection Operations

North Korea's intelligence organizations are under the supervision of the National Intelligence Committee of the Central Committee of the Korean Workers Party and are directly responsible to the President. There are several intelligence agencies within the government and the Korean Worker's Party. The majority of the North Korean intelligence agencies are within the Cabinet General Intelligence Bureau of the Korean Worker's Party Central Committee. The Liaison Department is responsible for conducting intelligence operations in South Korea and Japan. Its agents are used to undermine the South Korean government by supporting internal subversion and to gather information on U.S. forces in Korea. The Research Department for External Intelligence (RDEI) is the primary agency responsible for foreign intelligence collection. The RDEI is composed of four geographic subsections, one of which is North America. The third agency under the Central Committee is the General Association of Korean Residents in Japan (Chosen Soren). 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.

Other North Korean intelligence agencies include the Reconnaissance Bureau of the General Staff Department and the State Security Department. The Reconnaissance Bureau is responsible for collecting strategic, operational, and tactical intelligence for the Ministry of the People's Armed Forces. It is also responsible for infiltrating intelligence personnel into South Korea through tunnels under the demilitarized zone and seaborne insertion. The State Security Department is responsible for North Korea's counter intelligence and offensive counterintelligence programs.

North Korea primarily depends upon HUMINT for intelligence collection in South Korea and other parts of the world. The North Koreans do have a limited SIGINT capability, however, it is largely focused on South Korean activities. The North Koreans have a limited HUMINT capability in the United States and Canada that has been directed at acquiring technologies related to nuclear weapons. The primary threat posed by North Korean intelligence operations is to American forces in South Korea.[47]

Romanian Intelligence Collection Operations

Romania continues to pose a HUMINT and limited SIGINT collection threat to United States Government and commercial activities operating in the Central European region. Additionally, the Romanians have used their intelligence services to collect information on advanced technologies in the United States. The three intelligence agencies that operate against the United States are the Romanian Intelligence Service (SRI), the Foreign Intelligence of the Ministry of Foreign Affairs, and the Special Telecommunications Service (STS). The SRI is an autonomous agency responsible to the President of Romania. It is responsible for collecting foreign intelligence and protecting the state. It has approximately 5,000 personnel, many of whom are former members of the Securitate. The Foreign Intelligence Service is responsible for collecting political and economic intelligence. Intelligence officers are located at Romanian embassies and consulates. The STS performs SIGINT functions for the Romania government and actively targets foreign embassies and businesses for collection.[48]

The next section of this handbook examines the intelligence services of terrorist states.

[FAS](#) | [Space](#) | [Guide](#) | [Russia](#) | [Military](#) |||| [Index](#) | [Search](#) |



F Space **World**
A Policy **Space**
S Project **Guide**

Russia and Image Intelligence

Between 1962 and 1994 the USSR/Russian Federation placed more than 800 photo reconnaissance spacecraft into Earth orbit on dedicated military missions (another 25 spacecraft were lost in launch failures). These missions have ranged in length from only a few days to more than 400 days, a record set by Kosmos 2267 in 1994. Only seven dedicated military photo recons were launched during each of 1993 and 1994. However, on average more than two spacecraft were operational during the entire period, and no observation gaps appeared (Figure 6.2).

Declassified photographs with resolutions of 2-30 m can now be purchased commercially, while resolutions on the order of one-third meter have been acknowledged.

Since the first Soviet photo spacecraft was successfully orbited (Kosmos 4 in 1962), a variety of specialized spacecraft have been developed. Today, four basic classes of the 6-7 metric-ton photo recons are operational, and a possible new generation spacecraft began flight testing in the second half of 1994 (Figure 6.3). All such spacecraft are now launched by the Soyuz-U/U2 launch vehicle from either the Baikonur or Plesetsk Cosmodromes. Whereas most spacecraft physically return film to Earth for development and processing, some, longer duration spacecraft possess either digital transmission or dual transmission/capsule capabilities.

Unlike many satellites designed to photograph the Earth, Russian photo recons fly in posigrade (normally 63 degree-83 degree) orbits rather than sun-synchronous trajectories. Consequently, when altitude restoration maneuvers are made every 7-10 days, the satellite's argument of perigee is normally adjusted to keep perigee phased with acceptable lighting conditions. For example, during a typical 2-month mission, the argument of perigee will be rotated progressively from ascending passes (first month) to descending passes (second month). Fifth-generation satellites are an exception with arguments of perigee normally maintained between 80 degrees and 110 degrees.

- [Third Generation Photo Recons](#)
- [Fourth Generation Photo Recons - Yantar](#)
- [Kometa](#)
- [Fifth Generation Photo Recons](#)
- [Sixth Generation Photo Recons](#)
- [Seventh Generation Photo Recons](#)
- [Almaz](#)

Sources and Resources

- Adapted from: [Europe and Asia in Space 1993-1994](#), Nicholas Johnson and David Rodvold [Kaman Sciences / [Air Force Phillips Laboratory](#)]

Third Generation Photo Recons

The so-called third-generation photo recons are derived from the original Zenit-2 spy satellites and share many characteristics and systems with the manned Vostokspacecraft of the time and the Resurs-F1 civil Earth observation spacecraft of today. The spacecraft are approximately 2.4 m in diameter with a length of 6.5 m and a mass of about 6.3 metric tons. Film is returned (along with the entire camera system) in a spherical 2.3 m diameter, 2.4 metric ton capsule. Within each capsule is a special detonation package (originally 10 kg TNT) which is activated in the event

that a malfunction would prevent a retrieval of the capsule on former Soviet territory ([References 37-39](#)).

In recent years, the launch rate of these battery-powered vehicles with lifetimes of 2-3 weeks has dropped dramatically as more capable, longer lived spacecraft have assumed medium-to-low-resolution reconnaissance duties. Only one third-generation Resurs-T spacecraft (possibly also designated Oblique) was launched from Plesetsk in each of 1993 and 1994 and both were described as fulfilling geodetic and cartographic objectives from high inclination (83 degree) orbits: Kosmos 2260 (22 July 1993) and Kosmos 2281 (7 June 1994). Characteristics of their camera systems are unknown.