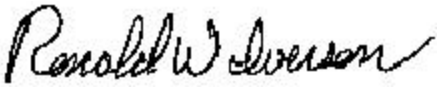
Technology Collection Trends in the U.S. Defense Industry 2002

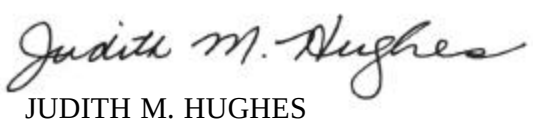
Foreword

The Defense Security Service (DSS) is charged with the mission of assisting cleared defense industry in the recognition and reporting of foreign contacts and collection attempts as outlined in paragraph 1-302.b of the National Industrial Security Program Operating Manual. This sixth edition of Technology Collection Trends in the U.S. Defense Industry is a direct result of cleared defense industry reporting pursuant to this program.

Designed for use by security officials, cleared contractors, intelligence professionals and DoD policy and decision makers, this report summarizes prominent topics associated with foreign targeting and collection attempts directed at defense industry including what is targeted and how the targeting is accomplished. DSS also provides this publication via DSS web page www.dss.mil, at its Security Library, to maximize threat awareness and improve security practices in cleared industry. DSS intends for this publication to enhance counterintelligence and security integration by providing information and examples that apply to security risks throughout defense industry. This goal is tied to the ultimate goal of this publication: threat awareness and related research and technology protection from foreign collection attempts directed at U.S. defense industry.



RONALD W. IVERSON
Deputy Director for Industrial Security



JUDITH M. HUGHES
Deputy Director for Personnel Security Investigations

Contents

This Defense Research and Technology Horizontal Protection publication was prepared by Elisa Cruz, Peter DeCesare, Rebecca Morgan, Susan Porell, Gene Smith, and Bill Wrigley. Comments and queries are welcome and may be directed to the DSS Counterintelligence Office at 1340 Braddock Place, Alexandria, VA 22314-1651. Special thanks to Annette Frye Gunter for graphic design and layout, Laurie Dungan and Mamie Hill, Technical Editor, ACIC, for editorial support, and Mark Mooney for final editing.

Introduction

This sixth annual study is the Defense Security Service (DSS) counterintelligence (CI) tool for security professionals. The data presented in this study is based solely on reports of suspicious foreign activity provided by DSS Industrial Security Representatives and DSS Special Agents. These reports are composed of information provided by U.S. cleared defense contractors and industry personnel who have experienced suspicious foreign activity. This publication provides general information and conclusions that help cleared company personnel and DSS personnel recognize and responsibly report suspicious foreign activity so DSS can assist cleared contractors in enacting responsive, threat-appropriate, and cost-effective security countermeasures (SCM). Numerous government agencies also use this reported information to analytically confirm or deny assessments of U.S. technology targeting, to identify suspicious foreign entities, and to strengthen and supplement their investigative missions.

Key Judgments

Foreign collection attempts against cleared contractors increased significantly during the fiscal year 2001 and will continue to increase in the near future. U.S. militarily critical technologies remain the most sought after in the world, with more countries and foreign entities attempting to obtain high-technology weapons components through various means. Collection attempts increased exponentially with worldwide Internet availability and web site usage by cleared contractors. This increase was reflected in cleared contractor reporting, which reached an all-time high of 717 suspicious contact reports. Availability of product information, anonymity of requestors, and increased demand for high-technology weapon systems require that U.S. security personnel and the U.S. cleared contractors remain vigilant in protecting these products.

The weapons systems of today and those of the future command high-technology information systems for enhanced communications, targeting, and battlespace control. The U.S. cleared contractor remains the forerunner in design and development of these much-needed systems. Longer-range, multiple reentry vehicles (MRVs) require information systems for effective deployment. Foreign attempts to collect against U.S. space and energetic materials technologies increased significantly as more powerful nations obtain long-range ballistic missiles and develop intercontinental offensive weapons systems.

The increased demand for defensive systems, such as coastal defense radar technologies and shallow-water rigid inflatable boats for patrol of claimed territorial waters and navigable rivers was reflected in overt attempts to acquire these systems. While more countries now include submarines in their order of battle, the emphasis for foreign procurement of marine systems remains in coastal defense and shallow-water technologies vice deep-water systems such as submarines.

Executive Summary

Reporting Trends

In 2001, DSS received 717 suspicious contact reports from cleared contractors and DSS Industrial Security Representatives and Special Agents. This represents a significant increase over any previous reporting year. DSS associates this rise with heightened threat awareness by DSS field personnel, cleared

defense contractors, and increased Internet use. DSS also observed a leveling off in the categories of reporting. In the past, the recognition of suspicious activities (and the reporting thereof) was often focused on a few countries or particular Method of Operation (MO). As threat awareness sharpened, cleared contractors began to recognize, and to report, suspicious contacts across a broad spectrum of foreign actors and foreign MOs.

Country Trends

DSS received reports of suspicious activities concerning interests associated with 75 countries in 2001. The number of reported countries has increased steadily during this time, from 37 reported foreign countries in 1997 to 47 in 1998, 56 in 1999, 63 in 2000, and now 75 in 2001. These countries represent every region of the globe and the entire spectrum of social and political environments. In 2001, as in prior years, reports to DSS indicate the majority of countries targeting cleared contractors are those with economies and technology industries that are competitive with the U.S. with varying degrees of military capabilities. For the most part, these countries are seeking general technological advancement.

Technology Interest Trends

In 2001, the majority of targeted weapons systems and technologies were associated with Defense programs and were covered by the International Traffic in Arms Regulations (ITAR). As noted in the past, foreign entities continue targeting weapon components, developing technology and technical information more intensely than complete weapons systems and military equipment. Suspicious activity reports received in 2001 included every militarily critical technology category. For the 2001 report, DSS expanded the analysis of the most frequently targeted technology categories. This effort is intended

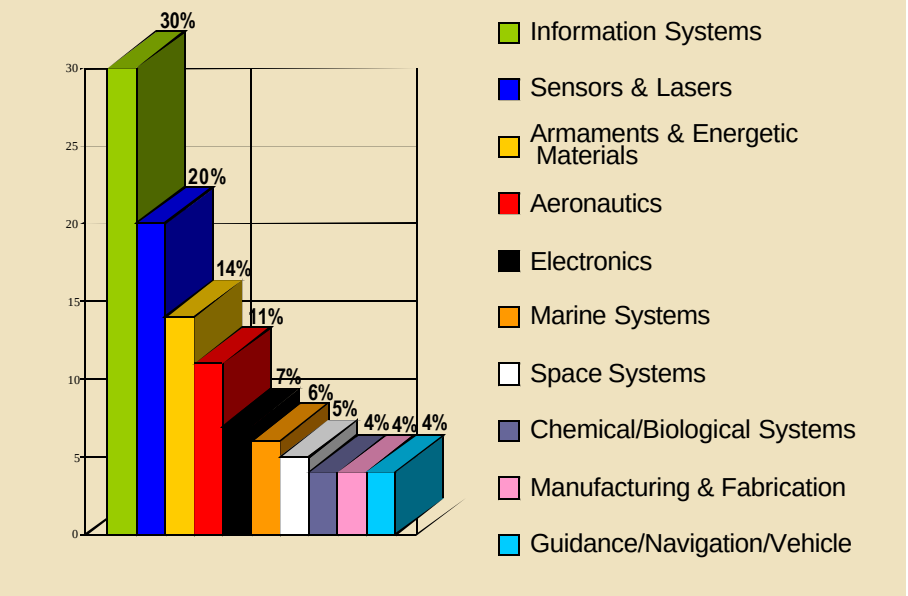
Table 1

Technology Interest Trends

Military Critical Technology List	Percentage Targeted
Information Systems	30%
Sensors and Lasers	20%
Armaments and Energetic Materials	14%
Aeronautics	11%
Electronics	7%
Marine Systems	6%
Space Systems	5%
Chemical/Biological Systems	4%
Manufacturing and Fabrication	4%
Guidance/Navigation/Vehicle	4%

Figure 1

Technology Interest Trends



to enhance DSS field personnel and cleared contractor understanding of why a foreign entity chooses to target a particular technology and the most effective means for countering the action.

Most Frequently Reported Technology Targets

In order of frequency, those technologies generating the most foreign interest in 2001 included information systems, sensors and lasers, armaments and energetic materials, aeronautic systems, and electronics. This ranking is similar to previous years and has varied little over time. However, the extent of foreign interest and collection methodology employed against these specific technologies varies dramatically, from a passive request to sophisticated collection activities using various MO.

Most Frequently Reported Methods of Operation (MO)

MOs are the techniques employed by a foreign entity against a given target to collect intelligence, scientific, and technical information. MOs associated with potential collection efforts in 2001 are as follows, ranked in order of frequency of occurrence:

- Requests for scientific and technological (S&T) information
- Attempted acquisition of U.S. technology/company
- Soliciting and marketing of services
- Targeting of U.S. legal travelers travelling abroad
- Inappropriate conduct by foreign entities during visits to U.S. facilities
- Exploitation of existing relationships

including joint venture or research
- Exploitation of Internet (hacking)
- Targeting at international conventions, seminars, and exhibits

Requests for S&T information was the most frequently used collection method employed by foreign interests in 2001. While foreign interests employed a variety of methods, these methods are consistently similar to those reported from 1995 to 2000. Foreign entities may use combinations of methodologies or invent new methodologies, as a particular situation demands. Although these practices can sometimes make it difficult to assess the methodology used by a foreign entity in a particular matter, in an effort to achieve a high standard of analysis, DSS reviewed the MO categories assessed to each reported incident in 2001. DSS refined each category and, ultimately, arrived at a "pure" MO for each reported incident. Information regarding this process, as well as foreign collection methods and their frequencies, is described in the Foreign Collection Methods section of this publication.

Reporting

DoD Directive 5240.2 requires DSS to assist industry in recognizing and reporting suspicious activity including foreign contacts and collection attempts. Cleared companies and DSS responded well in 2001, as in previous years. This active response continues a trend of increased awareness and reporting. The following criteria are most often cited in assessing potential foreign collection efforts:

- Technology is classified/export-controlled
- Information has a national defense/ military application
- Redundant requests from a country for each technology target
- Identifying consistent patterns across government agencies reporting on collection efforts by that country
- Foreign entity is affiliated with foreign government defense organization
- Request/offer is from an embargoed country
- Possible front company and known technology target
- Foreign country is associated with diversionary practices

All threat information is evaluated in the context in which it takes place. DSS evaluates the criticality of the requested information: whether or not the technology exists at the cleared defense contractor facility, association of the foreign collection method to those reportedly used by foreign intelligence services, history of previous suspicious activity by the foreign entity, and access of the contacted, cleared employee to the requested information. Only then can DSS apply a value judgment to the threat information and, subsequently, more rigorously analyze the information if warranted. Foreign targets of interest to DSS include any technology that is classified, requires an export license, and is listed in the ITAR or Military Critical Technology List (MCTL).

MOs of interest to DSS include economic and industrial espionage activities related to intelligence, scientific, or technical collection operations, which normally involve a complementary set of activities. These activities vary based on a nation's culture, political system, business practices, and resources. These MOs include, but are not limited to, the following:

- Request for information
- Exploitation of visits including violation of foreign visit protocols
- Exploitation of existing relationships including joint research
- Acquisition of U.S. companies or technologies
- Hacking
- Targeting cultural commonalties
- Targeting at international conventions
- Solicitation and marketing of services
- Exploitation of foreign employees
- Targeting former employees

Submitted incident reports continue to emphasize the importance of using company Facility Security Officers (FSOs) as the central coordination point for each cleared company and each cleared employee. By experience and repetition, FSOs ensure timely and comprehensive review, recognition of suspicious indicators, and reporting of suspicious activity. The FSO, when appropriate, can be a force multiplier. Whether for investigation or analysis, reporting helps educate industry, security, and CI professionals about foreign collection methods employed against U.S. industry. The DSS Office uses the information provided by IS Representatives for further analysis. Therefore, FSOs may be able to help identify the following:

- The ultimate target (understandable description of technology, system, or research)
- Foreign identity (name, affiliation, descriptive features, previous contact, and postal and electronic addresses)
- Circumstances of the incident and background information (e.g., "met at convention in 2000," "denied a visit in 2001," "prime ignored several requests before foreigner approached us [subcontractor]")
- Suspicious activity (e.g., called a few times and E-mailed inquiring about program or technology)

Timely reporting of suspicious foreign activity enables DSS to evaluate foreign collection activity immediately, recommend threat-appropriate SCM, and expedite referrals to U.S. government agencies that can neutralize and, in turn, exploit foreign efforts. DSS successfully contributed to government intelligence and law enforcement activities that resulted in the neutralization of foreign threats. In 2001, DSS referrals of exploitable information to government law enforcement activities increased, as did resultant arrests and success in neutralizing threats.

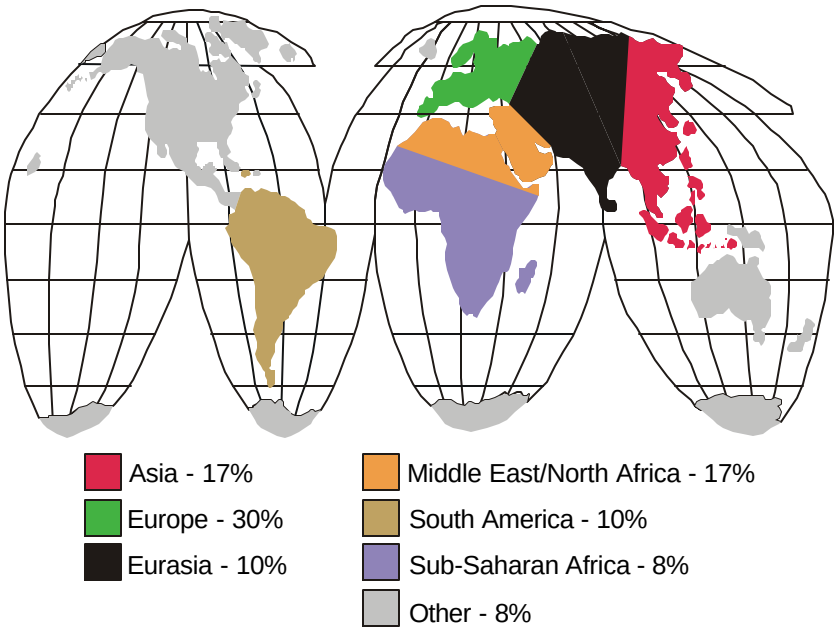
Cleared company reporting also indicates numerous successes in applying appropriate SCM to potentially threatening situations. Based on information provided to DSS, cleared companies refused tours to unauthorized visitors, did not respond to suspicious foreign requests for information, requested and received additional information from

Table 2

Year	1997	1998	1999	2000	2001
# of countries with identified collection involvement	37	47	56	63	75

Figure 2

Worldwide Sources of Targeting



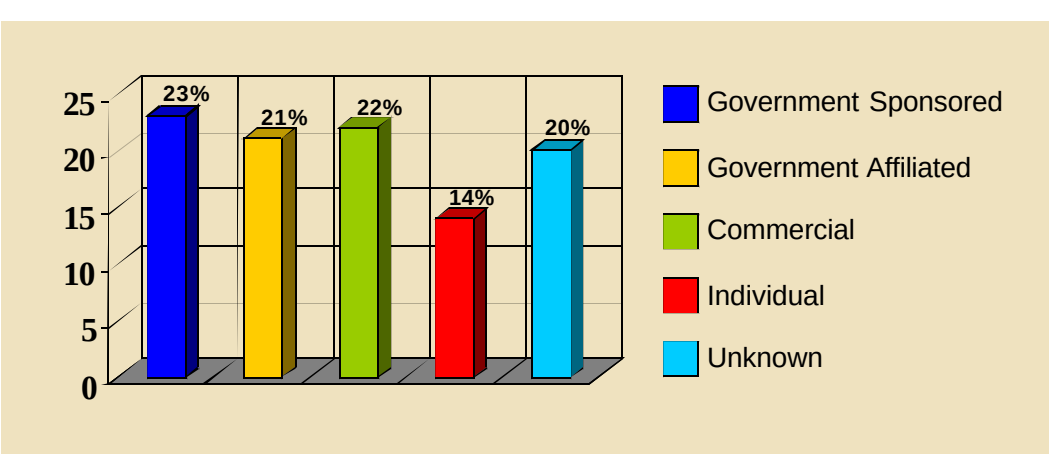
The map above reflects the associated areas of origination for collection efforts. The percentages indicate the level of collection activity reported in 2001. The map does not imply national-level support of the collection activity. The collector may have based his operation in a third country to conceal his intentions, such as being ultimate end-user of the technology.

foreign entities, refused inappropriate visit sponsorship requests, used effective escorts to control visiting delegations, applied security to web-based design and advertising, and questioned foreign entities about the reason(s) for their inquiries. This professional handling of foreign collection efforts assisted in identifying and reporting inappropriate foreign activities.

Associated Countries

Since 1997, the reported number of countries associated with suspicious activities has increased. Many countries exhibit interest in the same technologies. Newly identified countries, for the most part, were those developing nations that may be interested in upgrading existing defense systems or acquiring similar technologies to level the playing field against potential adversaries. It is possible some of the newly identified countries were collecting for other nations whose own collection efforts have either failed or needed to be supplemented.

Figure 3



DSS identifies types of collectors after evaluating reported information, conducting extensive research, and assessing relationships and representatives in each incident. Foreign government-sponsored targeting, including Ministry of Defense, foreign military attaches, and other official government entities, accounted for 23 percent of all matters reported to DSS for 2001. Foreign government-affiliated activities, including research institutes, laboratories, government-funded universities, and government contractors representing government interests accounted for 21 percent. Foreign companies whose work is exclusively or predominantly in support of government agencies are also assessed as government-affiliated. Foreign commercial activities (22 percent) are those that engage in commercial business, in the commercial and defense sectors, whose suspicious activity is not associated with a foreign government. Foreign individuals (14 percent) are entities for whom DSS has been unable to determine affiliation due to lack of information. While it is likely the majority of these foreign individuals have a foreign sponsorship or affiliation, a small percentage were identified by DSS as seeking personal financial gain. In some reported cases, only an individual name or an E-mail address is known.

The high ratio of foreign government-affiliated collectors may be due to foreign government mandates to their universities, research institutes, and S&T academies to develop technologies. Because many critical military technologies are dual-use, technological expertise in these areas not only contributes to military superiority but also can be used to develop a profitable industrial base. The high number of corporate collectors may be attributed to the dual-use nature of many technologies; however, the large number of foreign joint venture and joint research relationships with cleared U.S. industry must be factored in as well. These relationships provide many opportunities for the targeting of particular technologies.

Technology

Information Systems

Information systems (IS) remained the most sought after militarily critical technology in 2001. Forty-four of the foreign countries associated with suspicious activity in 2001 attempted to collect IS technology. This made IS the most diversely sought technology category. However, three countries accounted for 41 percent of all the reported collection activity this year. Most of the activity reported involved activities by foreign corporate entities, which accounted for 32 percent of all IS matters. In the extremely competitive business environment of IS, corporate espionage is to be expected. Foreign government entities also targeted IS heavily, accounting for 23 percent of all matters, followed by foreign individual targeting at 13 percent, and foreign government-affiliated targeting at 10 percent.

Information systems are present in virtually all aspects of our lives. This is particularly true for military, commercial, and industrial activities, and at all levels of government. The pervasiveness of IS technologies make them vital to U.S. warfighter capabilities. Use of IS encompasses a wide range of applications from information systems embedded in individual smart weapons and sensors to local processing and communications systems, including transportable and personnel hand-held devices to international wide area computer networks.

Access to these technologies by potential adversaries could enhance the performance of their military systems and may be used to counter U.S. capabilities. There were 226 total incidents reported this year vice 142 in 2000, resulting in a 58 percent increase. Most increases occurred in the software; command, control, communications, computing and intelligence (C4I), signals processing; modeling and simulation; and information security subcategories.

The large increase in suspicious activity involving software may be attributed, in part, to the phenomenon of "off-shore software

services." Of growing concern to the CI community is the use of foreign research facilities and software development companies located outside the U.S. working on commercial projects related to protected programs. Anytime a U.S. facility relinquishes direct control of its processes and products they are exposing the technology to possible exploitation. Dealing with foreign software companies can pose a collection risk in that codes could be embedded into the software to extract data. In addition, spawning processes and multi-thread tasks may be coded into the program.

The targeting of C4I technology is also on the rise. C4I technology is essential in providing error-free communications, information management, and decision-making capabilities in intense combat situations. The speed and

Table 3

Collection Incidents per Sub-category per Year

Information Systems	1997	1998	1999	2000	2001
Command, Control Communications, Computing, Intelligence (C4I)	6	5	5	8	24
Computer Aided Design, (CAD) Computer Aided Manufacturing (CAM)	1	1	2	4	2
High-Performance Computing	2	5	0	3	3
Information Security	13	6	2	21	16
Intelligent Systems	4	3	0	11	5
Modeling and Simulation	5	6	6	12	17
Network Switching	4	1	0	1	10
Signal Processing	0	1	3	9	20
Software Systems	10	15	13	33	27
Transmission Systems	5	6	4	29	1

accuracy with which information is available for use may mean the difference between success and failure on the battlefield. C4I encompasses a multi-disciplined set of technologies with which U.S. forces maintain a superior ability to detect, localize and effectively engage enemy forces. In asymmetric, high-threat environments, such as those presented by the war on terrorism, secure and uncompromised C4I technologies are an essential element of force protection. As such, it is understandable that this form of IS technology would be sought after by foreign collectors. C4I products and programs targeted in 2001 include digitization tracker data, E-mail interception systems, and communications components associated with telemetry and direction-finding systems. While some countries are developed in this area, many have limited C4I capabilities. However, due to the fast changing technology environment, even countries with advanced C4I capabilities will look to the U.S. and cleared contractors for developments in this field.

Signals processing is the basic enabling technology for all telecommunications and military sensors. Accuracy and reliability of data are critical to mission success. As such, effective signal processing technology is highly desirable. Collection of signal processing technology in 2001 was attempted for SIRRM code (calculates infrared emissions of rocket exhaust plumes), WAM system (regarding AEGIS warship program), ERDAS (imaging software), and radio parts/frequency for VHF receiver for tactical communications for VRC-12. A few nations, mostly in the West, have advanced signal-processing technology. However, most lag far behind the U.S. and, therefore, will continue to target cleared contractors working in these technical fields.

Modeling and simulation software is particularly in demand now. Some of the items targeted in modeling and simulation included a scene simulator, battlefield visualization, airborne radar simulation, flight simulators, H-60 (derivative VH-60), M1A1 and other tank sim-

ulators, UAV simulators, target simulation systems, and aggregate level simulation protocols. Modeling and simulation technologies are attractive for a variety of reasons. Training is expensive and labor intensive. Simulated training is far more desirable. Modeling and simulation programs also help a foreign actor determine the makeup and workings of technology from the program itself, saving on R&D expenses. Due to its high value, foreign collectors are persistent in their attempts to retrieve simulation technology. DSS reports of suspicious activity suggest a particular country made six attempts from 1998 to present to obtain export or ITAR-controlled simulation technology.

The principle elements of information security systems are cryptographic and cryptanalytic algorithms. Although it is hard to judge the state of many foreign nations information security posture, the CI community assessed that most nations have limited to no capabilities in the information security arena. The great influx in communications technologies and the vast array of options in communications mediums have increased the need for stronger and more varied information security technologies. As such, even those countries that possess some capabilities in this area will continue to target the U.S. for this type of technology. In 2001, information security collection attempts involved an asynchronous transfer mode (ATM) monitor and voice and data encryption devices.

Transmission systems saw the greatest decrease in IS targeting in 2001. Transmission

Targeting of Communications Security Devices

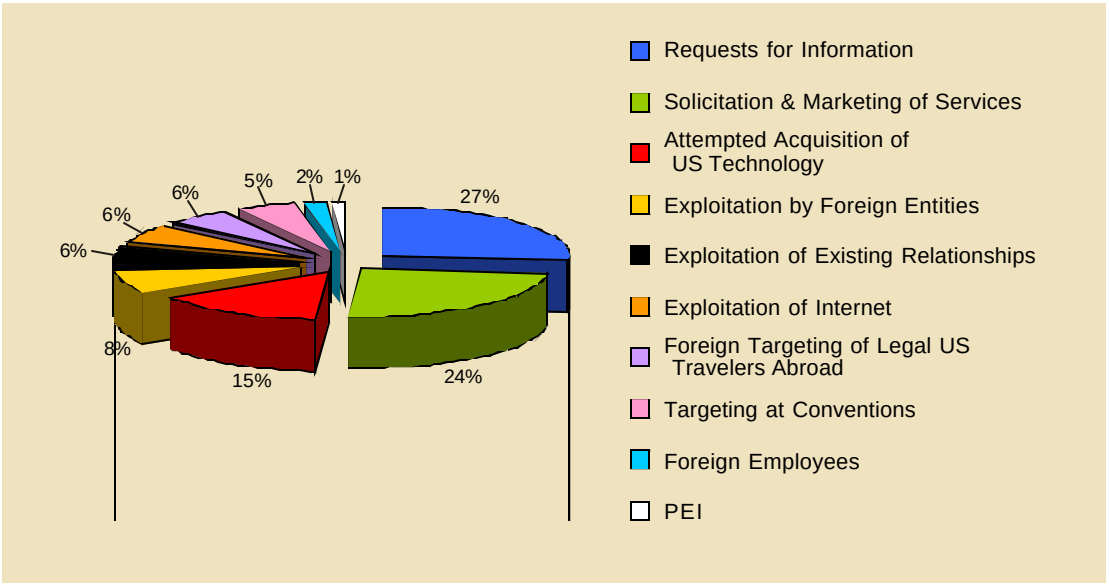
DSS reporting revealed a suspicious contact and solicitation occurred involving the possible purchase of a crypto embedded device, the sale of which is export controlled.

On 2 January 2001, a foreign individual telephonically requested information for a "friend" who was described as living in a foreign country. The foreign caller wanted to purchase a crypto embedded device. The telephone call was received by a U.S. cleared contractor, which then forwarded to DSS the following information: The foreign individual stated he would be ordering a large amount of crypto embedded devices but that first he would like to try out one or two units. He asked the contractor if it was okay to ship to the foreign country and the U.S. representative at the facility stated she would have to check. The caller expressed an additional desired interest in obtaining a crypto embedded device user's manual and that it be express-mailed to him because he was going out of the country and would like to take it with him. The foreign individual contacted the company again on the next morning to further inquire about the probable sale or acquisition of the user manual. This information was reported to U.S. Customs Service and arrests were later made under the Arms Export Control Act.

This U.S. cleared facility currently writes encryption-to-encryption code and troubleshoots circuit boards for the crypto embedded device but forwards repair work to another repair facility in the U.S. Before the stated incident, the repair facility also received an unsolicited request from the same foreign country for the same type of system.

Figure 4

Information Systems



systems include equipment and components used for transfer of voice, data, record, and other information by electromagnetic means either through atmospheric, exoatmospheric or subsurface media or via metallic or fiber-optic cable. These systems mostly are associated with radio. The majority of technologies associated with information transmission are common to both military and civil systems and was made readily available to the foreign market or was developed jointly by U.S. and foreign firms. This may be partially responsible for a decrease in targeting of this technology. However, due to rapid advances in IS technologies including transmission systems, it is likely that, with the introduction of a particular new system, reporting may increase and then return to lower levels once the technology is acquired.

The request for information is the most frequently used collection methodology directed against all technologies and is predominant in the collection of IS. However, other collection methods were not far behind.

The high number of solicitation and marketing of services attempts against IS are mostly attributed to offshore software services. Although some solicitations may be legitimate requests for business, as noted above, the use of offshore software services for intelligence collection purposes poses a grave risk to U.S. security. The effectiveness of this method of operation against software technology can be judged, in part, by the increase in its use. From 1998 to present, DSS recorded 21 incidents of solicitation and marketing of software services from one particular country to cleared U.S. defense contractors.

Attempted acquisition of IS technology (the offer to purchase) may be indicative of extensive reverse engineering programs

employed by some foreign governments. Often the requestor will offer to purchase one sample of a program for evaluation with the false promise of buying more. In addition, IS technologies often require multiple copies of the same code or software to outfit each end user or end product with the application. This can be costly. By purchasing one edition of the technology and illegally making a limitless number of copies, foreign collectors mitigate expenses. IS technology also can be costly and time consuming to develop. Acquisition of IS technologies is an effective and low cost means of obtaining the most cutting-edge IS developments and avoiding expensive R&D.

Sensors and Lasers

Sensors and lasers remained the second most frequently targeted technology for the third consecutive year. Targeting incidents directed against sensors and lasers increased by three percent to account for 20 percent of the total 2001 cases. Significantly, the total sensor and laser technology incidents tripled over the past year. Nearly one-third of these incidents were specifically directed against acoustic technologies. Forty-one different countries attempted to collect sensor and laser technology. The top five foreign countries attempting to collect U.S. technologies overall were responsible for 45 percent of the reported sensor or laser incidents. Half of the cases directed against sensor and laser technology were either government-sponsored or affiliated. One third of the collection attempts were received via E-mail. Requests for information (38 percent) and acquisition attempts (22 percent) were the most common methods of collection for this technology.

Acoustic sensors can be subcategorized into air platforms, marine active sonar, marine passive sonar, and marine platforms. Passive sonar is used militarily for the covert location of underwater objects that radiate sound and are used primarily for antisubmarine and anti-surface warfare. Except for academic research,

Table 4

Collection Incidents per Sub-category per Year

Sensors and Lasers	1997	1998	1999	2000	2001
Acoustic Sensors	4	18	2	5	41
Air and Terrestrial Platforms					(3)
Marine Active Sonar					(10)
Marine Passive Sonar					(17)
Marine Platform					(11)
Electro-Optical Sensors	3	13	3	9	25
Focal Plan Array/Infrared	8	11	5	5	7
Radars	5	8	22	9	20
Imagery	5	13	8	3	12
Lasers	0	0	4	8	24
Other	2	10	5	14	21

there are few commercial uses for passive sonar. Forty-one percent of the acoustic technology cases were specifically directed against passive sonar. Passive sonar systems remain the most effective acoustic sensor for anti-submarine and anti-surface ship warfare in the surveillance or standoff mode. The U.S. maintained a comfortable lead over the major western countries in passive sonar systems technology. Most reported collection efforts targeting passive sonar technology were requests for information E-mailed by alleged students at foreign universities or research facilities.

Twenty-four percent of the acoustic sensors targeting incidents were directed against active sonar systems. Most marine sensing systems use active sonar or sound waves to locate underwater objects. There are several commercial uses for active sonar, which include fish finding, mapping, seismic exploration at sea, petroleum and mineral exploitation, and academic studies. Militarily, active sonar is used for antisubmarine warfare, weapon homing, torpedo defense, mine warfare, deep-sea salvage, and underwater communications and navigation. As submarine technology advances, reducing a submarine's signature and acoustic detection capability becomes increasingly important. The strategic and tactical importance of active sonar for ASW has continued to increase.

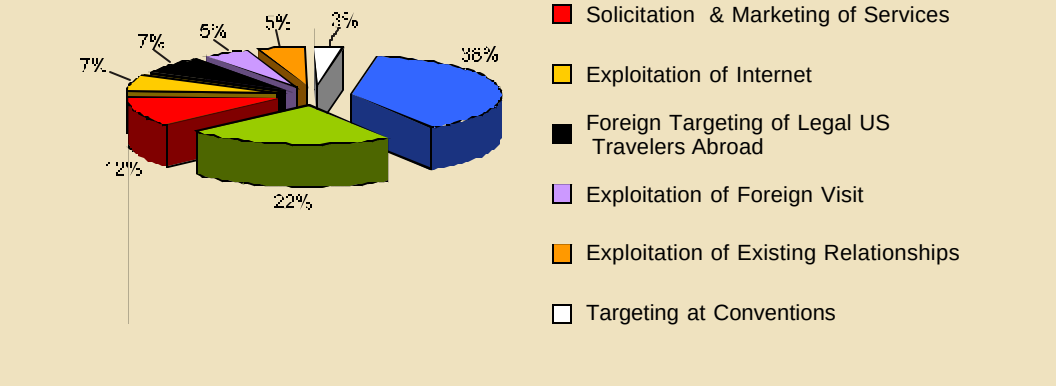
Marine platform acoustics encompass all measures taken to reduce the self-noise of ships, submarines, or other platforms. There are no known commercial uses for the acoustic domes and windows that are considered militarily critical. Twenty-seven percent of the acoustic sensors targeted were directed against these marine platforms.

Twenty-four percent of sensor targeting was directed against electro-optical sensors. These sensors have military applications that seek to facilitate the conduct of operations at night or under conditions of limited visibility. This technology is used for equipment such as night-vision goggles, vehicle driver systems and weapons sights. The critical technology is in its second and third generation. These infrared imaging systems create images based on temperature differences within a scene. The Forward Looking Infrared (FLIR) technology is being used on our advanced weapons systems. The U.S. leads considerably in electro-optical sensor technology, but several countries have produced some second and third generation image intensifier capabilities based on assessed technology transfers.

Laser technology is used in weapons systems primarily for target acquisition. Many military forces use laser guided weapons, but a few produce the newer "eye safe" laser system. Over three percent of all 2001 collection attempts were targeting the limited dual-use laser technology that could avoid the eye blindness effect caused by older laser technology. Another 13 percent of collection attempts against sensor and laser technologies were specifically directed against radar systems. Radar is indispensable for a variety of military uses and is uniquely enabling since few other detection schemes are capable of ranging and direction finding in a variety of obstructing conditions. Most foreign countries have indigenous capabilities over a broad range of radar expertise. However, most nations are dependent upon U.S. technology for components such as power amplifiers, pulse

Figure 5

Sensors and Lasers



compression units, and signal processing subsystems.

In one 2001 case, a foreign delegation visited a contractor facility known for its research and production of SONAR and radar systems. Upon their arrival, the delegation attempted successfully to substitute three persons from the previously authorized list. Once the tour and meetings began, some delegation members attempted to wander away from their escorts. Delegation members persistently questioned facility personnel about critical technologies produced at the facility. In a second case, an applicant from an embargoed nation attempted to gain employment at a facility that produces Radar systems. During the job interview, the applicant refused to identify his nationality and questioned the recruiter on specific technical details of U.S. radar systems.

E-mail requests for information were the most popular means of collecting sensor and laser technology. In one such case, the requestor asked for information related to the Aegis Class Frigate; Towed Array Systems; Torpedo Defense Systems; Mine-Hunting Systems; and Airborne Radar. A similar request asked a defense contractor for information pertaining to specific Naval Electronic and Surveillance Radar and Sonar systems. Another unsolicited E-mail requested the Graphic User Interface for the Forward Looking Sonar System (FLOSS). Most Electro-Optical contractors presented technology to the public in published and web site ads, which generated interest from several countries requesting catalogs, product guides, or price lists for the technology.

Table 5

Collection Incidents per Sub-category per Year

Armaments & Energetic Materials	1997	1998	1999	2000	2001
Unidentified Technology	0	0	0	0	28
Ammunition, small/medium caliber	0	0	0	0	4
Bombs, warheads, large caliber projectiles	5	8	4	16	24
Energetic material	0	1	1	1	32
Safing arming, fusing, firing	1	1	0	5	9
Gun and artillery systems	1	4	4	1	9
Mines, countermines and demolition systems	1	1	0	1	2

Armaments and Energetic Materials

Armaments and Energetic Materials Technology (AEMT) was the third most targeted technology group by foreign entities at 14 percent. Foreign attempts to collect information on or to acquire these systems and technologies increased significantly since last year, with 24 incidents reported in 2000, to 108 incidents reported in 2001. AEMT, which includes small and medium caliber ammunition; bombs, warheads and large caliber projectiles; energetic materials; safing, arming, fusing and firing technologies; gun and artillery systems; and mines, countermines; and demolition systems, is the fundamental nucleus in virtually all weapons systems. Collection efforts for United States' high-technology armaments and energetic materials underscore the worldwide push to update and integrate the core weapons systems of military, paramilitary and terrorist forces.

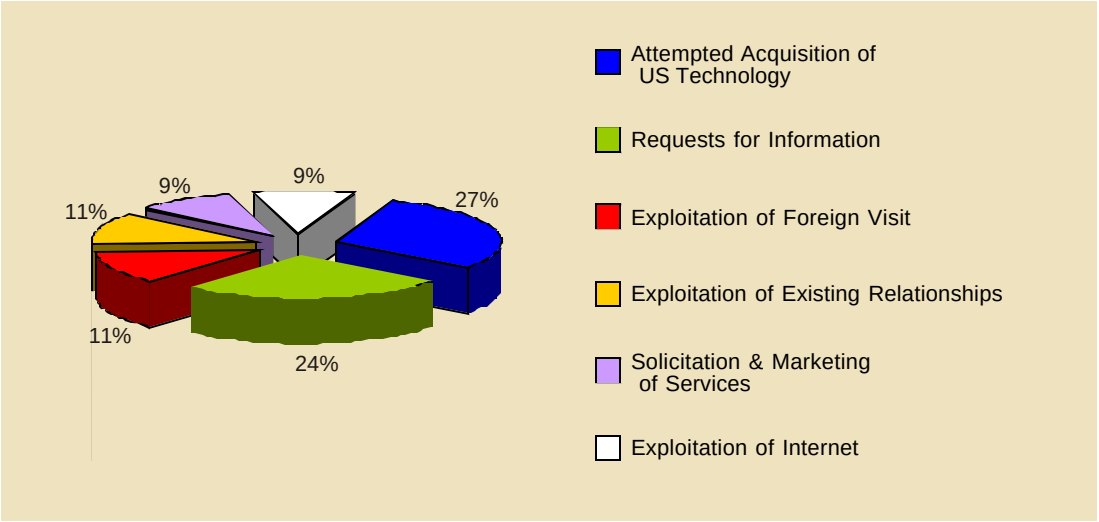
While overall foreign collection attempts against militarily critical technologies increased, the sharpest rise in this subcategory was in energetic materials, from one cleared-defense industry reported incident in 2000 to 32 in 2001. As illustrated in the chart above, the combined total of incidents for the years 1997 through 2000 was three. Collection attempts against bombs, warheads, and large caliber projectiles had the second highest number of incidents reported at 24, up from 16 in 2000. Guns and artillery systems collection also increased from previous years.

The dramatic increase in pursuit of this technology parallels the increase in "smart weapons" design and development. While many countries now have the capability to produce and acquire conventional weapons with limited range, few are able to produce guided and individually targeted multi-reentry vehicles. The extended range of these smart weapons and near pinpoint accuracy of the warhead will continue to make this critical technology a targeted commodity by foreign powers.

The most frequent method of operation, based solely on numbers, was attempted acquisition, at 28. Of particular note, 21 of these incidents occurred against energetic materials. One U.S. Company had 25 reported incidents

Figure 6

Armaments & Energetic Materials



in the overall category of Armaments and Energetic Materials, 21 of which were attempted acquisition. Solid and Liquid Propellant Mechanical Behavior Manuals were the predominant items sought by foreign collectors, with offers for purchases sent via E-mail.

Aeronautics

Aeronautics slipped to the fourth most frequently targeted technology, accounting for 11 percent of the total reported incidents for 2001. Although aeronautics may have dropped in ranking, the number of targeting incidents against this critical technology jumped 360 percent from 23 reported incidents in 2000 to 83 in 2001. Thirty-one different countries attempted to collect aeronautics technology with the top five most active countries responsible for 38 incidents, nearly half of those reported. In those cases whose source of interest in aeronautics technology could be identified, 58 percent were either foreign government or affiliated. Requests for information (28) and acquisition attempts (18) were the most common methods of collection for this technology, with 24 (29 percent) of the attempts made via E-mail.

For several years, aeronautics technologies have continued to be of high interest to many countries attempting to upgrade their indigenous aviation programs. In 2001, UAV systems and components were highly targeted with 21 reported incidents. Seven cases involved aero-elasticity as "students" from several foreign countries sent E-mail requests for technology required for their research programs. Additionally, helicopters are still targeted, with several defense contractors reporting suspicious activities.

Successful use of UAVs during Operation DESERT STORM and the Balkans crisis helped elevate a wide interest in this technology. The unmanned vehicles are a low

Table 6

Collection Incidents per Sub-category per Year

Aeronautics	1997	1998	1999	2000	2001
Aircraft, fixed wing	10	5	6	11	46
Gas turbine engines	8	5	7	3	7
Human (crew systems) interface	1	5	0	1	0
Helicopters	3	1	1	4	9
Unmanned aerial vehicles	4	4	1	4	21

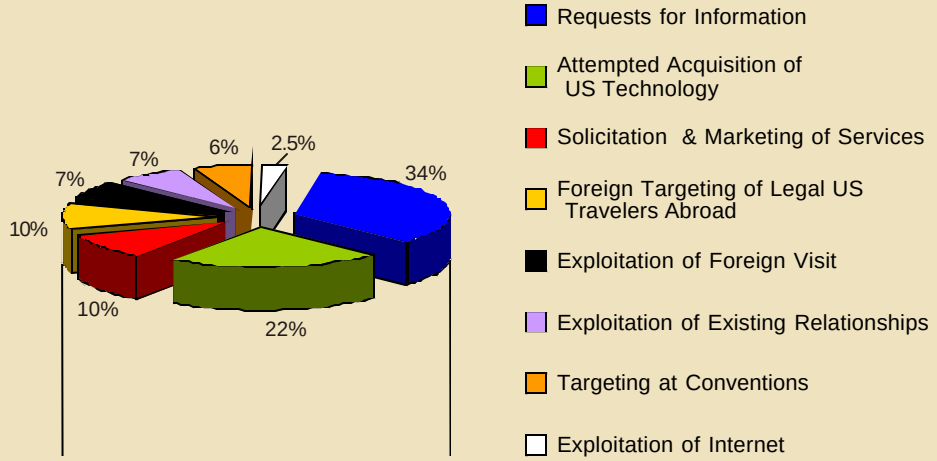
cost answer to the reconnaissance and surveillance requirements of numerous countries. In the past year, there were several incidents involving attempts to illegally obtain UAV technology. In one case, individuals were arrested, based on cleared contractor reporting, after being caught trying to smuggle UAV camera systems through Europe to an embargoed country. A few foreign companies are trying to take advantage of the needs of some countries by establishing themselves as the broker in business-to-business ventures. Several foreign countries are openly attempting to purchase UAV systems from the U.S. Both the UAV platforms and their components will continue to be highly targeted technology.

The electronics systems on all U.S. airborne platforms continue to be targeted. The hardening of electronic integration of aeronautic systems for the protection against electromagnetic pulse and radiation effects on the nuclear battlefield remains the key to this critical technology. With numerous applications of electronics and electro-optical technologies within space, weapons, or aeronautics systems, this critical technology will remain in demand. As the U.S. and other countries move into new generations of electronics weapons systems, more countries are forced to keep pace protecting their aeronautics systems.

Technology collected from open-source venues regarding aeronautics will continue to be our greatest threat. Increased Internet use is an indicator for future technology collection operations. Off shore, business-to-business solicitation, and the number of foreign student researchers attempting to acquire information or obtain employment will continue to grow as the second most popular collection method for illicitly attempting to obtain aeronautical technology. Although the ease of Internet use is becoming more popular, we continue to see traditional collection methodology used against aeronautics technology. In 2001, there was limited reporting regarding incidents where U.S. cleared contractors suspected surveillance activities and "bugged hotel rooms" while traveling abroad. DSS received several reports from defense contractors indicating the blatant and aggressive collection operations at conventions and air shows by foreign entities interested in the latest aeronautics technologies, an MO previously employed and expected during these events.

Figure 7

Aeronautics



TARGETING OF UNMANNED AERIAL VEHICLE TECHNOLOGY

During 2001, numerous countries targeted U.S. made unmanned aerial vehicle (UAV) platforms, although requests for aeronautical technology comprised 11 percent of all foreign requests reported to DSS. Of 21 cases involving UAV technology reported to DSS during 2001, at least 50 percent involved E-mail requests for UAV platform or its various components' technologies. Several of these E-mail requests originated from newly independent nations. Based on the failure to acquire UAVs, these foreign countries are expected to continue targeting UAV technology for the near future.

Currently, nearly 50 nations deploy UAVs for military purposes. The UAV platform is considered so essential for modern military use that the armies of many third world countries, including those in South America and the Middle East, now produce their own UAV platforms. These UAVs are utilized for training purposes and are usually similar to prototypes of remotely piloted vehicles (RPVs) or drones. Terrorist forces may have deployed UAVs during the military campaign in Afghanistan following September 11, 2001. Nations bordering Afghanistan have Asian-produced UAVs in their order of battle. A Persian Gulf country already deploys two versions of its own domestically produced UAV platforms. Both of these UAV models were initially designed for training

ground operators in techniques involving RPVs, Several import/export firms are suspected of diverting UAV platforms to Middle East countries which are on the U.S. government's embargo list of defense products. At least two incidents were reported to DSS during 2001 involving the attempted diversion of UAVs from the U.S. to the Middle East and may have been shipped to a third country or foreign entity.

While many technologically advanced nations deploy UAVs for military purposes, a number are eager to acquire UAV technology from U.S. entities, either for their own aerospace industry use or to reverse-engineer these platforms for domestic or international sales. Recently, exhibits of commercially available UAV platforms have attracted large numbers of visitors at international air shows. Other potential customers for the UAV were South American drug cartels, which attempted acquisition through approached aerospace firms in the Middle East. One South American government, which already produces its own UAV prototypes, approached U.S. entities directly with a formal request for information on such related technology as aerodynamics and wingspread data. According to last year's edition of Technology Collection Trends in the U.S. Defense Industry, four percent of all RFIs reported by DoD contractors to DSS that year originated from South America. This small percentage of South American RFIs is even more interesting, as 11 percent of all reported RFIs from foreign entities during 2001 involved aeronautical systems and technology; however, foreign interest in U.S.-made UAVs is not confined strictly to the Western Hemisphere.

Foreign nations also heavily targeted such UAV-related components as sensors and guidance systems during 2001, and included 20 percent of sensors and lasers technology, while another four percent of all such foreign requests involved guidance and navigation technology. Foreign targeting has included such components as Ultra-Wide Band Synthetic Aperture Radar, auto pilot controls, and data link subsystems including data link related technology involving encrypted systems. Three nations deploying UAVs are known to have the capability to protect their data link technology through encryption.

Five of the 21 UAV cases reported to DSS during 2001 involved scheduled visits by foreign military personnel, although the overall number of visits by foreign military personnel to acquire technology constituted eight percent of all reported MO during 2001. Nearly all these cases involved some overt incidents, including the photography of UAV platforms by visiting military personnel from an Asian nation.

Electronics

Electronics technologies are either a major component of or are used to produce every major weapons system in the U.S. arsenal. As such, electronics are one of the most critical elements in assuring the continued superiority of U.S. military capabilities. The majority of defense technologies targeted in 2001 were components rather than complete systems and this held particularly true for electronics. Foreign targeting of electronics technologies remained in fifth place for 2001, with 24 countries, accounting for seven percent of all targeting. Only three countries accounted for 46 percent of all reported electronic collection activity this year. Foreign government-affiliated entities accounted for most (33 percent) of the electronics technology-targeting activity reported to DSS for 2001. This was followed by foreign corporate entities at 27 percent, foreign government entities at 16 percent and foreign individuals at 14 percent. In 10 percent of reported electronics matters, DSS was unable to determine the affiliation of the foreign collector.

The high ratio of foreign government-affiliated collectors may be due to foreign government mandates to their universities, research institutes, and S&T academies to develop electronics technologies. Because many electronics technologies are dual-use, technological expertise in this area not only contributed to military superiority but also is used to develop a profitable industrial base. The financial gains realized from a strong electronics industrial market can contribute to a country's economy. Unfortunately, resale of protected electronics technology to rogue nations poses a substantial threat to U.S. security.

In 2001, the majority of electronics targets concerned defense applications of dual-use technology such as microwave and satellite communications components and antennas. There were 51 incidents reported this year, up from 36 in 2000. However, this increase is somewhat proportional to the overall increase in reporting from one year to the next and, therefore, does not actually represent a spike in electronics targeting. Most targeting occurred in the subcategories of components and materials and fabrication. Specific targets in 2001 included electronic elements of automatic target recognition for UAVs, Patriot missile electronic components, AgGaSe2 crystals, wave tubes, magnetrons, microencapsulation technology, Speckle interferometer, and missile specifications using MIL-STD-810 E or F, and LC 1911 camera technology.

Electronics components include technologies that provide electronic support to a variety of products including radar, communications, navigation, and guided munitions. Missile guidance components are included in this category and experienced heavy targeting in 2001. At least five incidents involved targeting of technology specifically designed as

Table 7

Collection Incidents per Sub-category per Year

Electronics	1997	1998	1999	2000	2001
Materials/components	4	6	12	1	17
Fabricated materials	2	3	1	0	5
Microelectronics	5	2	4	7	1
*Optoelectronics	4	1	1	1	2

*Many optoelectronic targets in 1997 may have concerned sensors. Detailed 1998 reporting allowed DSS to identify optoelectronic targets that were being applied to sensors. In 2000, due to the nature of reported incidents, only 9 fit neatly in sub-categories and in 2001 that was true of only 25 matters.

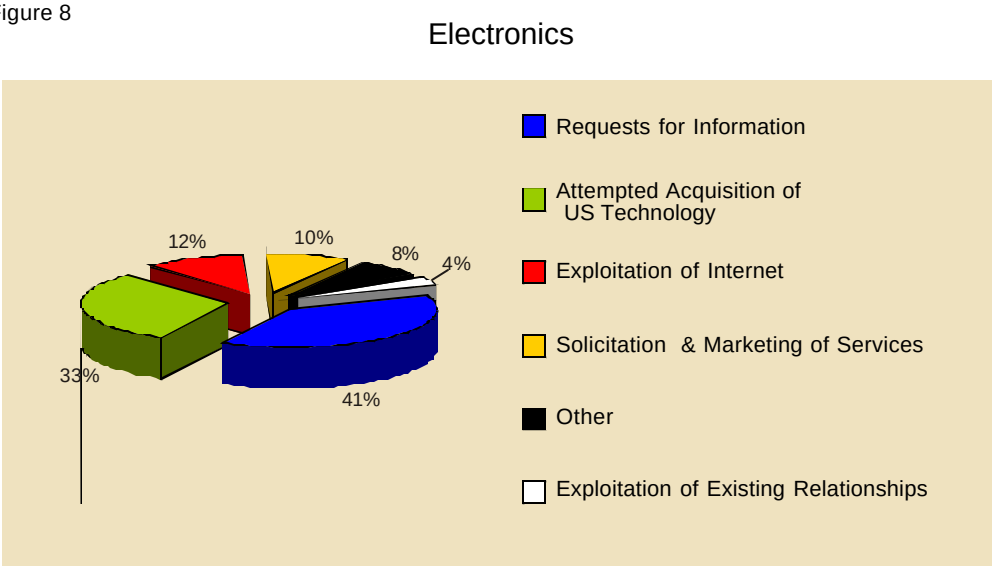
electronic missile components. Microwave technology also falls under electronic components and includes microwave-integrated transistors, integrated circuits, and power amplifiers. In 2001, there were seven instances in which microwave technologies were targeted.

Electronic materials support electronic devices, components, sensors, environment tolerant devices, compound semiconductors, and fabrication equipment. In turn, the fabrication equipment subcategory provides technology for nano-structures, integrated circuits, and micro-electrical mechanical devices. Microelectronics are prevalent in nearly all modern weapons and communications systems. The U.S. is one of two nations in the world with the capability to produce top of the line microelectronics technology. U.S. superiority in this area is essential to maintaining an edge over our adversaries. Finally, optoelectronics is the fastest evolving electronics technology. Optoelectronics are engaged in sensors, signal interconnectivity, image processing, radar, electronic warfare, and electronic intelligence applications.

The U.S. is a world leader in the development and production of electronic technology. As such, it is not surprising that cleared contractors participating in electronic technology programs would be targeted. Request for information is the most frequently utilized collection methodology against all technologies, and that held true in the collection of electronics technologies as well, accounting for 41 percent of all incidents. Attempted acquisition of U.S. technology was not far behind.

As with other technologies, attempted acquisition of electronics may be indicative of extensive reverse engineering programs employed by some foreign governments. Visitors to some foreign countries have noted a significant lack of imported hardware. Because of the dual-use nature of electronics technology, it lends itself to development for both military effectiveness and a strong industrial base. Such development is a priority for many foreign governments. In addition, the dual-use aspect of electronics makes acquisition an attractive MO in that a foreign collector may

Figure 8



*Totals equal more than 100% due to the use of multiple methods of operation in some suspicious incidents.

try to obscure the end-use of the technology in an effort to make a purchase. Many foreign collectors hope to confuse the issue when contacting a cleared U.S. contractor for purchase of an item and many conveniently feign innocence when confronted with the need to adhere to export regulations.

Marine Systems

Marine systems technology was the sixth most targeted technology by foreign entities during 2001 with 49 incidents, which accounted for six percent of the overall reported incidents by cleared contractors. Marine systems include propulsion and propulsion systems; marine signature control and survivability; and subsurface and deep submergence vehicles.

The U.S. has long enjoyed the position of superpower in the deep-water field of marine systems with the former Soviet Union once a close rival. Few countries in the world have the capability for sustained at-sea operations, with the predominance of those countries, being close allies of the U.S. Moreover, while there are countries whose maritime history is rich and long or which may have a particular area of expertise, none have across-the-board successes in technologies like the U.S.

The ability to control the seas, whether by air, surface, or sub-surface, is critical to U.S. national security. The U.S. maintains its superiority in this field by constant research and development in areas such as stealth technology, to include ship signature; deep-submergence hull design; and propulsion systems, which expand range; speed; and endurance of a platform. The land attack destroyer program was the single-most targeted individual program, primarily from one

country, with high-speed assault craft and anti-submarine warfare technology the next areas targeted by several countries.

With more countries having submarines in their order of battle, there is an increasing need for repairs, replacement parts, and upgrades. Cleared contractors must remain vigilant in protecting their technology from attempts by foreign entities to bypass export controls. While there were 49 attempts by foreign entities to obtain this technology, there were 25 countries identified as the collectors. Three MOs were predominant for collection attempts; request for information was the most frequent method, Internet offers to purchase or to offer services was second, and visits to facilities and personal contact to an individual combined for the third most frequent method.

Of particular interest is the geographical areas associated with these foreign entities and methods used. One country used the anonymity of the Internet almost exclusively. Moreover, while normally DSS would separate these categories, it is important to note that the tool used here was the Internet, and the method of operation was E-mail requests for information, E-mail solicitation of business, and E-mail offering of services. The Internet was further exploited by an attempt to hack into web sites to download critical technology information.

Also of note is that a long-time collector of U.S. technology maintained its normal method of operations, preferring to attempt to exploit the human element of the intended target. This country attempted collection through direct contact to an individual employed by cleared contractors or during group visits to a facility. Another country and long-time ally of the U.S. also used these methods to collect against cleared U.S. industry.

All marine platforms, whether surface or sub-surface, self-propelled, remotely operated or tethered, require some form of propulsion system. The ability to conduct long-range operations without numerous port calls for refueling was one of the major obstacles facing foreign naval forces in general. With advanced designs and accessibility, through whatever means, of high-output low-fuel consumption, this portion of the hurdle will be quickly overcome. Maintenance by skilled technicians and the availability of replacement parts underscore the need for indigenous production or ease of procurement through cooperative entities to make the final leap. Countries that have obtained high-technology platforms must still find the means to maintain the overall operational integrity of their naval forces. One embargoed country was noted E-mailing a request for replacement parts for a gas turbine governor, directly to the manufacturer, thereby attempting to bypass export controls.

Stealth technology is by far a crown jewel held by U.S. naval platforms. The ability to operate covertly or, at minimum, with a reduced acoustic signature, is crucial to survivability in non-permissive or hostile waters. These operations may take place in deep water, or, in highly trafficked areas in littoral environments. Many countries operating in these areas have advanced sonar technology and weapons, such as mines and torpedoes, designed to home-in on a particular sound or acoustic threshold. The U.S. Navy's effectiveness as the preeminent sea power depends, in large part, on its ability to operate below that acoustic threshold. Several foreign entities, with apparent foreign government sponsorship or affiliation, and with limited technology in this field, attempted to obtain information on U.S. systems during the year 2001.

There are 23 countries with at least some capability to produce subsurface vehicles indigenously; 45 countries currently have operational submarines, albeit to a limited degree in some cases. Virtually every country with a maritime concern now includes at least one operational submarine in its naval order of battle. Those countries, which have limited or no capability in this field, must go outside their own country to obtain these platforms or components to support their subsurface requirements. Many countries, including the U.S., sell either older platforms or exportable versions of current designs to meet the demand for these vehicles. The U.S. is the leader in design, development and production in technology for this category.

During 2001, there were multiple instances involving foreign entities requesting naval platform enabling technology. In contrast to foreign interest in subsurface vehicles, cleared contractors reported 14 foreign requests, for the stealth technology associated with various military components of surface vessels. These targeted areas of maritime technology included ship design, warfare systems, propulsion systems, noise reduction technology, and C4I. The procurement of stealth technology is a major priority for many naval powers, especially since foreign requests for sensors and lasers comprised 20 percent of all reported requests for U.S. technology. Many of these nations already have limited authorized access to the sensitive technologies of these various undersea and surface warfare systems through such arrangements as Data Exchange Agreements. Nevertheless, because they have major naval assets in their defense arsenals, all these nations are anxious to acquire more stealth technology and related systems.

Foreign media entities made several requests via E-mail or handwritten mail for photos and information about naval platforms and some of them made multiple requests. Nearly all these requests resulted from individual initiative that DSS cannot associate with government or commercial interests. Although nothing beyond publicity-class information has officially been released about certain naval platforms, several Asian and North American entities actually printed photos of a U.S. Naval platform and its related components on the Internet. The Asian perpetrator is a known collector of data that supports his nation's maritime power. Although the actions of these foreign media entities were largely innocuous, other foreign entities expressing interest in U.S. Naval platforms were rather determined to acquire sensitive military technology by illicit means.

The most obvious foreign threat to naval platform technology occurred online with the web sites maintained by DoD contractors. In three major incidents recorded during

2001, Asian hackers attacked several of these web sites. Yet another hacker, connected to an aggressive state technology and science commission in the Asian Pacific region, did the same to several web sites containing information on a particular naval platform. In a similar incident, European hackers, connected to a foreign state-owned aerospace/shipbuilding firm, attempted to download the naval platform computer files of a DoD contractor. In 2000, another employee of this same foreign firm, which serves as a subcontractor for U.S. Naval platforms, requested a badge in order to gain access to a naval platform. This sort of industrial espionage is typical from a nation whose government publicly admitted that its intelligence services spied on U.S. industries for years.

One maritime nation in Asia requested U.S. military technology and expressed interest in stealth capabilities of a naval platform, especially its sonar and radar absorbing materials. Asian maritime powers have expressed a serious interest in U.S. Naval platform as a means of modifying their own class of naval vessels. Petroleum-producing neighbors in immediate geopolitical region of this latter nation have also expressed an interest in U.S. Naval platforms and their warfare capabilities.

Many foreign entities targeted the various stealth components of naval platforms on an individual basis, rather than attempt to target a whole naval platform. Requests for stealth technology also included such support systems as computers and software. Many of these foreign sources reside in other maritime nations in Europe, although several such attempts involved Asian nations as well. In addition, a Middle Eastern state expressed much interest in undersea warfare technology (e.g. sonar), although it already receives such technology from the DoD through foreign military sales.

Space Systems

Collection efforts directed at space technologies doubled in 2001, accounting for five percent of DSS incident reports. Significantly, although 14 different countries targeted space technology, two countries accounted for 42 percent of the total reported collection attempts. Also of significance is the fact that two cleared defense contractors reported a combined 58 percent of these incidents. Propulsion systems and propellant technology were specifically targeted in 45 percent of the reported space-related cases.

With few exceptions, every country targeting space systems technology was interested in propulsion systems. The Joint Army, Navy, NASA, and Air Force (JANNA) Interagency Propulsion Committee and the

Chemical Propulsion Information Agency, reported numerous cases of requests for information or acquisition of restricted military technology by foreign entities seeking propulsion manuals, product lists, or meeting notes. In two cases, these requests were from foreign military attaches in Washington, DC.

The information highway is quickly becoming the shortcut to space technology. Thirty-seven percent of the reported collection efforts to acquire space technology were received by E-mail sent via the Internet. Of great concern is the possibility that critical information is lost through web sites provided by cleared U.S. defense contractors as a means of advertising. These web sites may also provide information such as a list of defense contractors or universities working the technology, government agencies involved in the R&D, a calendar of events, and the location of involved facilities.

Contractors also lose critical information through normal business-to-business practices. Some space technology is considered "dual-use", and several contractors sell the information through joint ventures with foreign entities.

In some space technology related cases, several reports suggested U.S. executives believed their hotel room or office space within foreign countries was "bugged". It is common to have U.S. executives report that they were repeatedly placed in the same hotel room over the period of several different trips.

DSS expects collection efforts directed against space-related technologies to continue to grow over the next few years. As more countries expand their military programs to include space, DSS assesses that foreign entities will be more aggressive in their collection efforts. As space technologies are used for purposes that are more commercial in the future, DSS expects a greater interest by public companies, foreign and domestic.

Chemical and Biological Systems

Chemical and biological systems technology was the eighth most targeted technology by foreign entities at four percent of overall reported incidents from cleared contractors. This technology category includes chemical and biological defense systems, and detection, warning, and identification. Recently, the U.S. and its allies were faced with increasing numbers of countries actively manufacturing chemical and biological warfare agents. The total of actual incidents reported during 2001 was 33, up from eight in the year 2000, and seven from 1999. Of particular interest, there was no country which had a higher number of reported incidents associated with this technology, although there were many new collectors reported. For instance, a particular country requested blast doors for a biological manufacturing facility in 2000, and in 2001. Coincidentally, a student from that country was arrested in the U.S. for technology diversion linked to anthrax. Countries in areas such as the Middle East and North Africa, where rapid procurement of these agents, coupled with the increasing likelihood of employment of chemical and biological weapons, drives the need for superiority in detection and countermeasures technology for the U.S. Over 50 percent of the requests for chemical and biological systems technology came from this region and associated countries. One request, which came from an individual who claimed to be a student of a country that is

currently embargoed, wanted to work with chemical (mustard gas) or biological programs or to establish an academic relationship on these topics with a U.S. entity.

The predominant tool used by foreign collectors to obtain chemical and biological systems technology was the Internet. Twenty requests for information and products came by E-mail. The number of requests for decontamination equipment, techniques, and antidotes were as high as requests for protective clothing and self-contained breathing apparatuses.

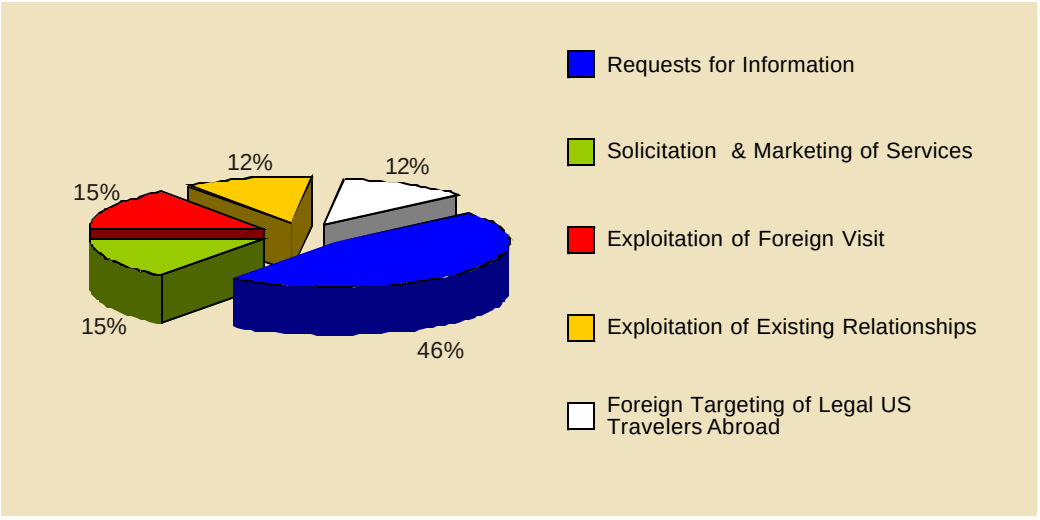
Of note, one country, which suffered from terrorist-induced chemical and biological attacks, overtly requested protective gear and detection equipment. Similarly, countries with no known anti-U.S. groups or links to terrorist organizations overtly requested similar technology. This may reflect the growing unease and fear of a chemical or biological attack occurring outside of the U.S. or in areas so far unaffected by terrorism.

Manufacturing and Fabrication

Technologies covered under manufacturing and fabrication include those required for the production of military hardware. In most cases, the technologies, equipment, and technological expertise required to produce the hardware are dual-use. All countries engaged in the production of military weapons, munitions, and systems possess at least some technical expertise in this area. As such, targeting of manufacturing and fabrication technologies has not historically been prolific. Still, foreign targeting of manufacturing and fabrication does occur. Developing countries attempting to obtain manufacturing and fabrication technology in an effort to produce weapons of mass destruction is of great concern. However, even the loss of restricted information regarding

Figure 9

Manufacturing & Fabrication



conventional weapons can pose a major threat to the U.S. warfighter. In 2001, targeting of this technology tied for ninth place (alongside guidance and navigation control) and accounted for four percent of all matters. DSS data shows targeting of manufacturing and fabrication technology remained stable over time as it placed 10th for 2000, accounting for three percent of all suspicious contact reports that year.

Specific manufacturing and fabrication targets in 2001 included aeroelasticity processes, F-15 horizontal stabilizer process specifications, titanium materials, robotics technology, isothermal forging methods, casting methods and wind tunnel technology. Fifteen of the foreign countries associated with suspicious activity in 2001 attempted to collect this type of technology. Most of the countries seeking manufacturing and fabrication technology had a few incidents each. However, several countries, including two U.S. allies, made three or four attempts to collect manufacturing and fabrication technology last year. Detecting such patterns helps DSS to identify targeting requirements for foreign governments and, eventually, effective SCMs necessary to protect U.S. technology.

Foreign corporate entities accounted for most (35 percent) of the manufacturing and fabrication technology collection activity reported to DSS for 2001. This was followed by official foreign government entities at 15 percent and foreign individuals and foreign government-affiliated entities at 11.5 percent each. In 27 percent of reported matters, DSS was unable to determine the affiliation of the foreign collector. The high ratio of corporate collectors is likely attributed to the dual-use nature of manufacturing and fabrication technology and to the large number of joint venture/joint research relationships in this field.

The request for information is the collection method used most frequently against all technologies, accounting for 46 percent of all matters.

The exploitation of a foreign visit is an effective method by which to collect manufacturing and fabrication technology. Foreign visitors to U.S. cleared industrial plants and facilities have an opportunity to observe the processes up close. Often the foreign visitor will go beyond the bounds of the agreed upon visit protocols, to include wandering unescorted in restricted areas. Several suspicious incidents in 2001 involved foreign visitors illicitly taking photographs during visits. The effectiveness of this methodology is fostered by foreign relationships such as joint ventures.

Often visits, some long term, are negotiated in coordination with an existing or proposed joint venture. Exploitation of relationships is also effective over time in lowering the guard of U.S. cleared employees. By becoming part of the fabric of the U.S. cleared companies' daily activity, foreign company representatives may attempt to blur the line between classified and unclassified programs and gain access to restricted materials. Relationships with foreign companies also create an opportunity for overseas travel by U.S. cleared contractors.

Guidance, Navigation and Vehicle Control

Targeting of guidance, navigation and vehicle control technologies by foreign entities represented four percent (28) of the total incidents reported by cleared contractors. This is an increase since 2000, when 2.5 percent (15) of reported cases were in this field. Twenty percent of total incidents in this technology category originated from one country in the Far East. The most sought-after technology was related to the Global Positioning System (GPS) at nearly 50 percent of the reported incidents. Virtually all air, surface ship, and subsurface vehicles, to include some missiles launched by various platforms, require accurate information, real-time, to carry out precise guidance and navigation. Military forces rely on GPS for land-craft guidance as well as do the foot soldiers and sailors, in particular, special operations forces. The U.S., through GPS, and Russia, through Global Navigation Satellite System (GLONASS) possess the only worldwide satellite navigation systems. This near monopoly by two countries underscores the appeal of obtaining these technologies. Faster, more accurate, and longer-range systems are supported and guided by these technologies, driving foreign collectors to attempt to procure them through illegal channels.

Foreign Collection Methods

The 2001 data on foreign collection MO is derived from increased reporting from cleared contractors. As in previous years, DSS is providing the frequency of reporting per MO category as a percentage of the whole. Percentages exceed 100 percent due to multiple reporting.

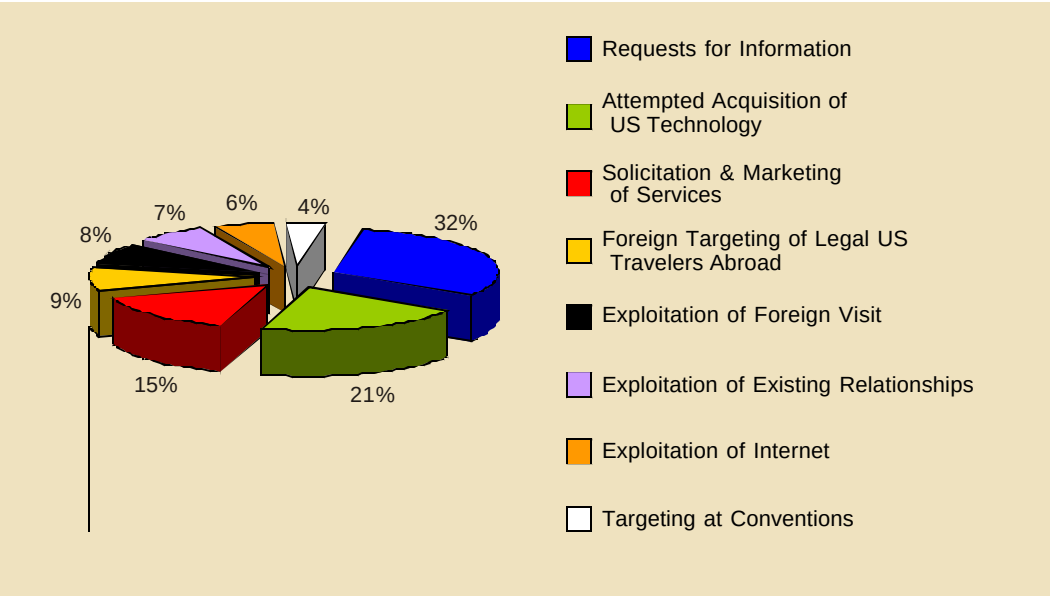
Requests for (S&T) Information

RFIs are broken down into fields including E-mail, letters, faxes, direct and in-person, telephone, and survey requests. E-mailed RFIs accounted for 70 percent of the total RFI reporting, up from last year's 64 percent. Letters accounted for the next most often used RFI approach, representing 11 percent of the total reporting. A decrease in mailed RFIs was seen by this office but is offset by the E-mail increase. Telephone, direct and in-person, fax, and survey requests account for six percent, three percent, two percent, and two percent respectively.

Sixty percent of the E-mailed RFIs were related to web-based advertising. Since the 2000 reporting year, DSS proactively encouraged cleared defense facilities to incorporate the concepts of security with web-based design and advertising. In most cases, cleared contractors had already incorporated security with design and advertising. Additionally,

Figure 10

FY 2001 Methods of Operation



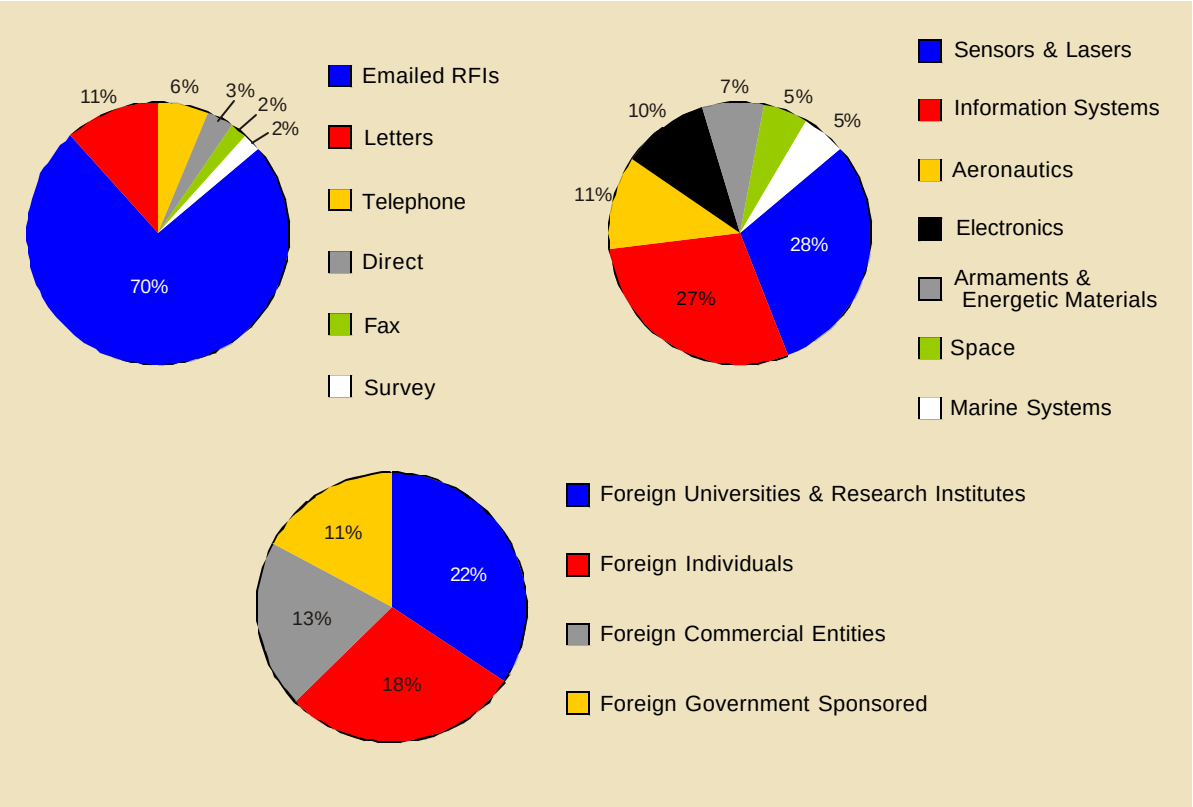
DSS and cleared contractors believe the threat from the Internet and E-mailed RFIs is mitigated with a strong security education program wherein cleared employees are instructed to recognize the difference between suspicious E-mail and a sincere business request. If suspicious, cleared defense employees report the suspicious E-mail to DSS. DSS reviews the suspicious E-mail for referral to either an investigative or intelligence agency.

An increasing trend observed since 1999 concerns E-mailed RFIs from foreign universities and research institutes. A majority of these entities are state-funded and are heavily involved in military applicable technologies. Representatives of the research centers attempt to collect information on foreign technology through the use of requests for technology exchanges and discussions with experts. These foreign efforts involve identifying and contacting experts in various fields of interest and forming greater cooperative information exchanges with U.S. defense contractors and military Research Development Test and Evaluation (RDT&E) facilities. A large number of affiliations were not assessed due to limited data.

E-mailed RFIs accounted for 23 percent of all foreign attempts to collect ITAR. Most the E-mailed RFIs targeted information systems technology, sensor and lasers, and aeronautics respectively. In addition, E-mailed RFIs accounted for 20 percent of all foreign targeting directed at classified programs. More than half of the E-mailed requests were directed at sensor and laser technology including infrared decoy devices. Almost entirely, requests for ITAR and classified technologies

Figure 11

Request for Information (RFI)



were associated with a cleared defense contractor's web site and advertising on the Internet.

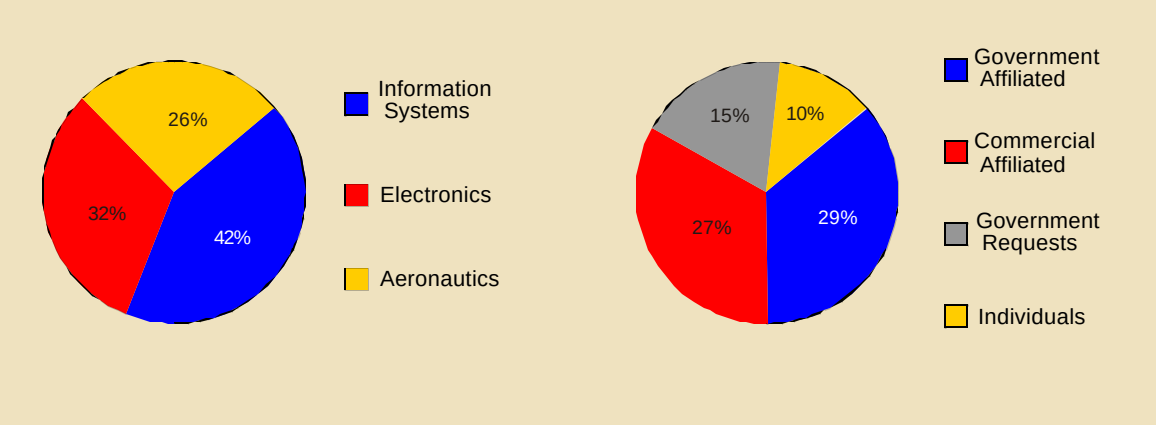
The following is a list of technology targeted by E-mailed RFI (the technologies are quoted exactly as they were received by cleared defense industry from a foreign entity):

- Aeroelasticity Research
- Radioisotope Thermoelectric Generator (RTG)
- MC9128 and MC9256 Cameras
- Robotics
- Airplane Design
- Warship Design
- Mark 58 Sparrow Missile Motor
- Hawk Defense Systems
- AN/FPS-108 Cobra
- PAPA Detectors

Mailed RFIs were the second most often used method for initiating RFI. The mailed RFI accounted for 11 percent of the total RFIs reported to DSS. The technologies targeted included marine systems, sensor and lasers, and aeronautics. For example, one individual sent two separate handwritten RFIs to the same company for DD-21 photographs. This same requestor continued to ask for shipyard and company information.

Figure 12

Attempted Acquisition



Twenty-two different countries used the letter RFI. This was the most diverse distribution of countries for any MO category. Letters tended to be handwritten and from individuals. In addition, letters came from both government-sponsored and affiliated entities equally as often. Surprisingly, no letter RFI was sent by a foreign commercial activity.

Telephone RFIs accounted for the third most reported type of RFI with six percent of the reporting. A total of 14 telephone requests were made by foreign entities. One-third of the requests were for armament and energetic materials including cable assemblies for bomb racks, missile detonator cord, and advanced propellants. Fifty percent of the telephone requests were made by foreign commercial activities.

Attempted Acquisition of U.S. Technology or Company

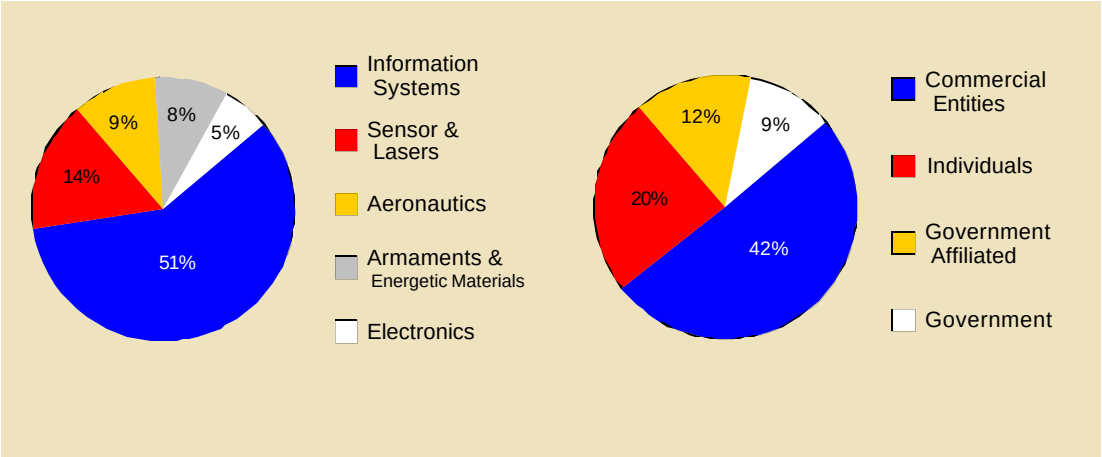
Acquisition was the second most used MO reported in 2001, up from fourth position in 1999 and third position in 2000. This MO includes attempted purchases of technology and requests for price lists. Tempest and UAV technology were most often requested for purchase while acquisition attempts tended to target sensor and lasers, armaments and energetic materials, information systems, aeronautics, and electronics.

Acquisition attempts were E-mailed 58 percent of the time. Fax, letter, and telephone RFIs also often preceded acquisition requests. Nineteen acquisition attempts were directed at classified technology. The following is a list of 11 targeted technologies receiving acquisition attempts:

- Patriot Missile Electrical Parts
- Radar Enhanced Surface Target Balloon
- Standard Infrared Radiation Model
- NBC Mask Handbook
- UAV Data Link Subsystems
- Photocell Vacuum
- C and Ku Antenna
- Monopulse Doppler Tracking Radar

Figure 13

Solicitation and Marketing of Services



- Multi-Channel Gamma Spectrometer
- UH-1H Helicopter Circuit Boards
- Spatial Light Modulators

Acquisitions accounted for 35 percent of total reported suspicious incidents believed to involve a third party. Third party involvement indicated a probability of technology transfer or diversion. Third parties are not the actual entity acquiring the technology but are ultimately the end user or recipient. Reports involving third parties include either a country with a history of third party sales or a country used by other foreign countries as a venue for acquiring denied technology. Thirty-five percent of the diversionary acquisitions involved airborne platforms, especially high tech components of UAV.

Solicitation and Marketing of Services

Solicitation and marketing of services dropped to third during this reporting year from last year's second place. Solicitation and marketing of services was the third most frequently reported MO in 1999, moving up from fourth place in 1998. Consistent with past reporting, individuals, companies and research facilities offer their technical and business services to U.S. research facilities, academic institutions and the cleared contractors in 2001.

The following is a list of technologies targeted using the solicitation and marketing of services MO:

- Active Electronic Scanned Array Radar
- Low Observable Technology
- Unmanned Underwater Vehicle
- Magnetrons
- Joint Tactical Information Distribution System
- Objective Infantry Combat Weapon
- GSM, Wireless Technology
- Javelin UAV
- Optical Grade Germanium Blanks
- Microwave Components

Offshore software development solicitations accounted for 20 percent of all marketing and solicitations directed at cleared facilities. All solicitations were E-mailed and predominantly originated at commercial entities in Eurasia and a nation embargoed during most of 2001. In addition, most were associated with mass E-mail. The solicitations offered offshore software development and marketing representation in the foreign country. All solicitations were directed at the web sites of cleared facilities. At least one foreign entity sent three separate solicitations to different cleared facilities.

The resume solicitation accounted for 14 percent of all marketing and solicitations directed at cleared facilities. Most were sent by individuals and were associated with both educational and industrial experiences. Aeronautic and information systems experiences were the two most proffered categories.

Foreign Targeting of Legal U.S. Travelers Abroad

DSS saw an increase in the level of reporting on foreign collection missions directed against U.S. legal travelers. Since increased amounts of foreign collection activity are occurring, DSS decided to consider foreign collection missions directed against U.S. legal travelers an MO for collecting U.S. technology from U.S. cleared defense employees. This new MO falls under security for reporting purposes at DSS. At the end of the reporting year, foreign targeting of legal U.S. travelers abroad was the fourth most utilized MO for targeting U.S. critical technology, which is up from a three-way tie for sixth place for frequency of use by foreign entities last year.

Events held on the collector's home territory leave legal U.S. travelers vulnerable to exploitation by traditional Foreign Intelligence Service (FIS) tradecraft, e.g. electronic surveillance. Entrapment ploys such as inducement of the target into a compromising situation, which put the legal traveler at risk were also used. Cleared defense contractors should use caution and review the type and amount of information contained in the registration, biographic and other materials requested by the host country. A number of events that caused legal U.S. travelers to be recognized by FIS included international conventions, combined military operations, and joint ventures.

In other cases, short-term custodial detentions by host government officials occur at ports including both airports and waterways during which foreign officials attempt to gain information regarding the U.S. traveler's visit. These detentions tend to disrupt travel. Fifty-eight percent of the reporting in this category received from cleared contractors related to custodial detentions including search and seizure.

For targeting purposes, DSS contends the security clearance level and access to a particular technology that the legal traveler possesses are of great value to the FIS collection effort. The following is a list of technology targeted:

- Comanche
- F404 Engine

Figure 14 Foreign Targeting of Legal US Travelers Abroad

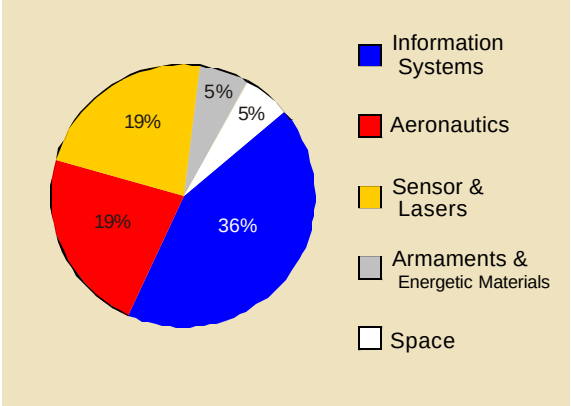


Table 8

Exploitation of Foreign Visits	
Percentage of foreign visits conducted on behalf of a foreign government and foreign government affiliated entity.	82%

- JSTARS
- SH-60 Sea Hawk
- Synthetic Aperture Radar
- RD-180 Atlas Engine
- Joint Land Attack Cruise Missile Defense Elevated Netted Sensor (JLENS)
- Patriot
- AN/ALQ-135 Tactical Electronic Warfare System
- Digital Radio Frequency Memory (DRFM)

Exploitation of Foreign Visit

Exploitation of foreign visit reports concerning suspected exploitation of visits to U.S. facilities dropped to fifth in frequency of reporting down from last year where this MO stood at fourth. The term "foreign visitor" includes one-time visits, long-term visitors (such as exchange employees, official government representatives and students) and frequent visitors (such as foreign sales representatives). Suspicious conduct includes actions before, during, and after a visit. The one factor, which made many foreign visits suspicious, was the extent to which the foreign visitor would request access to facilities or to discuss information outside the scope of approved activities.

In several incidents in 2001, foreign visitors ignored security required by a company's technology control plans (TCP). A TCP stipulates how a company will protect its technology. The plan establishes procedures to protect classified, proprietary, and export-controlled information; to control access by foreign visitors; and to control access by employees who are non-U.S. persons.

The following is a list of technologies targeted:

- Seawater Pumps
- Explosives
- Eutectic Technology
- M1A1 Tank Simulation
- Scramjet Motors
- WJ-8629 Signal Surveillance
- Vessel Traffic System (VTS)
- Crusader
- Spark Gap Switches
- Camouflage against Infrared Detection

Figure 15

Exploitation of Foreign Visit

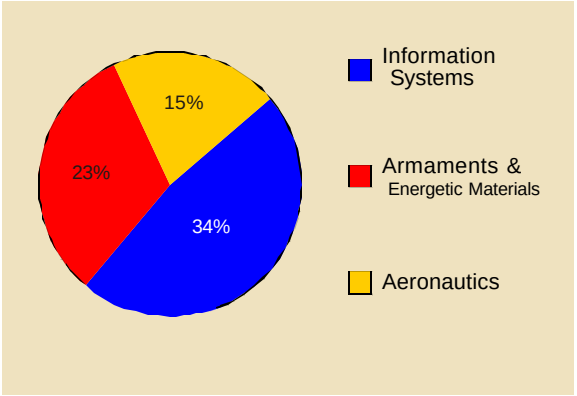
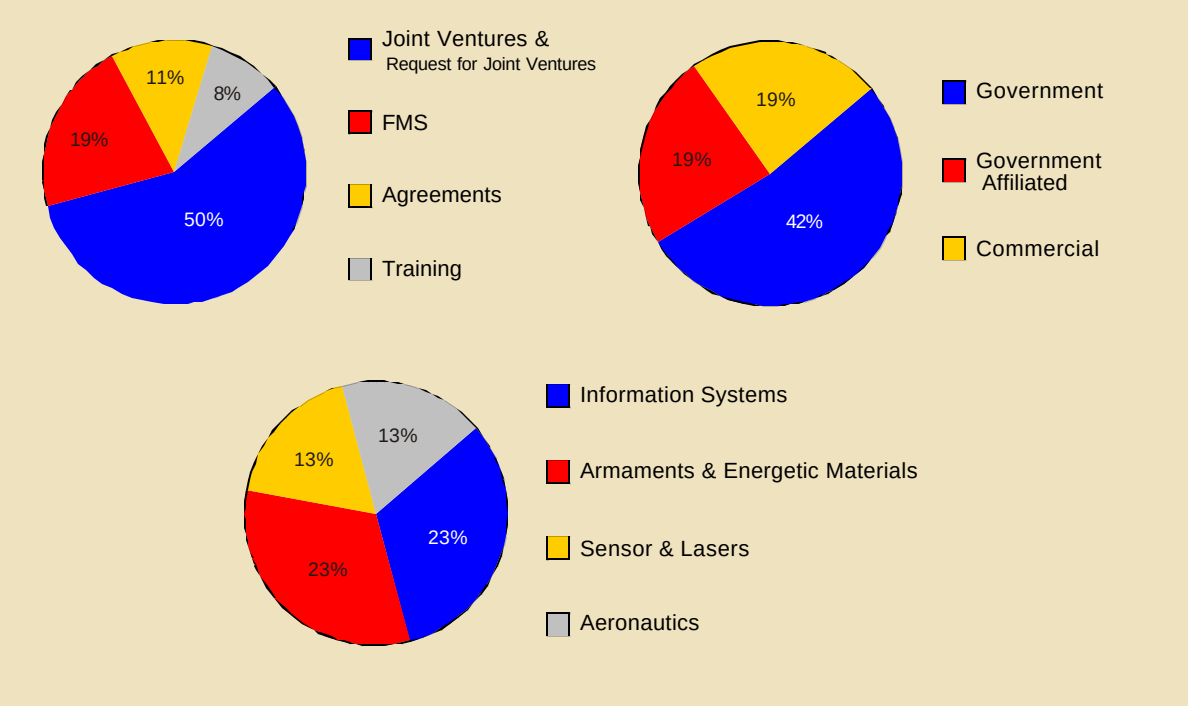


Figure 16

Exploitation of Existing Relationships



Exploitation of Existing Relationships

Associations, or exploitation of existing relationship (EOR), previously titled joint venture and research, remained sixth in frequency of use. This MO offers significant collection opportunities for foreign interests and venues for expanding foreign interests' own industrial base without having to pay for the research and development. As with frequent foreign visits and other international programs, joint ventures place foreign personnel in close proximity to U.S. personnel and technology and can facilitate access to protected programs.

Exploitation of existing relationships include the following areas: joint venture, foreign military sale (FMS), agreements, training, and requests for joint venture.

The following is a list of specific technologies targeted during the exploitation of a relationship:

- Joint Direct Attack Munitions
- Focal Plane Array Technology
- Arrow Missile ADA Program
- Multiple Launch Rocket System
- OH-58D Kiowa Warrior
- Sparrow Missile
- TPS Radar Training
- Acoustic Sensors

Exploitation of Internet

Targeting associated with exploitation of the Internet (hacking) fell to seventh place in use of frequency by foreign entities from sixth place last reporting year. DSS maintains security cognizance regarding classified systems.

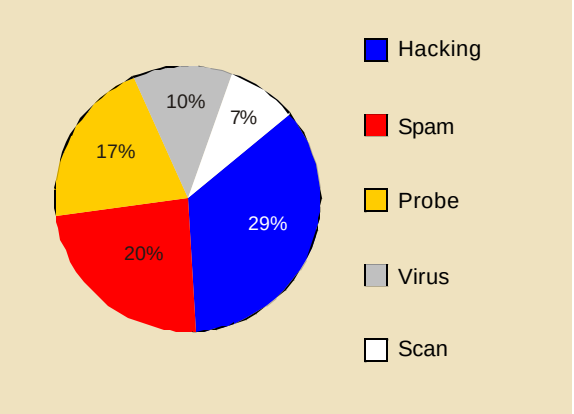
The majority of Internet endeavors were correlated with probing efforts, which account for the majority of activity in this category. This category is not related to the Internet-based RFI. The computer probes are most likely searching for potential weaknesses in systems for exploitation. By detecting probes, the cleared companies already demonstrated they have the SCMs in place to thwart attempts to penetrate their computer systems. Although probing a system is legal, once a port is breached, a crime is committed.

Internet activity is broken out into the following categories: hack, probe, scan, ping, spam, and virus. In all cases, except spam, DSS relates to the activity in the way the cleared contractor reports the incident. For example, a cleared contractor's Information Security Officer reported "probes" occurred during a time when his company was in negotiations with a foreign entity. DSS looks at an E-mail for signs of spamming such as having the same E-mail already annotated in our database or by finding an exact example of the same E-mail on another web site, or by conducting either a reverse IP search or domain look up and discovering if the registrant is a mass mailing company.

Most hacking events ended as defacements with derogatory remarks. Other hacking events included attempts to download information, Trojan horses, and penetrations of firewalls.

Figure 17

Exploitation of Internet



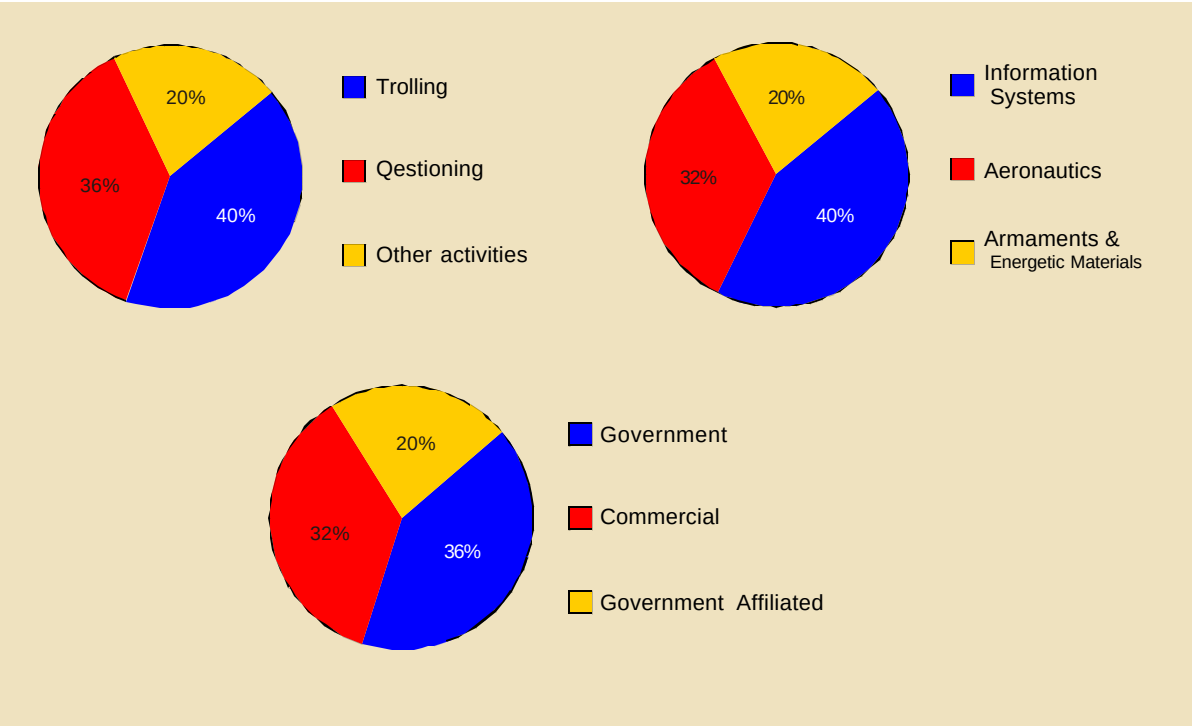
Targeting at Conventions

Targeting at conventions moved down to eighth position from fifth place in frequency of use by foreign entities in the previous year. One explanation for why reporting is down in an apparently "target rich" environment for foreign intelligence collection is that U.S. attendees are marketing personnel rather than the more knowledgeable engineers. Marketing personnel usually are not cleared employees and this is of less value to foreign collectors. Additionally, they do not receive the more informative classified threat briefings, which would facilitate higher levels of reporting. Conventions, however, continue to directly link U.S. programs and technologies with knowledgeable personnel. International exhibits provide a unique opportunity for foreign entities to study, compare, and photograph actual products in one location.

All these technology groups are associated with international conventions. Some technologies targeted at conventions include:

Figure 18

Targeting at Conventions



- F110-129 Engine
- UAV Technology
- Joint Strike Fighter
- Rhenium Powder Metallurgy
- Parametric Airborne Dipping Sonar (PADS)
- Sensor Fuzed Weapons
- AIM-9X Sidewinder
- Information Systems
- Storage Area Networks

The audiences at international seminars are composed principally of leading national scientists and technical experts, who pose more of a threat than intelligence officers due to their level of technical understanding lead. Technical experts focus their questions and requests on specific technical areas having direct application to their work. Reports show during seminars, foreign entities attempted subtle approaches such as sitting next to a potential target and initiating a casual conversation. This establishes a point of contact that may later be subjected to exploitation. The use of membership lists of international business and technical societies as a source to identify potential targets and as a means of introduction is increasing. Because the threat is designed to compromise the cleared defense employee, the approach will be subtle and unrecognizable. The targeting will be directed at U.S. persons with cultural commonalties such as origin of birth, religion, and language.

Of note this year is the increased use of foreign professional groups contacting U.S. academic and technology experts via their academic affiliation, R&D association, or professional memberships. Foreign professional groups use these well-established platforms for collection, gleaning information for their technological needs. An example was the use of a non-profit technical professional association with more than 360,000 individual members in 150 countries. This association, internationally recognized, sponsors conferences and symposiums in the furtherance of information exchange. DSS received reports regarding several foreign E-mailed requests made to cleared defense contractors. The foreign entities used this platform to offer an exchange of ideas. The E-mailed requests involved exchanges of information on sensors to detect electrode for training welding, packaging and manufacturing technology, and battery chemistry.

Assessment of Future Trends

The weapon systems of tomorrow will demand high technology in nearly every venue. Foreign entities will continue collection attempts against cleared contractors in pursuit of these technologies. Information systems will remain in the forefront of sought-after commodities, primarily by foreign government and affiliated collectors. Armaments and energetic materials will continue to be heavily targeted by various foreign entities, with emphasis on less technologically developed nations and non-government-sponsored, or affiliated entities. Biological, Incendiary, Chemical, and High-Explosive (B-NICE) technologies to include protective and decontamination equipment will be targeted.

As DSS assessed in the 2001 Trends, nongovernment-affiliated or sponsored entities will continue to increase their collection efforts against cleared contractors. Universities, commercial entities, and individual persons will attempt collection against U.S. technologies, employing E-mail as the primary method of operation.

Foreign collectors will continue the use of front companies or cooperative or unwitting third-party entities to obtain denied technology. These foreign collectors will attempt to divert dual-use and export-controlled technology through these third party entities, employing various means of shipment to include freight-forwarders and overseas sales brokers.

Cleared contractors will continue to be targeted by foreign entities using various MOs and must adopt a proactive security posture through training and SCMs to thwart these attempts and protect our nation's militarily critical technologies.