ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM: D/CCISCMS/ICS, Via Ames/ISC
Rm. 1225 Ames Bldg.

EXTENSION | NO. DCI/ICS-86-0866 and /1

DATE 23 July 1986

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DD/ICS				JRF 7/25
2. LC/ICS	JUL 24			FYI
D/ICS				Concurrence
3. DDCI				FYI
4. DCI				FYI Signature
5. CCISCMS/ICS Rm. 1225 Ames Bldg.				Reproduction and distribution
6.				Also send the identical letter to counterpart (in HPSCI this time) (see change on distribution)
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

DCI EXEC REG

FORM 1-79 610 USE PREVIOUS EDITIONS

X-Ref: C-402-1R

X-Ref: B-318-1R

DCI/ICS-86-0866/1
23 July 1986

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence
Director, Intelligence Community Staff
Deputy Director, Intelligence Community Staf

STAT
STAT

FROM:

STAT

Director, Community Counterintelligence and Security
Countermeasures Staff

SUBJECT: Unclassified Assessment of the Hostile Intelligence Threat (U)

REFERENCE: SSCI Interim Report on Espionage and Security

1. Attached for your signature is a letter forwarding subject assessment to the SSCI, as requested in reference report on Espionage and Security, undated but received in January 1986.

2. By reference, an extract of which is at left, the SSCI requested an unclassified report on the hostile intelligence threat. This report has received full Intelligence Community review and coordination. Final coordination was received from CIA and FBI as directed by the DDCI. We have designated copies of the report, and your letter forwarding it to the SSCI, for all contributors.

3. Recommend you sign the letter to Senator Durenberger.

STAT

Attachment:
Letter to Senator Durenberger

All portions of this memorandum
are Unclassified

DD/CCISCMS/ICS:dmf: [redacted] STAT

Distribution of DCI/ICS-86-0866/1 (w/att):

1 - DCI
1 - DDCI
1 - D/ICS-DD/ICS
1 - ER
1 - LL/ICS
1 - [redacted] SIG-I Secretariat STAT
1 - ICS Registry
1 - CCISCMS subject
1 - D/CCISCMS chrono

The Director of Central Intelligence

Washington, D.C. 20505

29 July 1986

The Honorable Dave Durenberger, Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Dave:

Forwarded, as requested in your Interim Report on Espionage and Security, is an unclassified assessment of the hostile intelligence threat. The basic information is current through 31 December 1985. Additionally, portions of the report have been updated through 22 July 1986.

We have made a special effort to be as forthcoming as possible in identifying the threat, within the limits of security and good judgment.

Sincerely,

[redacted] STAT

William J. Casey

Enclosure

All portions of this
letter are Unclassified

DD/CCISCMS:dmf: [redacted] (23 July 1986) STAT

Distribution of DCI/ICS-86-0866 (w/enclosure):

0 - Senator Durenberger
1 - [redacted] D/S/CIA STAT
1 - CI Staff/DO
1 - Joseph Tierney, FBI
1 - [redacted] NSA STAT
1 - David Major, NSC Staff
1 - L. Britt Snider, OSD
1 - Robert Krell, OSD
1 - Daniel Carlin, State
1 - Francis Corry, State
1 - [redacted] DIA STAT
1 - A. R. Cinquegrana, Justice
1 - Steven Garfinkel, ISOO
1 - Louis Ritchie, Energy
1 - DCI
1 - DDCI
1 - ER
1 - D/ICS-DD/ICS
1 - LL/ICS
1 - SIG-I Secretariat
1 - ICS Registry
1 - CCISCMS subject
1 - CCISCMS chrono

HOSTILE INTELLIGENCE THREAT

A. SOURCES OF THE THREAT

-- OVERVIEW

Among foreign intelligence services, the Soviet services, the KGB and the GRU*, represent by far the most significant intelligence threat. The Soviet threat is both the largest and, in terms of the ability and intent of the Soviets to act against US interests, the most important. In fact, the activities of the Warsaw Pact and Cuban intelligence services are primarily significant to the degree which they support the objectives of the Soviets. The threat from intelligence activities by the People's Republic of China (PRC) is of a different character. The first arrest of an American citizen on charges of committing espionage for the PRC occurred in 1985. The intelligence activities of another group of Marxist-Leninist states--Nicaragua, North Korea, and Vietnam--pose a lesser, but still significant, threat to US foreign policy interests although these countries have a limited official presence in the United States.

Many other countries, hostile, allied, friendly, and neutral, engage in intelligence operations against the United States. While these activities cannot be ignored, they do not represent a comparable threat. Nonetheless, in 1985, arrests for espionage included US Government employees who were charged with passing classified information to Israel and who had disclosed the identities of CIA personnel and assets in Ghana.

-- Soviet Union, Other Warsaw Pact, and Cuba

The highest Soviet collection priority is accorded to policy and actions associated with US strategic nuclear forces. Other high priority subjects are key foreign policy matters, Congressional intentions, defense information, advanced dual use technology, and US intelligence sources and methods. The Soviets also target NATO intensively, partly as a means to obtain US foreign policy and military information. The Soviets heavily influence the collection activity of the Cuban and Warsaw Pact services, in effect expanding their collection resources through exploitation of ethnic ties and the normally less stringent US controls on the activity of non-Soviets.

The open US society permits the Soviets to acquire much of the information they require through non-clandestine means. Collection is carried out through diplomatic facilities, trade organizations, visitors, students,

---

*The KGB, or Committee of State Security, and the GRU, the Chief Directorate for Intelligence, both operate on a worldwide basis. The KGB maintains internal security in the USSR and, as a secret intelligence service, conducts intelligence collection abroad, as well as covert political influence activities (active measures). The GRU as the military intelligence organization engages only in foreign intelligence.

and other open inquiry. It is aided by Soviet access to computerized US and other Western reference systems, by US Government programs designed to facilitate the legitimate dissemination of information, and by the US Government's inability to exercise stringent controls over foreign visitors and exports.

The spearhead of the Soviet, other Warsaw Pact, and Cuban intelligence collection effort is their official presence in the United States. In 1985, there were about 4,250 diplomats, commercial officials, and other representatives from Communist countries in the United States, 2,100 of whom are from the Soviet Union and the other Warsaw Pact countries. Cuban and other Communist country officials make up the balance. It is estimated that 30 to 40 percent of these officials are affiliated with their country's intelligence services. The Soviet Mission to the United Nations in New York has approximately 275 accredited diplomats; the Department of State has recently mandated a reduction in this number to 170 by April 1988.

The Soviet Union is using effectively UN organizations, particularly the Secretariat, in the conduct of its foreign relations and as a cover for the activities of Soviet intelligence service officers and co-optees. The United Nations employs, worldwide, approximately 800 Soviet nationals as international civil servants, with about 300 of them in New York. Approximately one-fourth of the Soviets in the Secretariat in New York are considered to be intelligence officers, and others are co-optees. Other Soviets in the Secretariat have been tasked to respond to KGB and GRU requests for assistance. The Soviet intelligence services also use their developed agents in the UN to collect information on UN activities; to spot, assess, and recruit American and foreign national agents; to support worldwide intelligence operations; and to collect scientific and technical information on the United States.

The KGB has succeeded in infiltrating its officers into the UN bureaucracy, with some reaching positions of authority. The KGB has held the position of Assistant to the Secretary General since Viktor Lesiovskiy held the post under U Thant. The current Assistant is a KGB China expert. The Soviets take full advantage of UN personnel procedures such as liberal sick leave. This permits KGB UN employees to be absent as often as they desire, enabling them to carry out intelligence activities further abetted by the comparative freedom of movement enjoyed by UN employees.

Within the Soviet services, GRU personnel are targeted primarily against military and scientific and technical information while KGB personnel are assigned to one of four operational departments or "lines"--Scientific and Technical (X), Political (PR), Counterintelligence (KR), or Illegals Support (N). S&T personnel specifically target US advanced technology. Often, clandestine collection of S&T information is preferred over buying or developing technology because it is cheaper and provides the best short-term results, although there is a risk factor in the theft. KGB Line PR personnel target governmental policy information and, frequently, seek to advance Soviet objectives via contacts with persons of influence or through covert activities. Line KR officers have the security responsibility for preventing defections of Soviet personnel and particular concern for penetration of the

US Intelligence Community, although all lines are tasked with this important function as a matter of general concern. Illegal support personnel comprise a small group involved with the operation of illegals--intelligence officers and agents infiltrated into the United States under false circumstances to operate clandestinely, having no overt connection with the Soviet Union.

The Soviets aggressively seek information on Western technology to avoid technological surprise and to improve their economy and weapons systems. Indications are that their acquisition efforts are becoming more selective than in the past, and that future collection will concentrate on technology which is used either in developing and producing US weapons and military support equipment or which is specifically needed in Soviet industry for USSR weapons systems. The methods used to acquire technology will depend largely on the cost and the risk involved. It is likely that increased controls on trade with the Soviets and on Soviet visitors and official personnel will cause more changes in Soviet collection techniques. Even greater use of Warsaw Pact services as collectors, for example, is probable. More use of clandestine methods to acquire technology is also likely, when it cannot be obtained in other ways.

The extent of the hostile intelligence threat in the United States is furtner illustrated by the fact tnat the intelligence services of the USSR, other Warsaw Pact countries, and Cuba have some 130 diplomatic, commercial, and other entities in the United States which can be used as cover for clandestine collection activities. The commercial presence of the Soviet Union and other Communist countries in the United States has been shown to afford their intelligence collectors wide opportunities. These commercial establishments (such as the USSR's Amtorg and Intourist; the Polish Polamco; and similar East German, Czechoslovak, and other East European entities), through their legitimate activities, have access to Americans in business, industry, and government who are potential targets for agent recruitment. Economic data and advanced technology are the primary interests of the hostile collectors operating under commercial cover.

In addition to the threat posed by their official establishments, these intelligence services have infiltrated intelligence collectors into the United States among the thousands of exchange students, commercial and cultural visitors, tourists, and ship crewmen who enter this country each year. Further, in recent years, a number of intelligence agents of the USSR, Cuba, and other countries have been uncovered among the flood of immigrants into the United States from Communist countries. While not all of these agents are considered classic illegals, investigations have determined that many have been sent with intelligence missions. The deep-cover illegals dispatched to the United States in the emigre flow and through other means by the Communist intelligence services represent a particularly perplexing problem because of their completely clandestine manner of operation.

-- People's Republic of China

The PRC has several intelligence services whose personnel are represented among the approximately 1,500 Chinese diplomats and commercial community located at some 70 PRC establishments and offices in the United

States. They also have some access to the approximately 15,000 Chinese students and 10,000 individuals arriving in 2,700 delegations each year. There is, of course, a large ethnic Chinese community.

The implications of the intelligence activities of the PRC are markedly different from those of the Soviet Union and its surrogates. The forces of the Warsaw Pact are arrayed against those of NATO; and the Soviet Union's expansionist policy poses a current and continuing global challenge to the United States and its allies. The PRC is not now in strategic competition with the United States. Indeed, the United States has fundamental interests in maintaining friendly relations with the PRC and in promoting its modernization, to include selective upgrade of its military defensive capabilities. Collection priorities of the two major communist powers reflect their respective foreign policies: the Soviet services with urgent requirements with respect to US plans, intentions, and capabilities, as well as technology; the PRC services concentrated primarily on advance technology not subject to release to further PRC modernization in the 1990s and beyond. There is evidence that the PRC's traditional, careful, and patient development of assets has resulted in the establishment of a large human intelligence infrastructure in the United States.

-- Other Countries' Threats

Other countries conduct human intelligence collection in the United States, both overt and clandestine. Their targets include the same range of interests as those of the Soviets, et al, including high technology and political, military, and economic policies and intentions which might impact in an adverse manner on the particular country.

Among the more common activities of foreign intelligence services in this country are attempts to penetrate emigre communities. A large number of expatriate political and ethnic groups in the United States are viewed as a threat by authorities in the former homelands. The list includes Libyans, Croatians, and Iranians, to name only some. From a national security viewpoint, these activities are of less significance than those of the USSR and its allies, although they are clearly in violation of US sovereignty and may have an effect on US foreign policy. Foreign intelligence services also target ethnic groups in the United States, directly or through front organizations, to influence US decisions on foreign aid, trade agreements, and other issues where the foreign government has valid interests.

B. HUMAN TARGETS

-- Espionage

During 1985, a total of 11 people were arrested and accused of spying for either the Soviet Union, its allies, or other countries. Ten of the 11 have since been convicted or pleaded guilty to espionage charges. Also, 11 persons who had been arrested on espionage charges during 1984 were subsequently convicted. Between 1 January 1981 and 31 December 1984, 23 arrests were made; from 1 January 1976 to 31 December 1980, 11 people were

arrested; between 1 January 1966 and 31 December 1975, there were six espionage arrests.

The spy of the 1980s has been described as a new breed, motivated more by greed than by ideology. However, the cases uncovered in 1985 demonstrate that this is not always the case--political beliefs, intrigue, job dissatisfaction, and alienation also appear to have been reasons for engaging in espionage. Moreover, nine of the 11 noted above volunteered their services to the other side.

While in the past most espionage cases in the United States have involved the Soviet Union or other Warsaw Pact countries, three 1985 arrests were markedly different. One was the first arrest of an American on charges of spying for the PRC. Larry Wu-Tai Chin, a retired CIA foreign media analyst, was charged and convicted of spying for the Chinese. He was a "plant" who received intelligence training before his employment by the US Army in 1943. In a second case, charges of espionage were made against Sharon Marie Scranage, a CIA clerk who furnished a Ghanian national the names of CIA employees and assets in Ghana. Scranage was subsequently convicted. In the third case, Jonathan Jay Pollard, a civilian intelligence analyst with the Naval Investigative Service, pleaded guilty to criminal charges that he had illegally passed classified documents to Israel.

The case involving John Anthony Walker, Jr.; his son, Michael Lance; and his brother, Arthur James, was long-running and caused significant damage to US national security. Walker admitted to having spied since 1968, and his information may have enabled the Soviets to read some of the US Navy's most secret messages to the fleet from the 1960s to the time of his arrest. His espionage activities have possibly reduced the US lead in anti-submarine warfare. The three Walkers have been convicted and a close friend, Jerry Alfred Whitworth, at this writing, is on trial for espionage.

Ronald William Pelton, a former NSA communications specialist from 1965-1979, was convicted of selling the Soviets information about a highly classified US intelligence collection project targeted at the Soviet Union. Edward Howard, a former CIA officer, is accused of selling intelligence secrets to the Soviets based on his knowledge of CIA operations in the Soviet Union. Howard, who resigned from CIA in 1983, disappeared from his home in New Mexico in September 1985.

Soviet intelligence efforts also include active programs outside the United States against US Government personnel and businessmen. Even those recruited agents who live in the United States are frequently met in third countries to avoid US domestic counterintelligence. KGB residencies emphasize that the principal targets are American embassy employees, particularly code clerks and other communications personnel with access to classified information. Other targets include American journalists, businessmen, and scientists who can furnish sensitive technology information, and students with job prospects in sensitive positions for long-range development. Of concern are reported instructions from KGB Headquarters to its residencies that the KGB connection of some Soviet embassy officers is to be made known so that a

US official considering volunteering his services would be aware of the right person to contact.

US military installations and personnel abroad continue to attract major Soviet intelligence interest, both to gain potential access to military plans and to acquire sensitive technical data. There have been some recent instances in which the Soviets have contacted and attempted to recruit military personnel who have discussed financial or other personal problems during long distance telephone calls to the United States from their overseas posts.

The widespread use of foreign nationals in US embassies and consulates compounds the problems faced by US intelligence in most hostile countries. Over 9,800 foreign nationals are so employed for a number of reasons, including cost considerations. Despite their value in dealing with local government organizations because of their language fluency and understanding of local customs and regulations, the threat to US security has been recognized. Even when barred from restricted areas in the official US establishment, foreign nationals can glean information useful to the hostile security service, such as personal data on pay, movements, assignments, telephone calls, and vulnerabilities to recruitment.

The employment of foreign nationals in US establishments in the Soviet Union and other Eastern European countries, as well as in numerous other countries where the Soviet Bloc has influence, affords hostile security services the opportunity to conduct a variety of technical penetrations. Offices, residences, and cars are all vulnerable to the planting of audio devices by foreign nationals with access, legitimate or otherwise, to the US target.

Although all high technical threat posts have eliminated the access of foreign nationals from the vicinity of classified work areas, there remains a serious problem of common walls with uncontrolled adjacent areas from which technical attacks can be mounted. Offices and residences are also vulnerable to planted devices when access by foreign nationals is not properly monitored and routine technical countermeasures are not employed.

The US Embassy in Moscow poses particular problems. Soviet nationals operate the carpool, including making mechanical repairs; staff the canteen where embassy personnel gather for food and conversation; and, until recently, operated the telephones. Approximately 200 Soviets are employed at the embassy, contrasted to fewer than a dozen Americans in the Soviet establishments in Washington.

Soviet intelligence continues to successfully target foreign nationals employed by US establishments abroad. The foreign nationals are used by the KGB to obtain assessment information on possible recruitment targets among the American personnel (e.g., those with money, family, drinking, or drug problems). The Soviets strictly limit the use of local hires in their own embassies, apparently concerned that if they can succeed, so can US intelligence.

Third countries are commonly used by the Soviets as meeting places with recruited agents. Vienna, Austria, for example, was used as the meeting place for John Walker, who was convicted of spying for the Soviets.

Both as a command structure and as part of each member country's governmental structure, NATO is also a high priority target of the Soviet Union and other Warsaw Pact countries. These intelligence services place a very high priority on the recruitment of human assets with all levels of access to NATO classified information; based on what is known of Soviet modus operandi in general, it is also presumed that a similar effort is made to effect physical penetration of NATO installations wherever they exist. Recent arrests in West Germany and Greece are indicative of the successes the USSR is having in targeting US and NATO classified weapons systems.

The Chin case is an example of one of the PRC intelligence services' recruitment techniques. Chin, who admitted to passing classified information to his PRC contacts, operated in place for a very long period of time following his recruitment as an agent. He admitted to suggesting a recruitment approach to another ethnic Chinese CIA employee. To use a recruited agent as a talent spotter of other potential agents among his peers is a standard intelligence practice employed by most intelligence services.

-- Counterintelligence

Over the past several years, the KGB has stepped up its efforts to penetrate the CIA. The KGB recognizes the difficulty of this tasking in view of the lack of opportunities to approach CIA officers. Greater use of recruited agents, either local or third country nationals, who have easier access to Americans abroad, may be the result. The KGB has not lessened its efforts to penetrate the FBI, but apparently believes it may be less difficult to attack CIA personnel who are not on their "home turf."

State Department employees, military personnel, and other government employees with access to classified information continue to be actively targeted, as are personnel of US allied governments who have access to classified US foreign and security policy information or US weapons and military doctrine.

Additionally, hostile intelligence services try to gain access to our communications or office equipment in order to "read our mail." In 1978, security officers discovered that a shipment of IBM Selectric typewriters destined for the US Embassy had been shipped from Antwerp to Moscow by a Soviet trucking line, thus affording the Soviets access to the typewriters. Fortunately, the equipment was returned to the United States before being placed in service. Subsequently, the Soviets again gained access to several similar IBM machines. These typewriters, like their 1978 predecessors, were shipped to the Soviet Union by unaccompanied commercial means. When discovered, the technical compromise of these typewriters ended a Soviet operation of some duration.

-- Technology Transfer

The Soviet drive to achieve technological equality with the United States and other Western countries has required the USSR to commit enormous resources to the effort. As a result, the Western lead in many key technological areas has been reduced. The clandestine Soviet program to acquire illegally Western technology continues to be a massive undertaking. Information from the past few years indicates that the success in this program has had serious economic and military consequences for the United States.

Moscow has devised two programs to obtain Western technology. The first, under the Military Industrial Commission (VPK) of the Presidium of the Council of Ministers, seeks to obtain military and dual-use hardware, blueprints, product samples, and test equipment to improve the technical levels and performance of Soviet weapons and defense manufacturing equipment. By adapting design concepts from the acquired hardware and documents, the Soviets reduce their own research and development costs. In the early 1980s, more than 3,500 requirements were levied by the VPK each year, with about one-third satisfied. Some 60 percent of the most significant acquisitions (to the Soviets) was of US origin, although not necessarily collected in the United States. Nearly half of the up to 10,000 pieces of military hardware and 20 percent of the 100,000 engineering and research documents the USSR acquires annually (worldwide) are used by the Soviets to incorporate Western technology into their military research projects. Most of these documents, about 90 percent of which are unclassified, are patented or copyrighted proprietary information illicitly obtained. The R&D cost savings to the Soviet Union is believed to be enormous--the Ministries of Defense Industry and Aviation Industry alone are estimated to have saved half a billion rubles (the 1980 dollar cost of equivalent research would be $800 million) between 1976 and 1980. The saving figures may be biased since the ruble figures probably reflect operating cost.

The GRU is believed to have satisfied considerably more VPK requirements than the KGB for defense-industrial activities such as the communications equipment industry and various machine building, and other industries. This success is attributed to the GRU's greater scientific orientation, a wider variety of technology-related cover positions, and other factors. The approximately 1,500 GRU officers serving outside the USSR have technological/scientific collection as an integral part of their responsibilities.

The KGB First Chief Directorate's Line X has nearly 300 officers on foreign assignment operating under cover of Soviet embassies, trade and commercial organizations, as members of exchange groups, and as employees of international organizations (the United Nations, for instance). The largest KGB contingents are believed to be in New York, Bonn, Cologne, Vienna, and Tokyo. Until the French mass expulsion of 47 KGB officers in 1983, Paris was counted as one of the larger KGB establishments, as was London before the 1985 expulsion of a large number of Soviet officials. The KGB, more so than the GRU, relies on the collection capabilities of other Warsaw Pact intelligence services, notably those of East Germany, Poland, Bulgaria, and Czechoslovakia. In recent years, these services, especially the Polish, have

had some significant coups--the 1983 case of James Harper, Jr., a California "Silicon Valley" engineer who worked as a Polish agent in the late 1970s and early 1980s, and the case of William Bell, the Hughes Aircraft engineer who was arrested in 1981. The success of East European services can be attributed to the Western misperception that Poland, Czechoslovakia, etc., are less of a threat than the USSR; East European nationals operating in most Western countries have fewer (or no) travel restrictions and, in some cases, find it easier to work in a Western cultural and commercial environment.

The 1,500 high-technology companies in the California area known as "Silicon Valley" constitute the largest collection of electronics and computer manufacturers in the United States. For example, ITT, Ford Aerospace, Teledyne, and Hewlett-Packard are among the US defense contractors in the Valley who are primary Soviet targets. Soviet trade or scientific representatives travel to California about four times a month in delegations ranging from two to 10 people, and the Soviet San Francisco Consulate has a staff of 41 persons. Based on the widely accepted figure that intelligence officers comprise 30 to 40 percent of the personnel in each Soviet establishment, and that the same percent of the personnel in a Soviet visiting delegation are intelligence officers and/or co-optees, the KGB has the means to target "Silicon Valley" and employees of the industries there.

The second program, managed by the Ministry of Foreign Trade and the KGB/GRU, seeks, through trade diversions, to acquire relatively large amounts of dual-use manufacturing and test equipment for direct use on production lines. This program attempts to obtain export-controlled microelectronic, computer, telecommunication, machining, robotic, diagnostic, and other sophisticated equipment. This second program utilizes both legal and illegal means to achieve success.

Major Soviet collection efforts are targeted at microelectronics fabrication equipment and computers; nearly one-half of detected trade diversions fall into these categories. The acquisition of much of the information and, in some cases, the hardware, concerning these high-technology areas is not particularly difficult. Many US Government agencies make information available to the public and it is, therefore, accessible to the Soviets and their surrogates. The Soviets and professional trade diverters hired by them can use dummy firms, false end user certificates, diplomatic pouch smuggling, and export license falsifications to acquire equipment and other hardware. Many advances in Soviet microelectronics have been made possible by the illegal acquisition of equipment from the West. The result has been a marked reduction in the Western technological lead of about 10 to 12 years a decade ago to about half that today.

Richard Mueller, a West German citizen, has been involved in illegal technology acquisition for the Soviets for more than a decade. Using dummy and front firms, he has diverted advanced computers and microelectronics equipment of significant value to the Soviets. Mueller was the moving force in the 1983 attempted diversion to the USSR of several US Digital Equipment Corporation VAX computers which would have assisted the Soviets in computer-aided design applications for microelectronics fabrication. Recent information reveals Soviet interest in the Cray family of supercomputers and

efforts to access these computers both in the United States and abroad. The more advanced Soviet computers are believed to be much slower than the Cray, and any Soviet access to Cray machines could lead to another situation similar to that in which the Soviets acquired IBM documents enabling them to produce a very versatile computer that is a functional, although less capable, duplicate of the IBM 370.

-- Open Source Exploitation

The task of responding to VPK technology collection requirements is made easier for the KGB and GRU by the openness of US society--both government and industry. The Soviet intelligence services are aided by certain of the surrogate services of other Warsaw Pact countries, which openly acquire large amounts of information of value to Soviet engineers, economists, scientists, military managers, and many others. A Czechoslovak, Polish, or other East European official is frequently able to contact US companies without arousing the suspicion that contact by a Soviet official would occasion.

Commercial data bases provide a wealth of information--the Commerce Department's National Technical Information Service (NTIS), NASA, the Government Printing Office, the US Geological Survey, and the General Services Administration are readily accessible. NASA, for example, from the mid 1970s to the early 1980s, was the source, in the form of unclassified documents and contractor studies, of the Soviets' best information in the aerospace area. The information obtained concerned airframe designs, materials, flight computer systems, and propulsion systems. NTIS has been a productive source of data dealing with design, evaluation, and testing of US weapon systems. Unclassified electronic data bases are regularly interrogated by the Soviet Institute for Automated Systems of the Academy of Sciences.

The Soviets and their allied intelligence services have for many years been regular attendees of scientific, technical, and industrial conferences in the United States and abroad. The Soviets considered some of the information obtained from these conferences to be among the most significant contributions to their military projects. The VPK identifies those having the most potential--and, in recent years, these have included the International Radar Conference, Conference on Integrated Optics, and the Conference of the Aerospace and Electronic Systems Society of IEEE.

In addition, the Ministry of Foreign Trade and academic-related collectors contribute to Soviet open source exploitation of Western information availability. The Ministry of Foreign Trade has hundreds of trade organizations and companies around the world. KGB and GRU officers operating under cover of these establishments collect quantities of data openly in addition to that derived from their covert operations. The Ministry, as an independent collector, helped meet about 15 percent of all fully satisfied VPK requirements during the late 1970s and early 1980s. It specializes in acquiring microelectronics, manufacturing equipment, and communications dual-use products. The Soviet Academy of Sciences, the GKNT, and the State Committee for Foreign Economic Relations not only collect overt information for non-defense industries, but also covert data in response to VPK tasking for military research projects. Some 2,000 Soviets come to the United States

each year under the auspices of these and other Soviet agencies. The number of US universities and institutes targeted by the Soviets increased from 20 to over 60 from the late 1970s to the early 1980s. The additions include MIT, Harvard University, Rensselaer Polytechnic Institute, University of Michigan, and Carnegie-Mellon, to name but a few.

-- Active Measures

"Active measures" and "disinformation" are the Soviet covert action operations designed to implement Soviet policy goals by attacking US policy and to promote a positive image of the Soviet Union. They remain major weapons in the Soviet strategy to discredit and deceive the United States and its allies. Soviet use of front groups, influence agents, and media manipulation continues at a high level. There is evidence of a major Soviet active measures campaign against US development of the Strategic Defense Initiative (SDI). The Soviets are making every effort to convince a world audience that SDI will destabilize an already precarious superpower armaments balance.

While the active measures emphasis is in the Third World countries, where the Soviets play to a less sophisticated audience, more subtle use of the techniques involved has been necessary in furthering Soviet objectives in the West. During July 1984, the Soviet Union began a widespread disinformation campaign to discredit the Los Angeles Olympic games and bolster worldwide support for their boycott of them. This "active measures" campaign featured three forged documents threatening Third World athletes with bodily harm if they participated in the Olympic games. Shortly after their discovery, former Attorney General William French Smith announced that the letters were KGB forgeries and part of a major Soviet disinformation effort. It has been determined that these documents fit the pattern of other Soviet forgery operations and were part of the overall Soviet "active measures" campaign to discredit the Reagan administration and its handling of US-USSR relations.

Soviet active measures directed at US allies, such as in West Germany and Japan, are designed to sow distrust of American policies and to intensify financial and commercial rivalries by holding out the promise of favorable terms to the business communities in both countries. These are all part of the Soviet campaign to split the United States from its friends.

Currently, the Soviets appear to be employing active measures in South Asia in an effort to depict the United States as interferring in the affairs of India, Pakistan, and Bangladesh. The media in all three countries have consistently carried stories to this effect. One long-running disinformation ploy concerns alleged attempts by CIA to aid separatist movements in India, thereby splitting the country to US economic advantage. Discrediting US intelligence agencies, particularly the CIA, has long been an important objective of Soviet active measures.

C. TECHNICAL THREATS

-- Interception of Communications

The Soviet electronic monitoring effort represents a significant worldwide threat to US military and civil telecommunications. This threat derives from large collection facilities which are operated in the Soviet Union, as well as in other countries around the world, such as Cuba. The Soviets also maintain a fleet of intelligence collection vessels which operate worldwide--including off both coasts of the United States. The latest of these vessels has been built from the keel up specifically for this role. The Soviets also use merchant ships and possibly commercial aircraft to perform collection operations against targets of opportunity.

A serious threat is posed by the Soviet intelligence collection facility located at Lourdes near Havana, Cuba. Established in the mid 1960s, the site has steadily grown to its present size of about 2,000 technicians, and represents the most sophisticated collection facility outside the Soviet Union. From this key listening post, the Soviets are able to monitor US domestic satellites, US military and merchant shipping communications, and US space program activities.

Evidence of the seriousness of the threat to electronic communications was emphasized by the issuance in 1985 of National Security Decision Directive No. 145 which concluded that "the compromise of US information, especially to hostile intelligence services, does serious damage to the United States and its national security interests."

The technology to exploit US electronic communications is widespread, and many foreign countries use it extensively. Certain terrorist groups and criminal elements also have the capability. Currently, more than half of all telephone calls in the United States made over any distance are transmitted by microwave. Calls which the caller believes to be on land-line circuits (unsecured) may be automatically switched to microwave. The Soviet diplomatic facilities at the Riverdale complex in New York City, at the consulate in San Francisco, and at the new Mt. Alto embassy in Washington all occupy high ground, thus providing superior opportunities for communications intercept. The "Silicon Valley" concentration of high technology centers and the government's sensitive facilities in Washington and New York are at risk of intercept because of these Soviet sites.

-- Other Forms of Electronic Surveillance

The Soviets have a long history of electronic attacks on the US Embassy in Moscow, dating back to the 1950s when a replica of the Great Seal of the United States in the embassy was found to contain an audio device. In the late 1970s, a Soviet antenna was found in the chimney of the chancery. Common wall facilities are particularly vulnerable to electronic penetration.

As noted previously, foreign nationals, with access to US embassies and other establishments abroad, provide a means whereby hostile intelligence services can make electronic penetrations.

-- Penetration of Computer Systems

The hostile intelligence threat to US computer systems is magnified by the enormous growth in the number and power of computers and the vast amount of data contained in them. The GSA has estimated that the number of US Government computers has increased from 22,000 in 1983 to over 100,000 in 1985. The increase in the number of computers in use in industry, business, and other private sectors has been equally staggering.

Computers and computer software are high priority items of both the VPK's and the Ministry of Foreign Trade's technology acquisition programs by legal or illegal means. The Soviet and other Warsaw Pact intelligence services have also obtained information concerning the methods used in the West to provide computer security, and constantly seek more knowledge. Over the past decade, the Soviets have acquired over 300 different types of US and other Western computer hardware and software which has enabled them to develop the technical ability to penetrate at least some US automated systems. The Soviets are making a concerted effort to access state-of-the-art computers like the Cray supercomputers.

-- Collection of Emanations from Equipment

The discovery of sensing devices in several typewriters in the US Embassy in Moscow and Consulate in Leningrad, noted previously, demonstrate the Soviets' technical ability to electronically penetrate such equipment. Placing the sensors required access to the typewriters, either while they were in the process of shipment or undergoing maintenance while out of US control.

The Soviets' technical threat continues to grow as their advances in microelectronics increase. Compounding the threat is the hostile environment in which many US establishments abroad must operate. The opportunity for technical attack is far greater in the Soviet Union and other Warsaw Pact countries than in friendly or neutral countries. In many countries where US facilities share building space with other uncontrolled offices, the potential threat is maximized. New construction or remodeling involving US establishments where local laborers and materials are used also create vulnerabilities to technical penetration.

-- Imagery

Intelligence collection against the United States and US interests worldwide using photographic means, or imagery, is carried out principally by the Soviet Union (with some assistance from its Warsaw Pact allies and Cuba). The Soviet imagery effort is mainly conducted from spaceborne and airborne platforms. The continued proliferation of Soviet satellites has given the USSR the concomitant capability for increased photoreconnaissance of its most obvious targets, US and NATO strategic and tactical military forces, and crisis situations anyplace in the world. In addition to these uses of photoreconnaissance, the Soviets employ it to conduct earth resources surveys for economic and agricultural data.

Soviet spaceborne satellite reconnaissance capabilities are supported by the capability of military and civilian aircraft to collect photographic intelligence. The potential value of airborne reconnaissance conducted by the Soviet airline Aeroflot, which, in April 1986, resumed operations to the United States, and other Warsaw Pact national airlines' flights remains of concern. These Communist country overflights in the United States are under the jurisdiction of an FAA committee.

The Soviets continue to pursue their manned space programs. In February 1986, they launched a new type of modular space station, the MIR, replacing the older SALYUT-type modules. The MIR, as did the SALYUT, gives the Soviets the capability to perform a number of functions in space, including the use of cosmonauts to augment their other reconnaissance and surveillance efforts. The apparent military usefulness of their manned space program has been indicated in the Soviet announcement that "earth surface surveys" have been conducted; however, no photographs were ever published.

The seriousness of the imagery collection threat posed by the Soviets and Bloc overflights in the NATO area can be illustrated by two examples. In March 1985, Norway banned or restricted Soviet and Bloc passenger airplanes from several airports on the basis that they were conducting electronic surveillance. Bulgarian aircraft were specifically mentioned as having departed from scheduled routes to overfly sensitive areas. In West Germany, some 1,500 Soviet Bloc overflights occurred in a three-month period in 1985, offering a tremendous opportunity for both electronic and photographic reconnaissance.

In summary, the intelligence collection threat posed by the activities of the Soviet Union, its Warsaw Pact surrogates and Cuba, and other countries must continue to be of concern to the national security interests of the United States both in this country and abroad. The techniques employed by hostile intelligence services range from the use of human agents to the most sophisticated technical means. The open nature of US society makes the task of the foreign intelligence officer easier than in most countries.