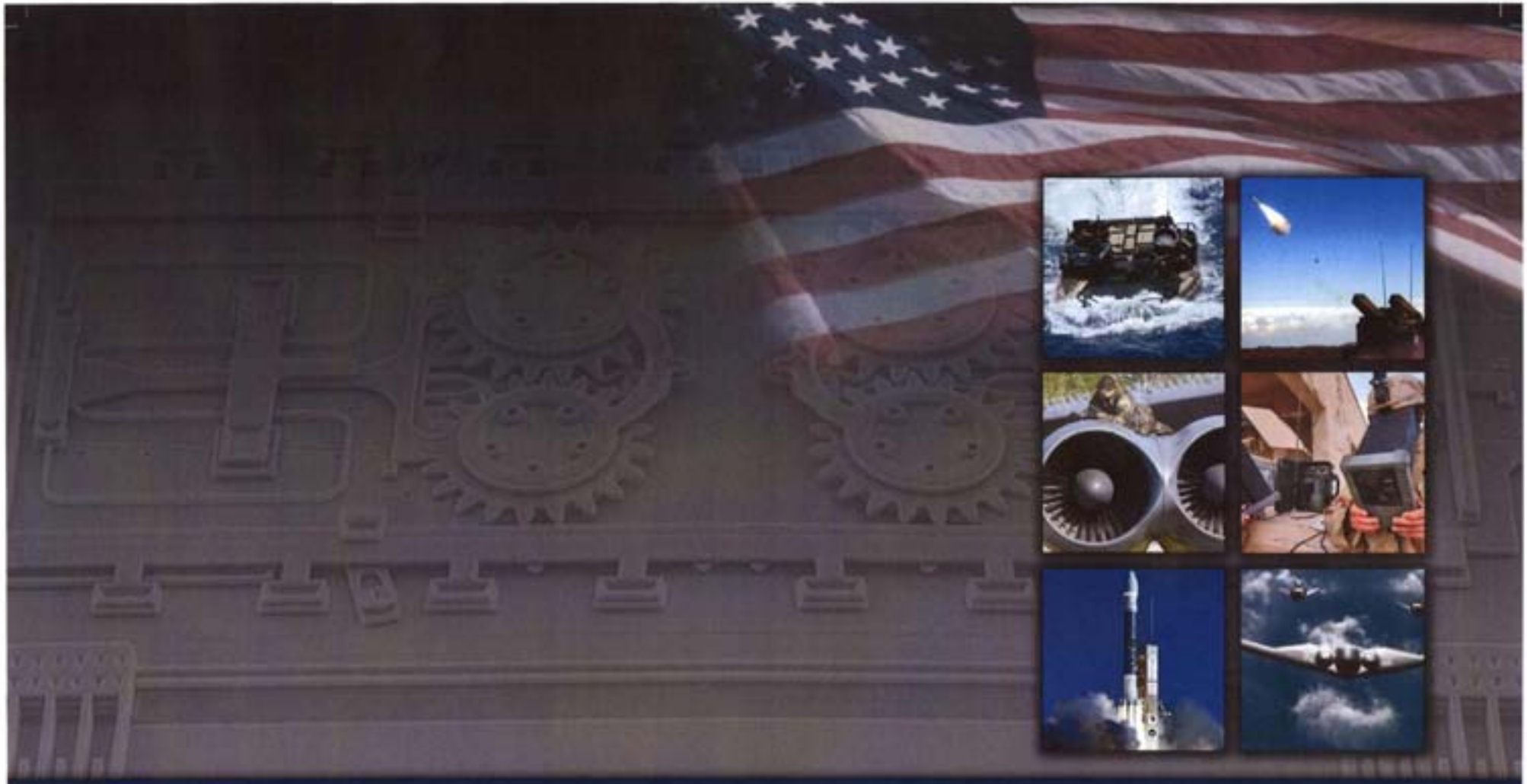


Technology Collection Trends in the U.S. Defense Industry - 2005

This publication has been produced by the Defense Security Service for use by DoD Contractors and Government Agencies as part of their security programs.

Questions and requests to further distribute this publication should be addressed to the Defense Security Service Public Affairs Office.

Foreword

The Defense Security Service (DSS) is responsible for assisting cleared defense industry in the identification and reporting of foreign contacts and collection attempts, as outlined in the National Industrial Security Program Operating Manual (NISPOM). The development of an annual trends document is a direct result of the efforts by cleared defense contractors reporting suspicious activity to their facility security officers and ultimately to DSS.

DSS intends the results and analysis contained in this report to be used by security officials, cleared contractors, intelligence professionals, and DoD policy and decision-makers. The annual trends document covers some of the most important topics associated with foreign targeting and collection attempts directed at the defense industry, including technologies being targeted, how targeting is accomplished, and where it originates.

The goal of DSS is to provide the community with technology collection trends that will help improve threat awareness and technology protection related to foreign collection attempts directed at the U.S. defense industry. DSS strongly encourages continued reporting of suspicious contact reports to DSS field offices. Prompt reporting of foreign collection activity is critical to an effective industrial security program.

H. Anderson
Acting Director, Defense Security Service (DSS)

Contents

Front cover background photo courtesy of Sandia National Laboratories, SUMMiT™ Technologies. All other photos courtesy of the Department of Defense.

The 9th Annual Defense Technology Collection Trends publication was prepared by the Defense Security Service Counterintelligence (DSSCI) Office. Comment and queries are welcome and may be directed to the DSS Counterintelligence Office, 1340 Braddock Place, Alexandria, VA 22314-1651.

Approved for public release, ASDA(PA)/05-S-2289

I. INTRODUCTION

The Defense Security Service (DSS) Counterintelligence (CI) Office presents the 9th annual trends document as a tool for security professionals. The trends and analytical assessments in this publication are based entirely on reports of suspicious foreign activity communicated by DSS industrial security representatives and DSS Field CI Specialists. These reports are composed of information provided by U.S. cleared defense contractors and industry personnel who identify suspicious foreign activity.

The U.S. defense industry develops and produces the bulk of our nation's defense technology and plays a significant role in creating and protecting the information that is critical to national security. The National Industrial Security Program (NISP) was established to ensure that the cleared U.S. defense industry safeguards classified information in its possession while performing work on bids, contracts, programs, or research and development efforts.

Based on significant analytical effort, this publication provides general information and draws conclusions that help cleared company employees and DSS personnel recognize and report suspicious foreign activity. In addition, DSS aims to improve this document each year based on comments and suggestions that are received from the community. Noteworthy changes this year include the transition to Section III "Emerging Critical Technologies" from the Militarily Critical Technologies List (MCTL). This section places greater emphasis on sensitive developing technologies and provides a higher degree of specificity for understanding the technologies targeted.

Through research presented in this document, DSS provides cleared contractors with a tool to enact responsive, threat appropriate, and cost-effective Security Countermeasures (SCM). Furthermore, government agencies are encouraged to use this report to evaluate their own threat environments and, when necessary, develop additional security countermeasures based on trends identified in this document.

II. EXECUTIVE SUMMARY

A. Reporting Trends

This report is based on an analysis of 995 suspicious contact reports received in Fiscal Year 2004 from cleared defense contractors, DSS Industrial Security Representatives (ISR), and Field CI Specialists (FCIS). While there was a greater number of reports in 2003, the overall reporting base for 2004 was larger. This means that more of the defense industrial base participated in reporting incidents this year, resulting in a study with greater depth and more representative of the industry as a whole.

An emerging global market, dependent upon mass communication, opens the door for legitimate profitable business opportunities to become the targets of subversive attempts by foreign entities to gain access to emerging sensitive technologies from the United States. This year's greater breadth of reporting is the result of better communication between the ISR, FCIS, and the defense industry. It also reflects a greater range of collection attempts based on the ability of collectors to communicate easily in the global market.

It should be noted that percentages given throughout this document may not total to exactly 100 percent due to rounding.

B. Country Trends

In 2004, DSS identified 90 countries associated with suspicious activities based on U.S. defense industry reporting, up from 85 countries in 2003. These results should not be taken to imply that the same 85 countries engaged in targeting U.S. defense technologies in 2003 remained involved in such activities in 2004. Of the 90 countries identified by DSS as collectors of sensitive and classified U.S.defense technologies in 2004, only 72 were also identified as collectors in 2003. Fourteen countries identified in 2003 data were absent from U.S. defense industry reporting to DSS in 2004. Eighteen additional countries were identified in the same reporting that had not previously been noted as active collectors in 2003. Furthermore, in 2004, the top ten collecting countries accounted for 56.6 percent of all suspicious activity, while the top five represented 40.5 percent of all suspicious activity.

C. Technology Interests Trends

In 2004, technology collection focused more on dual-use technologies than militarily specific technology. A significant amount of reporting centered around the targeting of sensitive but unclassified technologies and export controlled technologies. While interest in classified technologies remains high, traditional and non-traditional collectors realize the cost benefit of targeting sensitive, export-controlled technologies for diversion. These technologies are frequently cutting edge and provide the collector the advantage of saving time and costs associated with indigenous development of new technologies. Trends this year indicate a continued interest in targeting at the component and subcomponent level vice the targeting of complete weapons systems. Additionally, suspicious activity in 2004 included the targeting of all 20 militarily-critical technology categories, as identified in the Militarily Critical Technologies List (MCTL).

D. Most Frequently Reported Technology Targets

Technologies generating the most foreign interest in 2004 (by frequency of targeting):

- Information Technology - 21.0%
- Sensors - 12.6%
- Aeronautics - 11.8%
- Electronics - 11.1%
- Armaments & Energetic Materials - 9.6%
- Lasers and Optics - 7.5%

- Signature Control Technology - 4.7%
- Materials and Processing Technology - 3.3%
- Chemical Technology - 3.0%
- Space Systems - 2.7%

This year marked a transition from the Militarily Critical Technology List, Volume II to Volume III. This change in technology classification is focused on the developing and critical technologies that enable advanced U.S. defense capabilities. The new list raises the overall number of technology categories from 18 to 20. The division of the Chemical and Biological Systems category and the Sensors and Lasers category into two technology categories each accounts for the increase in number of technology categories.

The top ten technologies noted above accounted for 87.3 percent of all targeting. Signature Control, Aeronautics, and Electronics experienced notable increases in 2004. The most dramatic increase was that of Signature Control which experienced a 375 percent increase as compared to 2003 data. Targeting against Space Systems decreased by 32 percent.

E. Most Frequently Reported Foreign Collection Methods of Operation (MO):

Methods of Operation (MO) are the techniques utilized by foreign entities in an attempt to collect intelligence, scientific and technical information. In 2004, the MO associated with attempted collection efforts in order of targeting frequency included:

- Request for Information - 47.5%
- Acquisition of Controlled Technology - 20.0%
- Solicitation of Marketing Services - 13.1%
- Exploitation of Relationships - 5.3%
- Exploitation of a Foreign Visit (CONUS) - 5.1%
- Other - 2.9%
- Targeting at Conventions/Expositions/ Seminars - 2.8%
- Suspicious Internet Activity - 2.6%
- Foreign Employees - 0.4%
- Cultural Commonality - 0.3%

The top three MOs were used in 80.6 percent of all foreign collection attempts reported to DSS. Although Request for Information continued to be the most utilized MO, the use of Acquisition of Controlled Technology as an MO increased by 33 percent. In addition, collectors continued to use a combination of methodologies with a request for information often evolving into an acquisition attempt. Suspicious Internet Activity remained steady, but contributed to some of the most successful technology collection events.

III. WORLD COLLECTION TRENDS

Table 01. World Collection Trends - 1997 to 2004								
Year	1997	1998	1999	2000	2001	2002	2003	2004
Number of Countries with Identified Collection Activities	37	47	56	63	75	84	85	90

A. Worldwide Breakdown by Region. In 2004, DSS identified 90 countries associated with suspicious collection activities. This was an increase of five targeting countries as compared to 2003 data. While the final numbers between years reveal a difference of five countries, the difference in the actual countries targeting in those years is broader. For example, there were 14 countries with reported collection attempts in 2003 that did not garner suspicious contact reports in 2004. In addition, there were 18 countries identified with suspicious contact reporting in 2004 that did not appear in 2003 data. The combination of this information reveals that over the two year period of 2003 - 2004, 103 different countries reportedly attempted to collect U.S. sensitive and classified information. While many of these countries are as technologically advanced as the United States, others are either developing or underdeveloped.

The regions in Figure 01 are organized by the United States Department of State's six regional groupings. The regions represent geographically bound countries that share political, religious, and social similarities. In 2004, the majority of reported targeting originated from East Asia and the Pacific which accounted for 26.8 percent of all reporting. East Asian collection attempts were followed by attempts from Eurasia at 22.4 percent, the Near East at 20.9 percent, and South Asia at 17.3 percent of total targeting. The Western Hemisphere and Africa accounted for the minority of targeting in all technology categories for the period, with a combined overall total of 12.5 percent of the reported targeting in 2004.

B. Foreign Collectors. DSS identifies types of collectors after evaluating reported information, conducting extensive research, and assessing relationships and representatives in each incident. Each collection attempt is categorized as

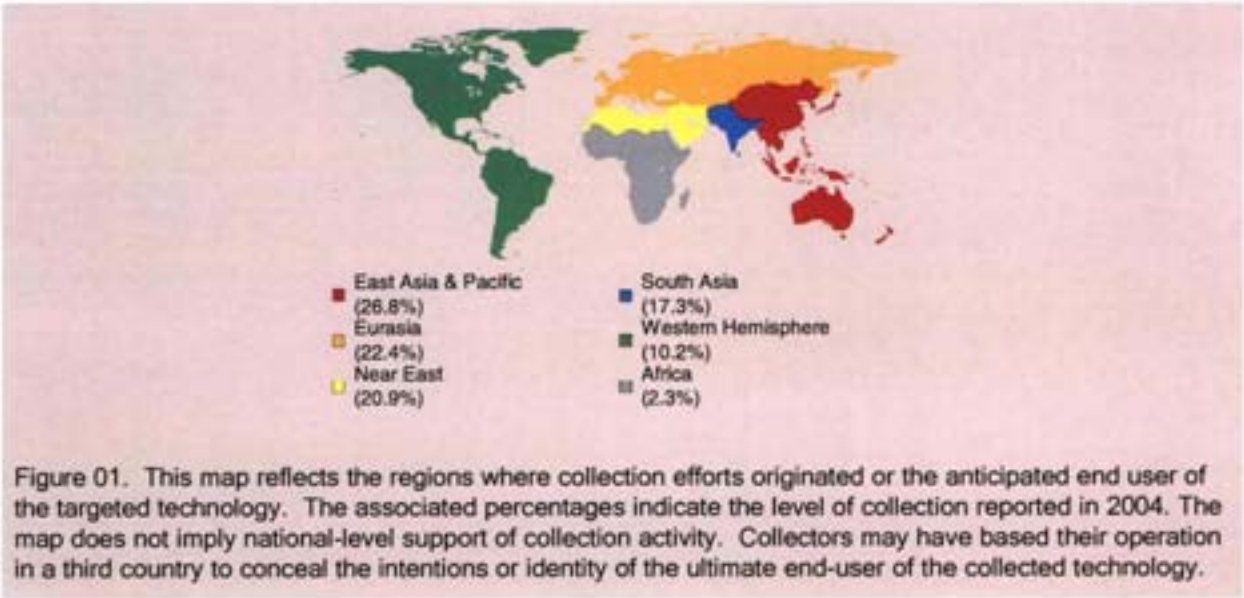


Figure 01. This map reflects the regions where collection efforts originated or the anticipated end user of the targeted technology. The associated percentages indicate the level of collection reported in 2004. The map does not imply national-level support of collection activity. Collectors may have based their operation in a third country to conceal the intentions or identity of the ultimate end-user of the collected technology.

originating for either a government, government affiliation, commercial, individual, or unknown entity.

Foreign government sponsored targeting, which includes Ministry of Defense, Intelligence Officers (including foreign military attaches), and other official government entities accounted for 21 percent of all reported cases in 2004. This represented a marked increase from 2003 for "traditional" (direct foreign government) targeting.

Conversely, the reported targeting by government affiliated collectors experienced a 43 percent decrease from 2003. Foreign government-affiliated collection includes research institutes, laboratories, government-funded universities, and contractors representing governments. Foreign companies whose work is exclusively or predominantly in support of government agencies are also included as government-affiliates. Government affiliated entities accounted for 25 percent of all targeting in 2003, but in 2004 accounted for only 15 percent of targeting.

Collection attempts by commercial entities remained steady with a slight four percent rise in targeting. Foreign commercial activities include those companies engaged in business, in the commercial and defense sectors, whose suspicious activity is not identified with a foreign government. Many of these commercial collectors may be acting in response to foreign government issued requests for products and technology that will be incorporated into indigenous weapons systems.

Targeting by individual foreign collectors decreased slightly in 2004. Foreign individuals include those individuals for whom DSS has been unable to identify an affiliation due to a lack of information (where only a name or e-mail address is known). It is clear that the majority of these incidents involved foreign sponsorship or affiliation; however, a small percentage were identified as seeking personal financial gain.

Entities with no known affiliation conducted at least 16 percent of targeting. This group of collection attempts included very little clarifying information and frequently did not include the name of the requester, email, or any other identifying information.

C. Methods of Operation. DSS analyzes each collection attempt to determine the method of operation used by a collector which allows for a better understanding of the tools and techniques used to target the U.S. defense industry. The direct request for information was the most commonly applied method of operation in FY04. These events are commonly associated with email, phone, and direct mail correspondence to a facility. The correspondence poses specific detailed questions that entail the release of sensitive or classified information if answered.

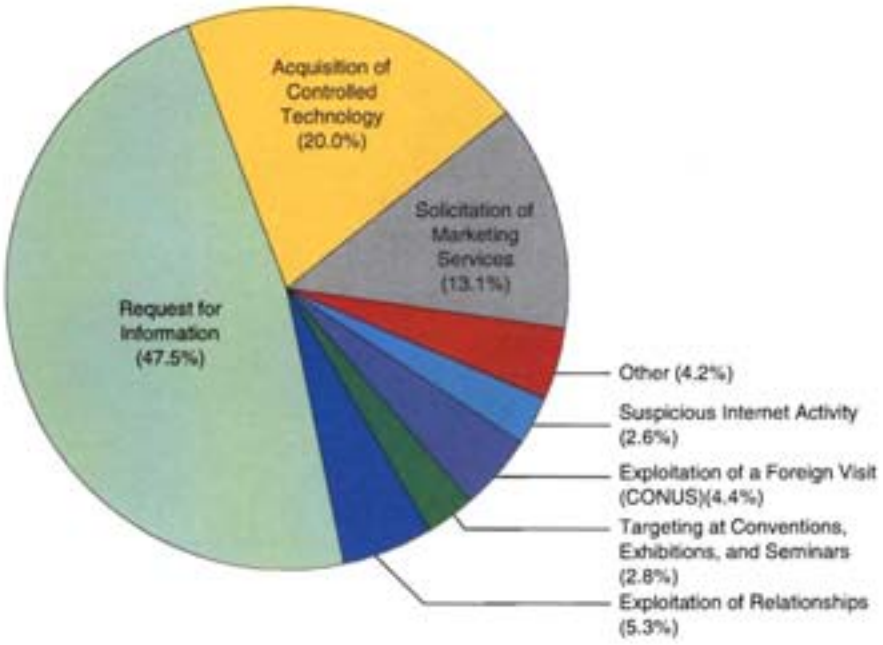
In 2004, 47.5 percent of all reported collection attempts involved a request for information. This represents is a slight decrease from 2003 data, and is attributed to the increase in acquisition as a means to collect technology. This year the use of Acquisition of Technology as a method to collect information and technology increased by 33 percent and accounted for 20.0 percent of all reported cases. These events appear to be legitimate sales opportunities for contractors, but will eventually involve the violation of export laws or illegal diversion of the purchased technology to an unlawful end user.

The third most popular method was Solicitation and Marketing of Services which experienced a slight decrease in 2004 and accounted for 13.1 percent of all collection attempts. Exploitation of Relationships again placed fourth in 2004 at 5.3 percent. Fifth, Exploitation of a Foreign Visit (CONUS) as method of operation increased, with the number of cases involving

this method doubling between 2003 and 2004, accounting for 5.1 percent of all targeting.

All other methods of operation combined for the remaining 9 percent of collection attempts reported in 2004. While these methods are not as broadly used as the previously mentioned methods, it does not imply that these methods of operation are any less successful or pose a lesser threat to U.S. defense technologies. This is truly evident with the method of Suspicious Internet Activity. Although this method accounted for only 2.6 percent of the total targeting, the potential for the collection of information from just one computer intrusion event is exponentially more damaging than that of other methods.

Figure 02. Methods of Operation in 2004



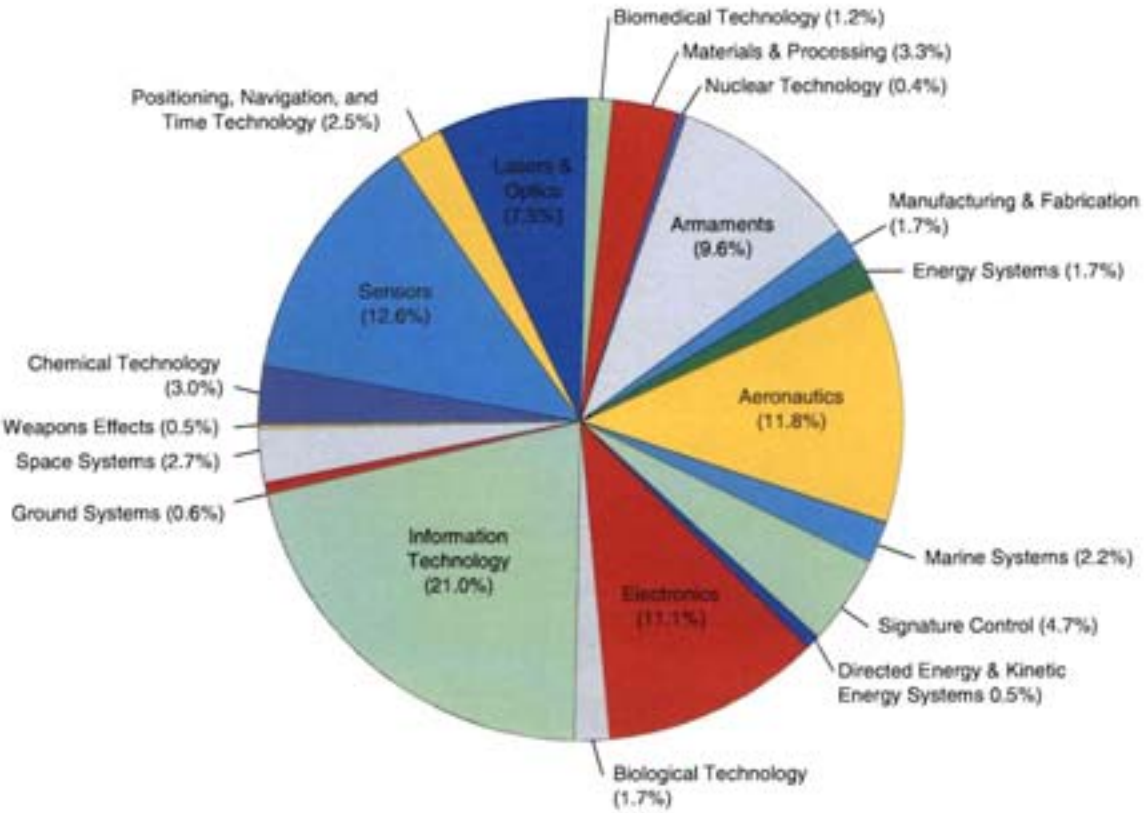
IV. TECHNOLOGY SECTION

DSS documents and reviews foreign interests in critical U.S. defense technology in 20 categories, up from 18 categories in 2004. These technologies are broken out in the Military Critical Technology List (MCTL), Volume III, and serve as the blueprint used by DSS to define categories and subcategories for each technology. The MCTL Vol. III is a detailed and structured compendium of emerging technologies the Department of Defense (DoD) assesses to be critical to maintaining superior U.S. military capabilities.

It should be noted that although DSS recorded 995 suspicious cases, some of the cases reported collection against multiple technologies. Therefore, the percentages for targeting are based on the number of collection attempts against the MCTL categories and not the total number of DSS cases. Specifically, the total number of collection attempts against all MCTL technology combined for 1208 incidents.

This methodology allows DSS to understand the true scope of collection without limiting statistical analysis to one technology collection event per case.

Figure 03. Targeting Against MCTL Vol. III Categories in 2004



A. INFORMATION SYSTEMS TECHNOLOGY

Overview

Fiscal Year 2004 experienced an increase of approximately 3 percent in the number of foreign entities targeting Information Systems (IS) technologies. With respect to defense technologies as a whole, however, Information Systems were targeted at a rate almost twice that of any other technology category. These statistics are consistent with FY03 levels.

A disturbing trend for the reporting period was the targeting by commercial entities, based in U.S.-friendly countries, that retain close ties with countries regarded as potential adversaries and/or threats to U.S. national security.

General information and communication systems were the most targeted subcategories of Information Systems accounting for 45.3 and 20.4 percent, respectively, of all reported cases.

The targeting of modeling and simulation technologies exhibited a marked increase over FY03 reporting, increasing eight-fold in FY04 to almost 9 percent of the overall total in this technology category. There was no discernable pattern with respect to the type of modeling and simulation technologies targeted. However, the East Asia and Pacific region was the most active in collecting against this specific subcategory, responsible for approximately 42 percent of targeting.

Image 01. A soldier adjusts outriggers on a Very Small Aperture Terminal (VSAT) satellite system. (Photo Courtesy of U.S. Army/Mike Kane.)

MCTL Vol. III Technology Categories

Table 02, below, shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Information Systems Technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Table 02. MCTL Vol. III - Information Systems Technology Sub-Categories in 2004.

Sub-Category	Percent
Information Systems Technology	45.3
Information Communications	20.4
Information Exchange	2.6
Information Processing	9.9
Information Security	4.7
Information Management and Control	1.1
Information Systems Facilities	2.9
Information Sensing	1.8
Information Visualization and Representation	2.6
Modeling and Simulation	8.8

Collection Attempts by Region

Countries of the East Asia and Pacific region were the most active collector in this technology category during FY04, accounting for 26.6 percent of all reported attempts. Countries of the Near East and Eurasia were a close second and third at 21.9 and 20.9 percent respectively. The South Asia region was fourth at 17.2 percent, followed by the Western Hemisphere and Africa at 10.1 and 3.4 percent respectively.

Figure 04. Collection Activity by Region for Information Systems Technology in FY04

Methods of Operation

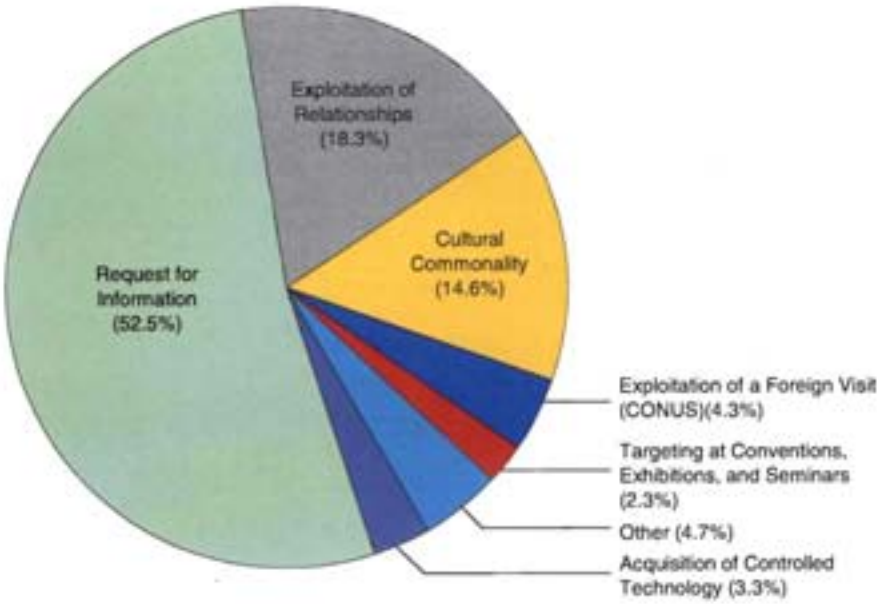
Approximately 52.5 percent of Information Systems targeting involved foreign Requests for Information (RFI), with commercial entities representing the largest group of collectors to employ the methodology.

Table 03. Affiliation of Collectors Targeting Information Systems Technology in 2004

Affiliation Type	Percent
Commercial	41.7
Government	16.5
Government Affiliated	16.1
Individual	8.3
Unknown	17.3

The use of hacking and security vulnerabilities to compromise U.S. contractors' unclassified systems became a serious concern during the

Figure 05. Methods of Operation: Information Systems Technology Collection Attempts



FY04 reporting period, with at least one successful compromise of a contractor's internet web site. While the use of this method was infrequent relative to other methods of operation, it should be noted that a single compromised system could negatively impact several U.S. developing technologies and weapons systems, resulting in significant losses.

Information Systems Collection Attempt

Image 02. U.S. Army Battlefield Medical Information System-Telemedicine (BMIS-T) (Photo Courtesy of the U.S. Army.)

In March 2004, a cleared defense contractor reported a collection event when what appeared at first to be a legitimate purchase of ruggedized Personal Digital Assistants (PDAs) became suspicious. The buyer implied that the end user of the technology was a U.S. customer, but then later confided to the sales rep that the end user was a foreign government. The buyer stated that the information should not be shared with anyone, The version of the PDA that the individual was attempting to acquire is export controlled and designed for military applications. The contractor successfully recognized several indicators of suspicious behavior that included the buyer's use of a free email service, insistence on purchasing the military version of the product, and requesting a demonstration unit.

B. SENSORS TECHNOLOGY

Overview

Fiscal Year 2004 marks the first year DSS separated Sensor and Laser technologies into two categories in accordance with MCTL Vol. III. Although this breakdown reduces the overall number of cases attributed to each category, sensors remained the second most sought after technology in 2004, at 12.6 percent of all collection efforts.

This year, the number of countries requesting sensor technologies experienced a slight decrease from last year, down from 46 to 41. Just over 29 percent of all foreign collection attempts for sensors focused on radar programs, with electro-optic sensors receiving 12.6 percent. The majority of foreign requests pertaining to radar programs sought software and simulation modules used to test radar capabilities.

Surveillance radar systems experienced an increase in targeting during 2004. Email requests for the Joint Surveillance Target Attack Radar System (JSTARS) were sent directly to cleared contractors. JSTARS is a long-range, air-to-ground surveillance system designed to locate, classify and track ground targets in all weather conditions. The JSTARS system is designed to detect, locate and track moving and stationary ground equipment targets, is used primarily by U.S. Armed Forces, and undergoes continual upgrades and improvements.

MCTL Vol. III Technology Categories

Table 04, below, shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Sensor technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Table 04. MCTL Vol. III - Sensors Technology Sub-Categories in 2004.

Subcategory	Percent
Sensors	45.7
Acoustic Sensors, Terrestrial Platform	0.7
Acoustic Sensors, Marine, Active Sonar	0.7
Acoustic Sensors, Marine, Passive Sonar	8.6
Acoustic Sensors, Marine Platform	2.6
Electro-optical Sensors	12.6
Radar	29.1
Land Mine Countermeasures	0.0
Sea and Littoral Region Mine Countermeasures	0.0

Image 03. The E-8C Joint Surveillance Target Attack Radar System (JSTARS) is the only airborne platform in operation that can maintain realtime surveillance over a corps-sized area on the battlefield. A joint Air Force-Army program, the JSTARS uses a multi-mode side-looking radar to detect, track, and classify moving ground vehicles deep behind enemy lines in all conditions. (Photo Courtesy of the U.S. Air Force.)

Collection Attempts by Region

Countries of Eurasia were tied with countries of the Near East as the most active collectors of sensor technologies during FY04, accounting for 24.5 percent each of all reported attempts. East Asia and the Pacific region was third at

Figure 06. Collection Activity by Region for Sensors Technology in FY04

20.4 percent, followed by South Asia, the Western Hemisphere and Africa at 17 percent, 10.2 percent and 3.4 percent respectively.

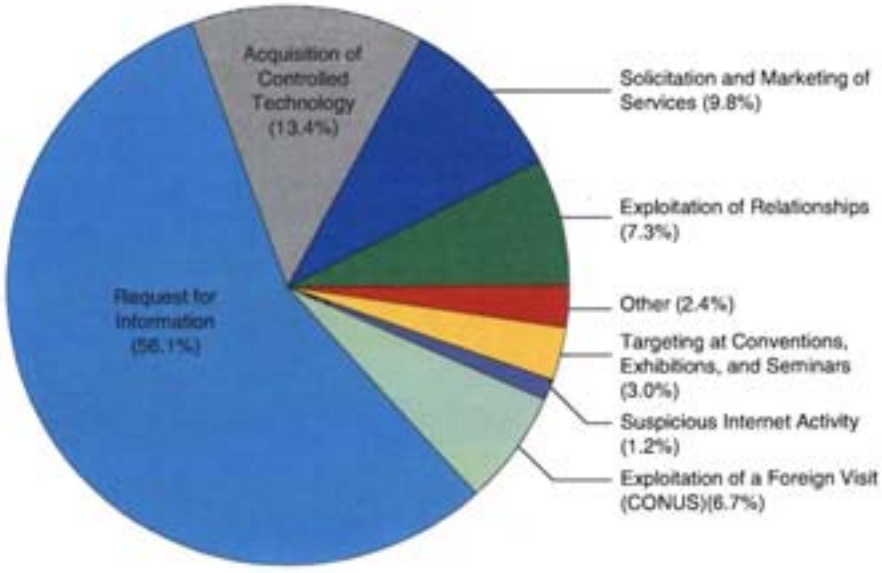
Methods of Operation

Request for Information was the most frequently utilized MO used by foreign collectors during this period, relating to 56.1 percent of reporting in this technology category. Acquisition of Controlled Technology was a distant second, at 13.4 percent, and Solicitation and Marketing of Services, third at 9.8 percent.

Table 05. Affiliation of Collectors Targeting Sensors Technology in 2004	
Affiliation Type	**Percent**
Commercial	34.1
Government	26.8
Government Affiliated	14.5
Individual	10.9
Unknown	13.8

The dual use nature of sensor technologies

Figure 07. Methods of Operation: Sensors Technology Collection Attempts



Sensors Technology Collection Attempt

A Middle Eastern company contacted several cleared defense contractors using a standard form email, requesting to purchase two sets of Long Range Position and Velocity Tracking Doppler Radars, complete with tracking antennas, data handling equipment, and essential spares. The requesting company stated it would sell the products to an unnamed third party. One of the DoD contractors received the same email more than once, even though the contracting company does not manufacture such materials.

Image 04. An air traffic controller with the 48th Operations Support Squadron, 48th Fighter Wing. (Photo Courtesy of U.S. Air Force / Tech. Sgt. Paul R. Caron Jr.)

qualifies them for export restriction based on the International Traffic in Arms Regulations (ITAR) or as classified technologies. Many collectors are attempting to capitalize on the dual-use nature of sensor technologies to bypass export restrictions.

Commercial entities are associated with over one-third of all sensor technology solicitations during the period, with government entities placing a close second at 26.8 percent.

C. AERONAUTICS TECHNOLOGY

Overview

In FY04, Aeronautics Technology was the third most targeted technology, with the total number of reported Suspicious Contact Reports (SCRs) related to U.S. defense aerospace systems increasing 35 percent over FY03 collection attempts. Table 06, below, shows collection attempts as compared to prior years, but is not inclusive of all collection attempts for this technology category in FY04.

as navigation, flight control, and sensors.

One significant trend during this period was the increased interest by foreign collectors in Miniature Aerial Vehicles (MAVs). This is likely spurred in part by the operational deployment of small tactical UAV systems by the Department of Defense in both Afghanistan and Iraq in 2003 and 2004.

MCTL Vol. III Technology Categories

Table 07, below, shows the collection activity

Table 06. Collection Attempts for Aeronautics Technology - FY97 to FY04.								
Sub-category	FY97	FY98	FY99	FY00	FY01	FY02	FY03	FY04
Aircraft, fixed wing	10	5	6	11	46	13	6	16
Gas turbine engines	8	5	7	3	7	12	12	9
Human (Crew Systems) Interface	1	5	-	1	0	1	3	0
Helicopters	3	1	1	4	9	3	4	7
Unmanned Aerial Vehicles (UAVs)	4	4	1	4	21	18	36	55

As Table 06 indicates, Unmanned Aerial Vehicles (UAVs) and their subsystems remained the most targeted Aeronautics Systems sub-category for this fiscal year. Collection attempts to obtain UAV systems and technologies ran the gamut from entire systems to subsystems such as reported by U.S. cleared defense contractors in FY04 for the Aeronautics Technology category. For an explanation of the technologies

Image 05. A Scan Eagle UAV sits on its catapult prior to launch in Al Asad, Iraq. (Photo Courtesy of the U.S. Marine Corps/Gunnery Sgt. Shannon Arledge.)

Table 07. MCTL Vol. III - Aeronautics Technology Sub-Categories in 2004.	
Sub-Category	Percent
Aeronautics Technology	35.7
Aerodynamics	7.0
Aeronautical Propulsion	9.1
Aeronautical Structures	11.9
Aeronautical Vehicle Control	4.2
Aeronautical Subsystems & Components	28.0
Aeronautical Design & Systems Integration	4.2

covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Collection Attempts by Region

The Eurasia region was the most active in targeting this technology category in 2004, associated with 28.2 percent of industry reporting. The East Asian and Pacific region was the second most active with 24.2 percent, followed by of the Near East region at 18.1 percent. South Asia, first in 2003, dropped to fourth in 2004 with 14.1 percent. The Western Hemisphere and Africa were fifth and sixth with 12.8 and 2.7 percent respectively.

Figure 08. Collection Activity by Region for Aeronautics Technology in FY04

Methods of Operation

Based on contractor reporting to DSS in FY04, Requests for Information (RFI) on sensitive and controlled aeronautics systems and technologies represented 48.0 percent of all reporting related to the technology category. Twenty percent of contractor reports were attempts by various foreign entities to acquire these systems and technologies through marketing ventures and offshore outsourcing. Another 8.7 percent of reporting in this category showed foreign entities attempting to acquired controlled technologies through the outright purchase through various schemes to mitigate ITAR restrictions.

Because many of the technologies in this category are dual use and can be used in civil avia-

Table 08. Affiliation of Collectors Targeting Aeronautic Technology in 2004

Affiliation Type	Percent
Commercial	32.3
Government	19.5
Government Affiliated	15.8
Individual	18.8
Unknown	13.5

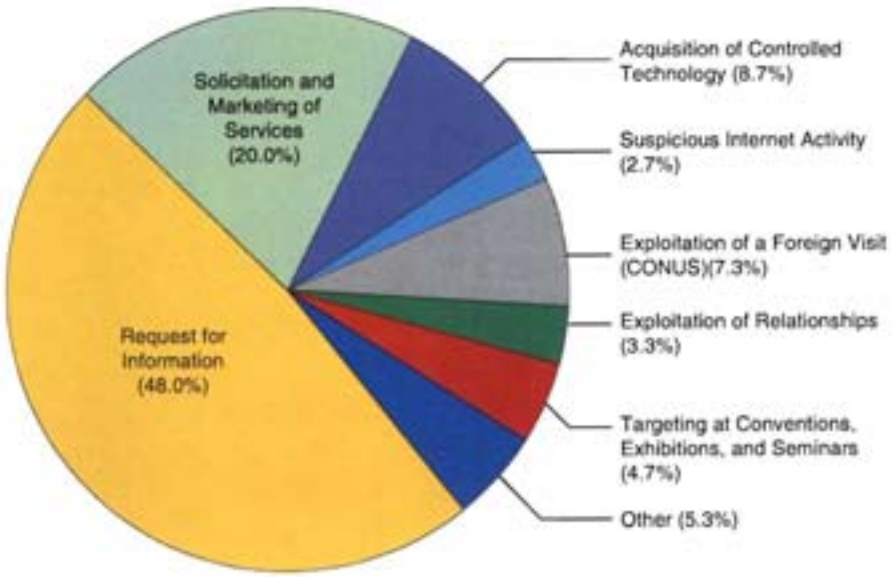
Aeronautics Technology Collection Attempt

The foreign-based subsidiary of a cleared DoD contractor received an email from an individual seeking to purchase several jet engines. The foreign-based subsidiary is a maintenance facility established to shorten the logistic chain for commercial aviation jet engine depot level maintenance. These engines are used to power a number of commercial passenger aircraft, but the requester specifically requested a military model. Research by DSS analysts into the requesting company revealed a number of close ties to a third country that is a major competitor in the design, manufacture, and sale of military aircraft, but has historically lagged behind the U.S. in jet engine design and performance.

Image 06. EDWARDS AIR FORCE BASE, Calif. - The Global Hawk unmanned aerial vehicle. (Photo Courtesy of the U.S. Air Force.)

tion as well as other technology fields, almost a third of the entities attempting to acquire this technology had commercial affiliations. Entities associated with a foreign government or individuals were the second and third largest groups to be identified attempting to acquire controlled and restricted U.S. defense technologies at 19.5 and 18.8 percent respectively.

Figure 09. Methods of Operation: Aeronautics Technology Collection Attempts



D. ELECTRONICS TECHNOLOGY

Overview

Electronics remained the fourth most targeted technology category for the second year in a row. Overall, entities from 46 countries attempted to purchase or otherwise acquire restricted or controlled technology in the Electronics Technology category during the fiscal year. Collection attempts in this category increased relative to targeting of other technologies from FY03 levels of 9 percent to 11 percent in FY04.

as reported by U.S. cleared defense contractors in FY04 for the Electronics Technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Table 09. Collection Attempts for Electronics Technology Sub-categories - FY97 to FY04								
Subcategory	FY97	FY98	FY99	FY00	FY01	FY02	FY03	FY04
Components / Microwave Tubes	4	6	12	1	17	50	73	36
Electronic Materials	2	3	1	0	5	31	0	7
Electronic Fabrication	5	2	4	7	1	1	3	2
Microelectronics	4	1	1	1	2	2	8	5
Optoelectronics	5	2	4	7	1	1	2	--
Nanoelectronics	--	--	--	--	--	--	--	28

MCTL Vol. III Technology Categories

Table 10, below, shows the collection activity

Table 10. MCTL Vol. III - Electronics Technology Sub-Categories in 2004.	
Subcategory	Percent
Electronics Technology	10.3
Electronic Components/Microwave Tubes	41.4
Electronic Materials	8.0
Electronics Fabrication	2.3
Microelectronics	5.7
Nanoelectronics	32.2

Collection Attempts by Region

Industry reporting for FY04 shows that the most significant collection attempts, 25.2 percent of all suspicious contacts in this technology category, are attributed to countries from the Eurasia region.

Countries in the Near East region were the second most active, followed by East Asia and the Pacific and South Asia regions at 22.4, 21.1, and 19.7 percent respectively. The Western Hemisphere and Africa were a distant fifth and sixth place with 8.2 and 3.4 percent respectively for FY04.

Figure 10. Collection Activity by Region for Electronics Technology in FY04

Electronics Technology Collection Attempt

A cleared DoD contractor reported several suspicious email contacts from at least two foreign entities, each seeking to purchase several two-axis MEMS-based gyroscopes. One of the entities forwarded a partial list of technical specifications for the devices requested. It is not believed that the entities were working in concert, however given the time between subsequent solicitations and the technical specifications cited, it is likely that all of the foreign entities involved were seeking to acquire the technology for the same end user. At least one of the entities inquired about establishing a marketing arrangement, in which they would represent the contractor in the region. Based on the technical specifications, it was determined that the intended end use of the devices was for a stabilized optical system under development by a foreign military R&D facility.

Image 07. An M1 Abrams tank at a remote location in Iraq. The Abrams uses a number of stabilized optical systems to achieve its battlefield supremacy. Soldiers are assigned to the 1st Infantry Division's Company B, 1st Squadron, 4th Cavalry Regiment, deployed in support of Operation Iraqi Freedom. (Photo Courtesy of the U.S. Army / Pvt. Brandi Marshall / April 30, 2004.)

Methods of Operation

Fifty percent of Electronics Technology targeting involved foreign Requests for Information (RFI), with commercial entities representing the largest group of collectors to employ the methodology, comprising 50.4 percent of all entities identified in this category.

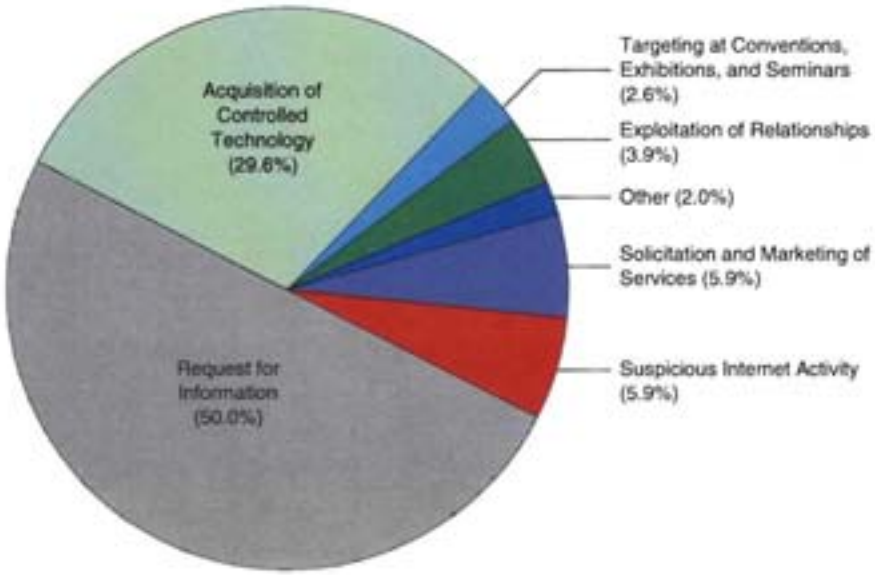
As with the majority of the technologies identified by the MCTL Vol. III, a large percentage of the technologies in this category have legitimate dual use applications. The second most common MO used by entities in this category was through the attempted acquisition of controlled technology, at 29.6 percent.

Table 11. Affiliation of Collectors Targeting Electronics Technology in 2004

Affiliation Type	Percent
Commercial	50.4
Government	13.0
Government Affiliated	15.3
Individual	9.2
Unknown	12.2

Although suspicious internet activity accounted for only 5.9 percent of incidents, events such as network vulnerability scans, incidents of hacking, and the exploitation of known security vulnerabilities to compromise U.S. contractors' unclassified systems became a serious concern during 2004. At least one defense contractor's internet website was successfully compromised by unauthorized entities. While the use of this method was infrequent relative to other methods of operation, it should be noted that a single compromised system could negatively impact several U.S. developing technologies and weapons systems, resulting in significant losses.

Figure 11. Methods of Operation: Electronics Technology Collection Attempts



E. ARMAMENTS & ENERGETIC MATERIALS TECHNOLOGY

Overview

Armaments and Energetic Material Technology was the fifth most targeted technology group in FY04 with 116 incidents reported. Targeting against this technology group tripled in 2004, jumping from 42 incidents in 2003 to 116 incidents in 2004. Foreign entities attempting to collect technology in this category were identified from 36 countries. Although a dramatic rise in the number of incidents was reported, this technology group remained the fifth most targeted technology group from 2003. Targeting of this technology group represented 9.6 percent of all reported incidents in 2004, an increase of only 0.6 percent from 2003. These relatively constant results are largely due to the overall rise in reported targeting incidents to all technology groups.

Image 08. A Standard Missile-3 (SM-3) leaves the USS Lake Erie (CG 70) enroute to intercept a short-range ballistic missile target, launched from the Pacific Missile Range Facility, Barking Sands, Kauai, Hawaii. (Photo Courtesy of the U.S. Navy / 24 Feb 2005.)

MCTL Vol. III Technology Categories

Table 12, below, shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Armaments and Energetic Materials Technology category. For an expla-

Table 12. MCTL Vol. III - Armaments & Energetic Materials Technology Sub-Categories in 2004.

Subcategory	Percent
Armaments and Energetic Materials Technology	9.5
Small- and Medium-Caliber Weapon Systems	3.4
Tactical Propulsion	0.9
Safing, Arming, Fuzing, and Firing (SAFF)	6.9
Guns, Artillery, and Other Launch Systems	6.9
Guidance and Control	6.0
Battlespace Environment	0.9
Warhead Technologies	2.6
Lethality and Vulnerability	2.6
Energetic Materials	23.3
Mines	0.9
Missile Systems	32.8
Survivability, Armor, and Warhead Defeat Systems	2.6
Nonlethal Weapons (NLWs)	0.0
Demilitarization and Decontamination	0.9

nation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Collection Attempts by Region

Geographically, 58.3 percent of all targeting in this technology category came from two regions in 2004: East Asia and Pacific at 30.7 percent and Eurasia at 27.6 percent. Near East and South Asia regions were ranked third and fourth with 20.5 percent and 15.0 percent respectively. The Western Hemisphere and Africa were fifth and sixth with 5.5 percent and 0.8 percent.

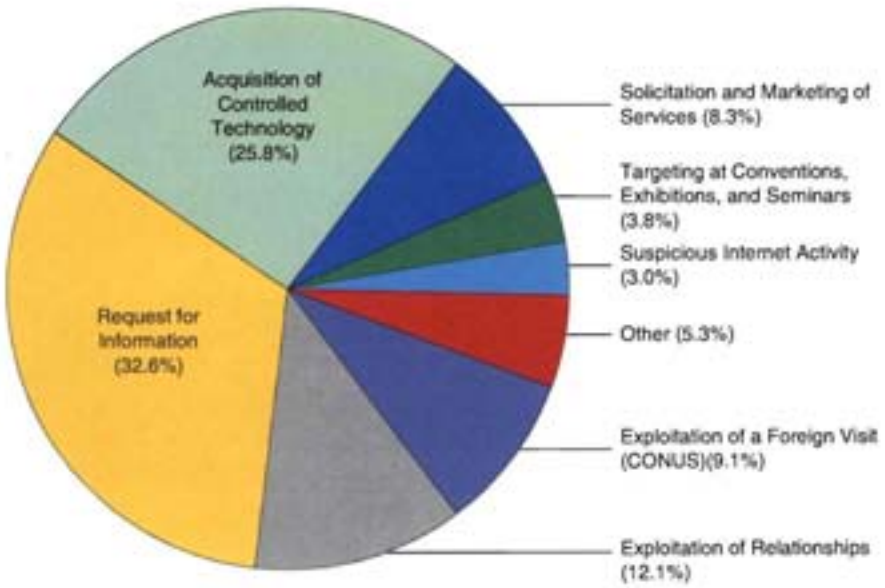
Figure 12. Collection Activity by Region for Armaments & Energetic Materials Technology in FY04

Methods of Operation

The most frequent Method of Operation utilized in targeting Armaments and Energetic Materials was the Request for Information, making up 33 percent of all industry reporting in this category. The second most utilized MO was the attempted acquisition of controlled technology, comprising 26 percent of all suspicious contact reports in this category by the cleared defense industry in FY04.

Several cases involved a foreign government or government affiliated entity targeting ITAR restricted missile systems. These entities

Figure 13. Methods of Operation: Armaments & Energetic Materials Technology Collection Attempts



sought information or associated technologies from cleared defense contractors primarily through attempts to exploit existing Foreign Military Sales (FMS) agreements. Attempts included contacts via inappropriate channels and inquiries beyond the scope of the agreement.

Other common cases involved exploitation of relationships in the context of military liaison dealing with missile defense or missile production and/or sales. In these cases, foreign entities sought to acquire restricted or classified information during visits to cleared contractors in the liaison program, attempted to visit unauthorized locations, or contacted a contractor claiming that approval for restricted information had been already granted by the U.S. government.

Unlike the other technology categories, Armaments and Energetic Materials is largely a single use technology, with a few exceptions for various civilian applications. As a result, it can clearly be determined that the largest percentage of all industry reporting in this technology category relates to government sponsored targeting, making up 40.9 percent in 2004. Entities with a commercial affiliation were the second largest group of collectors in 2004, comprising 20.9 percent of reporting in this category.

Table 13. Affiliation of Collectors Targeting Armaments & Energetic Materials Technology in 2004

Affiliation Type	Percent
Commercial	20.9
Government	40.9
Government Affiliated	13.6
Individual	10.0
Unknown	14.5

Armaments & Energetic Materials Technology Collection Attempts

In June 2004, an employee of a cleared defense contractor received a telephone call from a male who stated that he was responsible for a training issue for a foreign military service and working closely with the U.S. Army Training and Doctrine Command (TRADOC) in obtaining new training information. The caller told the cleared defense contractor employee that the TRADOC liaison suggested he call the contractor to gather information on "the Loitering Attack Missile, the Precision Attack Missile, and the Kinetic Energy Missile." The caller requested information on operational delivery dates and costs for these systems. When the cleared defense contractor employee refused to discuss any of these programs, the caller attempted to reassure them that it was okay, as it had been approved by TRADOC. The employee still refused to reveal any information to the caller, and the caller thanked the employee for his time, and terminated the call.

Image 09. A Tomahawk Land Attack Missile (TLAM) is launched from the guided missile cruiser USS Cape St. George. (Photo Courtesy of the U.S. Navy / Intelligence Specialist 1st Class Kenneth Moll / March 23, 2003)

F. LASERS & OPTICS TECHNOLOGY

Overview

Fiscal Year 2004 marked the first year in which DSS tracked Lasers & Optics Technology as a separate technology category from the Sensors category. Elements of the subcategories were drawn from both the Sensors and Electronics categories. As a result, both the Sensors and Electronics statistical data for this period are atypical when compared to trends developed over the last few years. In FY03, Sensors and Lasers combined to account for 17 percent of all targeting attempts. This year, Lasers & Optics were the sixth most frequently targeted technology accounting for 7.5 percent of all U.S. defense industry reporting and targeting from entities in 45 countries.

Examples of technologies sought by foreign entities in FY04 are laser range finders, laser target designators, and LIDAR (Light Detection and Ranging). These examples were the most heavily targeted technologies within the Lasers & Optics category.

Image 10. Night Vision Optics - A M2A2 Bradley Fighting Vehicle trains its 25mm chain gun on enemy targets in Samarra, Iraq. (Photo Courtesy of Department of Defense)

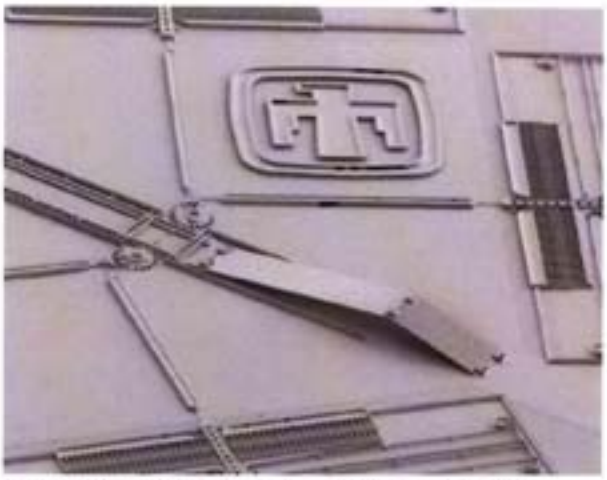


Image 11. Hinged Polysilicon Mirror and Drive Motors. (Photo Courtesy of Sandia National Laboratories, SUMMiT™ Technologies.)

MCTL Vol. III Technology Categories

Table 14, below, shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Lasers & Optics Technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Table 14. MCTL Vol. III - Lasers & Optics Technology Sub-Categories in 2004.

Subcategory	Percent
Lasers & Optics Technology	34.3
Lasers	21.2
Optics	21.2
Optical Materials & Processes	3.0
Supporting Technology & Applications	7.1
Optoelectronics & Photonics	13.1

Collection Attempts by Region

Interest in lasers and optics was evenly spread between regions of the Near East, Eurasia, and East Asia with each accounting for 25.8, 24.2, and 22.7 percent respectively. South Asia was fourth at 18.2 percent and the Western Hemisphere and Africa were a distant fifth and

Figure 14. Collection Activity by Region for Lasers & Optics Technology in FY-04

sixth with 8.3 and 0.8 percent respectively.

Table 15. Affiliation of Collectors Targeting Lasers & Optics Technology in 2004

Affiliation Type	Percent
Commercial	40.7
Government	17.6
Government Affiliated	18.7
Individual	9.9
Unknown	13.2

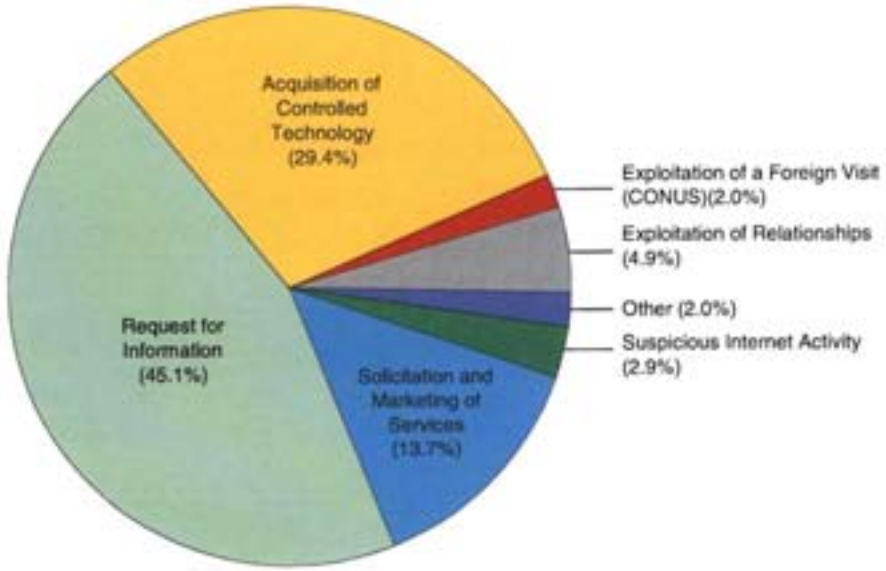
Methods of Operation

The most frequently observed MO for targeting technologies in the Lasers & Optics category involved foreign Requests for Information and accounted for approximately 45 percent of all reporting in this category. Attempts to acquire controlled technologies comprised 29.4 percent of industry reporting for this category in FY04.

The third most commonly used MO, at 13.7 percent, was the solicitation of marketing services, such as market representation in the country, or offshore back office services and engineering support.

Because of the rise in consumer demand for digital cameras, digital video disc (DVD) systems, and a host of other consumer and industrial applications, the largest single group of collectors in this category was associated with commercial organizations, accounting for 40.7 percent of targeting incidents.

Figure 15. Method of Operation: Lasers & Optics Technology Collection Attempts



Government and government affiliated entities, such as government sponsored academic institutions and research facilities, were the second and third largest groups identified by DSS with 18.7 and 17.6 percent respectively.

Example of Lasers & Optics Technology Collection Attempt

A cleared contractor received an email from a doctoral student requesting information on an "ultraviolet missile warning system." The student claimed that the request was the subject of a research project assigned by his professor. This incident is suspicious as the email originated from a commercial internet service provider vice an .edu top level domain, and the university that the individual claimed to be attending is known to be closely associated with military research programs for the national defense forces.

Image 12. Two F-15Es from the 90th Fighter Squadron, Elmendorf Air Force Base, Alaska, fire a pair of AIM-7Ms during a training mission. The mission took place over the Gulf of Mexico just off the coast of Florida. (Photo Courtesy of the U.S. Air Force.)

Requests such as these from university students to industry are common and rely on academic researchers to freely exchange information. However, the specific nature of the request is not consistent with a doctoral student research project, as it is focused on a specific system rather than a specific technology or field of scientific research.

G. SIGNATURE CONTROL TECHNOLOGY

Overview

In FY04, the Signature Control Technology category returned to the DSS Top 10 List, due to increased attempts by foreign collectors to obtain these technologies. Most notably, the level of targeting by foreign nationals made signature control technologies the seventh most targeted system for 2004, at 4.7 percent, and represents a more than threefold increase over 2003 levels.

MCTL Vol. III Technology Categories

Table 16 shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Signature Control Technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Table 16. MCTL Vol. III - Signature Control Technology Subcategories in 2004.

Subcategory	Percent
Signature Control Technology	94.7
Tailored Property Materials	0.0
Multifunction Systems and Subsystems	5.3
Systems Engineering and Integration	0.0

Signature Control Technology Collection Attempt

In a specific case, a Near East-based company contacted a cleared defense contractor involved in stealth technology research. The entity sought to purchase radar-absorbing material for an unidentified customer. DSS analysts determined the request was an attempt to acquire controlled technologies for a weapons program in an embargoed country in the region.

Image 13. A B-2 Spirit soars through the sky after a refueling mission. (Photo Courtesy of the U.S. Air Force / Tech. Sgt. Cecilio Ricardo.)

Collection Attempts by Region

Entities from a total of 35 countries attempted to gain access to ITAR controlled or classified technologies under the Signal Control category in FY04. Targeting of this technology category by East Asia and Pacific countries equaled that by countries of Eurasia, both regions accounting for 28.8 percent. The Near East and South Asia regions were third and fourth with 18.8 percent and 12.5 percent respectively. The Western Hemisphere and Africa placed fifth and

Figure 16. Collection Activity by Region for Signature Control Technology in FY04

sixth at 10.0 percent and 1.3 percent for FY04.

Methods of Operation

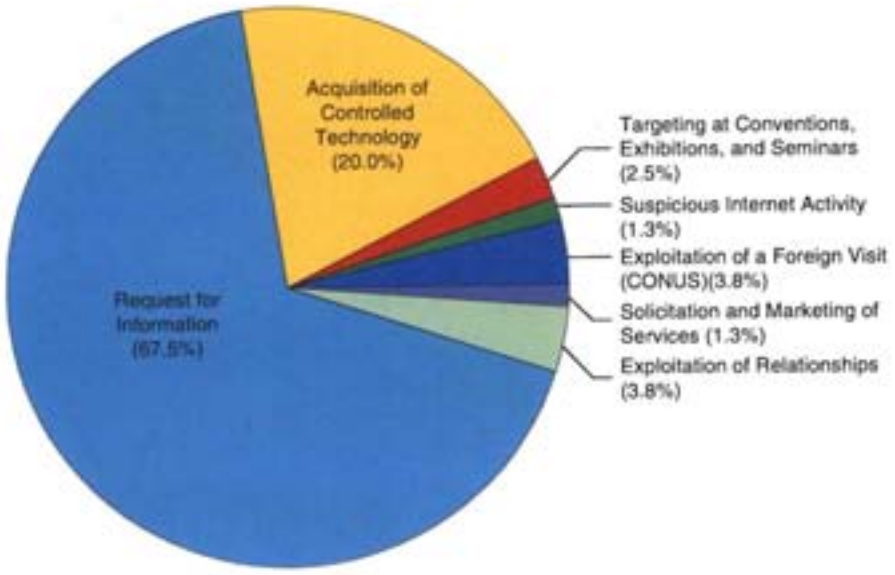
The most frequent method of operation utilized by entities attempting to collect against Signature Control Technology in 2004 was via Requests for Information with 67.5 percent of reporting in this category.

Another 20.0 percent of reporting had entities seeking to acquire the technology outright, making this method of operation the second most frequently used tactic.

Consistent with other targeted technologies, signature control systems were targeted primarily by commercial entities, identified in 44.7 percent of the cases in this category. The second and third largest groups identified were those with a government and government affiliated associations, at 21.1 and 18.4 percent respectively.

Table 17. Affiliation of Collectors Targeting Signature Control Technology in 2004	
Affiliation Type	Percent
Commercial	44.7
Government	21.1
Government Affiliated	18.4
Individual	5.3
Unknown	10.5

Figure 17. Methods of Operation: Signature Control Technology Collection Attempts



H. MATERIALS & PROCESSING TECHNOLOGY

Overview

Materials & Processing Technology was the eighth most targeted ITAR-controlled technology by foreign collectors during FY04. Incidents involving Materials and Processing Technology accounted for 3.3 percent of all reported incidents submitted by cleared defense contractors to DSS during FY04.

Targeting was primarily centered around structural and special function materials, which accounted for a combined total of 48.7 percent of targeting in this category. Collectors showed interest in composites, adhesives, magnets, and special properties of such metals as new special purpose aluminum and titanium alloys.

MCTL Vol. III Technology Categories

The table below shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Materials & Processing Technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Image 14. A NASA spacesuit consists of 14 layers of nylon tricot, spandex, urethane-coated nylon, dacron, neoprene, aluminized mylar, gortex, kevlar, and nomex. (Photo Courtesy of NASA / 1995.)

Table 18. MCTL Vol. III - Materials & Processing Technology Subcategories in 2004.	
Subcategories	**Percent**
Materials & Processing Technology	38.5
Armor and Anti-armor Materials	2.6
Electrical Materials	2.6
Structural Materials	25.6
Special Function Materials	23.1
Smart Materials and Structures	7.7
Micromachined Materials & Structures	0.0
Magnetic Materials	0.0

Collection Attempts by Region

Entities from 21 countries attempted to gain access to ITAR controlled or classified technologies under the Materials & Processing category in FY04. Regionally, South Asia was the most active accounting for 26.3 percent of all incidents in this category. The East Asia and the Pacific region and the Eurasia region are tied for second at 21.1 percent each. The Near East, the Western Hemisphere, and Africa placed fourth, fifth and sixth respectively with 18.4 percent, 7.9 percent and 5.3 percent in

Figure 18. Collection Activity by Region for Materials & Processing Technologies in FY-04

FY04's ranking of regional activity.

Methods of Operation

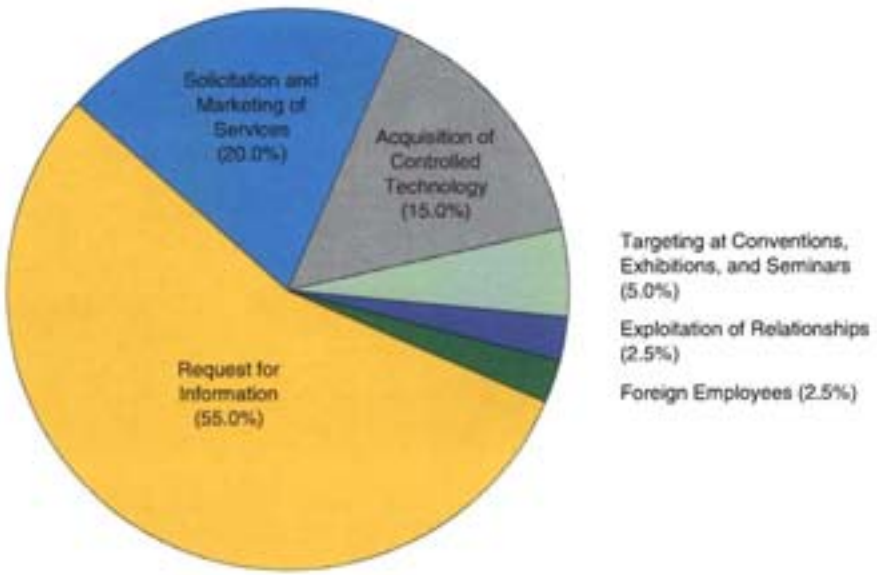
Overall, foreign collectors targeting Materials & Processing Technology used the RFI method of operation most frequently, often via the internet, accounting for at least 55.0 percent of all incidents reported to DSS during FY04. The solicitation and marketing of services was the second-most frequently used method to transfer Materials & Processing Technology, accounting for 20.0 percent of 2004 reporting in this category. Internet offers to purchase this technology outright were the third-most preferred method utilized by foreign collectors, accounting for 15.0 percent of industry reporting in this technology category.

From the standpoint of case histories, these particular statistics verify the trend that the main research and development efforts in advanced, dual-use technology originate with the commercial sector long before any government decides that such cutting-edge technology would be useful for its military forces, thus providing an exception to the established belief that these developments often evolve in the "tactical to the practical" mode.

Table 19. Affiliation of Collectors Targeting Materials & Processing Technology in 2004	
Affiliation Type	**Percent**
Commercial	47.4
Government	13.2
Government Affiliated	7.9
Individual	18.4
Unknown	13.2

In reference to the reported instances involving foreign collectors that targeted Materials & Processing Technology during FY04, DSS identified the majority of these foreign collectors as

Figure 19. Methods of Operation: Materials & Processing Technology Collection Attempts



having either commercial or individual origins, accounting for 47.4 percent and 18.4 percent respectively. Government and government affiliated entities accounted for 21.1 percent of the reported collection attempts.

Materials & Processing Technology Collection Attempt

On May 26, 2004, the sales email address of a cleared defense contractor received an email requesting the contractor to fabricate an electrostatic deflector from titanium. The email specifically cited machining and finishing requirements for the parts to be machined and included a partial set of drawings for the contractor to develop a price quote. It was determined that the request came from an entity associated with a foreign government-run debarred atomic research facility.

Image 15. Advanced Photon Source (APS) storage ring sector. (Photo Courtesy of Argonne National Laboratory.)

I. CHEMICAL TECHNOLOGY

Overview

As with Sensors and Laser technologies, FY04 marks the first year that DSS has separated into two categories the Chemical and Biological Systems technologies, in accordance with MCTL Vol. III. Although this breakdown resulted in a decrease in the overall number of cases attributed to each category, Chemical Technology remained a significant target of foreign collectors, with industry reporting to DSS showing individuals from 25 countries as having a suspicious interest in this category.

Those countries identified as the largest collectors of U.S. classified and controlled technologies were also the largest collectors in this technology category.

MCTL Vol III Technology Categories

Table 20, below, shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Chemical Technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

Table 20. MCTL Vol. III - Chemical Technology Subcategories in 2004.

Subcategory	Percent
Chemical Technology	61.1
Defense Systems	5.6
Dissemination & Dispersion	2.8
Material Production	2.8
Detection, Warning, & Identification	27.8
Obscurants	0.0

Collection Attempts by Region

In FY04, 25 countries were identified through

Image 16. Members of the Missouri National Guard's new CERFP (Chemical, Biological, Radiological, Nuclear, Explosive Emergency Response Force Package) spray a "victim" of a toxic chemical attack during an Army evaluation of the team's ability to deal with a weapon of mass destruction near Jefferson City on July 24, 2004. (Photo Courtesy of the Department of Defense / Master Sgt. Bob Haskell / 2004.)

requests for technologies associated with the Chemical Technology category. Regionally,

Figure 20. Collection Activity by Region for Chemical Technology in FY04

countries of the East Asia and Pacific region were the most active, accounting for 28.6 percent of all industry reporting in this technology category. Eurasia as a region were second with 23.8 percent, followed by South Asia, the Near East, the Western Hemisphere, and Africa, at 21.4, 16.7, 7.1 and 2.4 percent respectively.

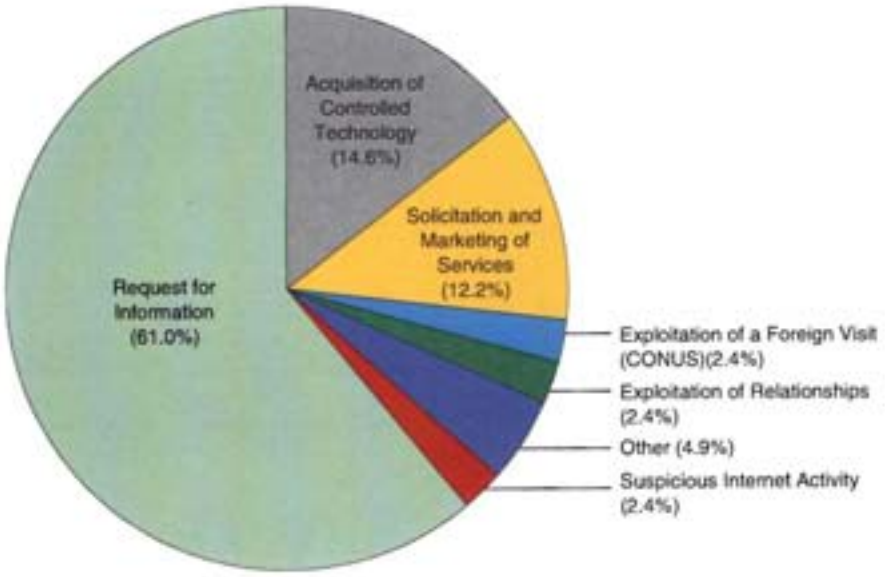
Methods of Operation

The most frequently used method of operation by entities collecting in this technology category were Requests for Information at 61.0 percent. The second and third most frequently used MOs were attempts to acquire controlled technology and the solicitation of marketing and offshore services at 14.6 and 12.2 percent respectively.

Nearly 42 percent of all collectors in this category were affiliated with commercial entities. The second largest group were those with ties to foreign governments, at 19.4 percent.

Table 21. Affiliation of Collectors Targeting Chemical Technology in 2004	
Affiliation Type	Percent
Commercial	41.7
Government	19.4
Government Affiliated	13.9
Individual	11.1
Unknown	13.9

Figure 21. Methods of Operation: Chemical Technology Collection Attempts



Chemical Technology Collection Attempt

During the spring of 2004, a US company received a telephone call from a "businessman" claiming to have interest in purchasing approximately 100,000 standard pounds, of Ammonium Perchlorate (NH4CLO4), an explosive material. The company informed the man it was unable to sell such materials to an unknown vendor. Investigation later disclosed the requester's address was located in a residential area and did not have storage or safeguarding capabilities.

J. SPACE SYSTEMS TECHNOLOGY

Overview

In FY04, Space Systems Technology ranked tenth in targeting by foreign collectors, down from seventh place in FY03. Foreign entities requested information, attempted to purchase, or attempted to acquire technologies related to satellite communications, the Global Positioning System (GPS), satellite design methodologies and simulation software, and space qualified electronics and materials.

While direct space access remains limited to a small number of countries, countries worldwide are increasingly dependent on services provided by space systems – international telecommunications and internet access, weather forecasting, banking and commerce, and precise navigation and timing are just a few examples.

Image 17. A Delta II, carrying a Global Positioning System satellite, launches from Cape Canaveral, Florida. In the first six days of Operation Iraqi Freedom, more than 80 percent of the munitions that hit several thousand targets were precision-guided. (Photo Courtesy of NASA / Carlton Bailie)

Examples of space systems technologies sought by foreign collectors during FY04 include optical systems for space observatories, composites and coatings used for spacecraft survivability, satellite communications systems, and Global Positioning System technologies.

MCTL Vol. III Technology Categories

The table below shows the collection activity as reported by U.S. cleared defense contractors in FY04 for the Space Systems Technology category. For an explanation of the technologies covered by each subcategory, please refer to the Militarily Critical Technologies List, Volume III.

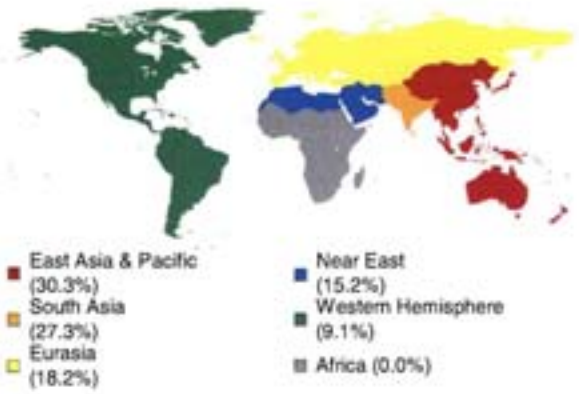
Table 22. MCTL Vol. III - Space Systems Technology Subcategories in 2004

Subcategory	Percent
Space Systems	42.4
Space Avionics and Autonomy	9.1
Electronics and Computers	12.1
Launch Vehicles for Space Systems	9.1
Space Optics	6.1
Power and Thermal Management	6.1
Propulsion for Space Systems	3.0
Sensors for Space Systems	3.0
Survivability in Space	3.0
Structures for Space	6.1
Integrated Systems	0.0
Space-Based Lasers (SBLs)	0.0

Collection Attempts by Region

The overall number of countries associated with Space Systems Technology collection in FY04, as identified by industry reporting to DSS, declined slightly from 19 in FY03 to 15. Of these, the East Asia and Pacific region countries, at 30.3 percent, were the most active in

Figure 22. Collection Activity by Region for Space Systems Technology in FY04



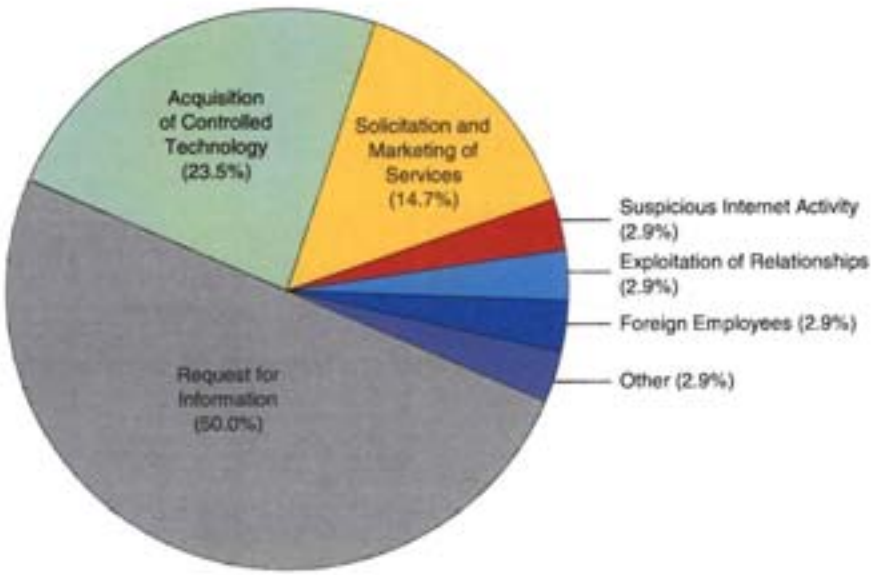
targeting classified and International Traffic in Arms Regulation (ITAR) restricted U.S. space systems and technologies. The South Asia region, first in FY03, dropped to second in FY04, with Eurasia countries placing third. The Near East placed fourth in FY04 at 15.5 percent. The Western Hemisphere and Africa placed fifth and sixth with 9.1 and 0.0 percent respectively.

Table 23. Affiliation of Collectors Targeting Space Systems Technology in 2004	
Affiliation Type	Percent
Commercial	38.7
Government	9.7
Government Affiliated	12.9
Individual	29.0
Unknown	9.7

Method of Operation

Based on contractor reporting, Requests for Information (RFI) on sensitive and controlled Space Systems and technologies represented 50.0 percent of all reporting related to the technology category. The second most commonly used method of operation, at 23.5 percent, was attempts to acquire these systems and technologies by purchasing them. The third most common MO , at 14.7 percent, was solicitations for marketing and off-shore services by various entities.

Figure 23. Methods of Operation: Space Systems Technology Collection Attempts



The largest group of entities identified from reporting were those with commercial ties, followed by individuals with no known other affiliations as 38.7 and 29.0 percent respectively.

Space Systems Technology Collection Attempt

A South Asian company contacted an East coast-based Cleared Technology Center via email, stating that their unnamed client had an outstanding requirement for two "high temperature diode stack arrays." The email also forwarded a short list of technical specifications. A review of the technical requirements by DSS analysts revealed that the company was in fact seeking to obtain two high temperature laser diode stacks based on the technical specifications forwarded by the South Asian company.

The approach by the company to the Cleared Technology Center was typical of a majority of contacts by foreign companies seeking to obtain ITAR controlled or classified technologies from U.S. defense contractors. The sender of the email also detailed business items, such as how to prepare the quote and a reminder to include a fixed percentage commission in the quotation as the commission to the intermediary.

Image 18. STS112-375-033 (16 October 2002) --- The International Space Station (ISS), photographed by a crewmember on board the Space Shuttle Atlantis. (Photo Courtesy of NASA)

V. Future Trends Assessment

The analytical work presented in this study brings into focus new as well as continuing trends from the past year.

Trends over the past five years indicate a progressively increasing number of suspicious contact reports by cleared defense contractors. DSS anticipates that this trend will continue in the future with a probable leveling in regard to the number of countries targeting each year. Collectors will continue to make good use of improved methods of communication and the vast amount of information that is available from open sources including advertising and information provided by defense contractors through their web-sites. As the defense business becomes increasingly global, contractors in the National Industrial Security Program (NISP) will encounter a greater threat from foreign adversaries and economic competitors who will use the pretense of legitimate business as a vector to steal and illegally transfer technology.

DSS anticipates increased targeting from commercial entities rather than government sponsored targeting. The benefit of economic gain from the transfer of developing technologies is likely to motivate foreign businesses who seek to improve their own fiscal health through the acquisition and application of advanced technologies without the investment for research and development. This slow erosion of our technological supremacy to foreign competitors may result in a degradation of the competitiveness of U.S. technology firms in the global market. Additionally, governments who have close ties to these companies will benefit from the advanced technologies.

DSS noted in its 2004 report that acquisition would likely increase in the coming years with precise targeting by foreign entities following well-placed request for information inquiries. Indeed, technology collection via attempted acquisition increased this year by 33 percent. Foreign entities are able to save significant time and money by acquiring technologies which cuts out costs associated with research and development. To this end, DSS anticipates a further increase in the use of acquisition as a method to collect and transfer technology. In addition, DSS anticipates that collectors will continue to use a combination of methodologies with a request for information often evolving into an acquisition attempt. Suspicious internet activity remained steady but accounted for some of the most successful technology collection events this year.

DSS also anticipates an increase in suspicious internet activity against cleared defense contractors in the defense industrial base. Due to the potential for the collection of massive amounts of information from just one successful computer intrusion event, the impact of collection via this method can be exponentially more damaging than that of other methods. Additionally, as more nations mature their computer network operations and exploitation capabilities, the risk to sensitive information on U.S. computer systems will increase.

With regard to actual targets, Information Technology and Sensors are firmly established as the two most frequently targeted categories. DSS believes that targeting of sub systems and components will continue to increase as more nations become capable of reverse engineering U.S. technology and incorporating U.S. advanced technology into their own indigenous efforts. Of note, targeting against Signature Control Technology experienced a sizable gain in 2004. Targeting of this technology may continue in 2005 as it appears that more universities and technical centers are establishing research programs involving this technology.

Overall, cleared defense contractors can expect

increased interest in all manner of advanced and developing technologies. The added dimension of increased commercial endeavors with foreign entities will have an impact on the security and counterintelligence community's ability to differentiate between technology collection and legitimate business. Collectors will likely use this venue to target and then exploit U.S. companies developing sensitive technologies.

Many countries already espouse a policy of collecting any and all U.S. military and dual use technology, no matter how insignificant, in an attempt to assemble a great body of technological work for their own exploitation.

Considering the aggressive collection posture of some nations, the U.S. defense industrial base will encounter an increasing tenacious and multidimensional threat environment.

VI. Appendix: MO Definitions, Indicators and Countermeasure

Request for Information (RFI). A request for information is any request, not solicited by the cleared company, received from a known or unknown source that concerns classified, sensitive, or export-controlled information. While the recipient may not have directly solicited the request, the inquiry may have been indirectly solicited through technical journal and website advertisements. An example of an unwanted, but indirectly solicited request is an incident where a cleared defense contractor's product was reviewed in a trade journal and the company subsequently received a number of suspicious, but "solicited," reader service card inquiries from an embargoed country.

Requests for Information (RFI)	
Indicators	**Countermeasure**
• Technology is ITAR-controlled • The CDC does not normally conduct business with the foreign requester • The request originated from an embargoed country • The request is unsolicited or unwarranted • The requester claims to represent an official government agency but avoids proper channels to make the request • The initial request is directed at an employee who does not know the sender and is not in the sales or marketing office • The requester is fishing for information • The requester represents an unidentified third party • The requester is located in a country with a targeting history directed at the U.S. cleared defense industry	• Incorporate security into web design and adver tising • Initiate an active monitoring solution website • Report requests to FSO, the Industrial Security Representative, and to DSSCI (similar requests may have been received by multiple U.S. cleared facilities for the same technology) • Ask who the requester represents and why they are seeking the requested information • Clearly post notification on company websites for those products and technologies that are export controlled

Acquisition of Technology. This MO involves foreign entities attempting to gain access to sensitive technologies by purchasing U.S. technology and in some rare cases, the companies that develop those technologies. The vast majority of acquisition is directed at acquiring specific components or technologies through an outright purchase.

Acquisition of Technology	
Indicators	**Countermeasure**
• Foreign individuals or competitors seek a position in the U.S. company that affords access to restricted technology • Statements that license is not necessary • Foreign company asks U.S. company to send information or product to another U.S.-based company for foreign transfer or via email to non-U.S. addresses • The requester appears to be "skirting controls". • Several similar requests are made over time	• Complete due diligence for the buyer and the end user. Ask questions on the end use of the technology • Request a threat assessment from the Industrial Security Representative, DSSCI or the program office whose work the contractor performs • Scrutinize employees hired at the behest of a foreign entity or business partner

Solicitation of Marketing Services. In this MO, foreign individuals with technical backgrounds offer their services to research facilities, academic institutions, and even cleared contractors. A number of incidents involved foreign nationals seeking postdoctoral fellowships at cleared universities or attempting to gain employment at companies that are involved in cutting-edge technologies.

Solicitation and Marketing of Services	
Indicators	**Countermeasure**
• Offer to provide offshore software support on defense-related projects • Invitation to cultural exchanges, individual-to-individual exchange, or ambassador program • Offer to act as a sales or purchasing agent in foreign country • Foreign government and business sponsored internship	• Have a technology control plan • Request a threat assessment from the Industrial Security Representative, DSSCI or the program office whose work the contractor performs • Scrutinize employees hired at the behest of a foreign entity or business partner

Exploitation of Foreign Visit. The term "foreign visitor" includes one-time visitors, long-term visitors (such as exchange employees, official government representatives and students) and frequent visitors (such as foreign sale representatives). Suspicious conduct includes actions prior to, during and after a visit. The primary factor that makes foreign visits suspicious is the extent to which the foreign visitor requests access to facilities or discusses information outside the scope of the approved activities.

Exploitation of Foreign Visit	
Indicators	**Countermeasure**
• Foreign Liaison Officer or embassy official attempts to conceal official identities during a supposedly commercial visit • Hidden agendas opposed to the stated purpose of the visit • Last minute and unannounced persons added to the visiting party • "Wandering" visitors, especially those who act offended when confronted • Using alternative methods. For example, if a classified visit request is disapproved, the foreign entity may attempt a commercial visit and/or may use a U.S.-based third-party to arrange the visit • Visitors ask questions that are outside the scope of the approved visit hoping to get a courteous or spontaneous reply • Visitor claims business interest but lacks experience researching and developing the technology (*Remember, the discussion of export-controlled technology also requires an export license*)	• Brief country threat to all employees involved with the foreign visit. Request country threat assessments from company security, FSO, Industrial Security Representative, or DSSCI • Ensure appropriate personnel, both escorts and those meeting with visitors, are briefed on the scope of the visit • The number of escorts per visitor group should be adequate to properly control movement and conduct of visitors • Conduct frequent checks of foreign visits to determine if the foreign interests are attempting to circumvent security agreements

Targeting at Conventions. Conventions, seminars, and exhibits are collection-rich targeting opportunities for foreign collectors. These functions directly link U.S. programs and technology with knowledgeable personnel. This type of event provides opportunities for foreign nations to employ a greater variety of MOs to target visitors. Also, exhibits offer a unique opportunity for foreign entities to study, compare, and photograph actual products in one location. Of even more importance, foreign events held on the collector's home territory are vulnerable to exploitation by traditional FIS technical means (for example, electronic surveillance) and the employment of entrapment ploys (such as inducement of the target into a compromising situation). The audiences at international seminars are comprised principally of leading national scientists and technical experts who can pose more of a threat than intelligence officers. Technical experts focus their questions and requests on specific technical areas that have direct application to their work. Reports show that during seminars, foreign entities may use subtle approaches such as sitting next to a potential target and initiating a casual conversation. This can establish a point of contact that may lead to exploitation at a later date. Use of membership lists of international business and/or technical societies as a source to identify potential targets and as a means of introduction is also increasing.

Targeting at Exhibit, Conventions, and Seminars	
Indicators	**Countermeasure**
• Topics at seminars and conventions deal with classified or controlled technologies and/or application • Country or organization sponsoring seminar or conference has tried unsuccessfully to visit facility in the past • Receive invitation to brief or lecture in a foreign country with all expenses paid • Requests for presentation summary 6-12 months in advance • Photography and filming appear suspicious • Attendees wear false name tags • Casual conversation and discussions during and after events that appears aimed at future contract/relations	• Have a Technology Control Plan for any items and proprietary information brought overseas • Monitor follow-up requests after a show for collection attempts and report them to the FSO and DSS. • Consider what information is being exposed, where, when, and to whom • Provide employees with detailed travel briefings concerning the threat, precautions to take, and how to react to elicitation • Take mock-up displays instead of real equipment • Request a threat assessment from program office • Restrict information provided to what is necessary for travel/hotel accommodations • Carefully consider whether equipment or software can be adequately protected

Exploitation of Joint Venture/Research Relationships. This MO offers significant collection opportunities for foreign interests. As with frequent visits and other international programs, joint business efforts place foreign personnel close to U.S. personnel and technology and can facilitate access to protected programs. Of growing concern is the use of foreign research facilities and software development companies located outside of the U.S. to work on commercial projects that are related to protected programs. Anytime a company relinquishes direct control of its processes or products to another company, it is exposing that technology to possible exploitation. Also of concern is the placement of foreign workers in close proximity to protected operations. While high technology programs receive the greatest

amount of public attention, low technology programs, such as fabrics for military battle dress uniforms, are equally at risk.

Exploitation: Relationships	
Indicators	**Countermeasure**
• Resident foreign representatives fax documents to an embassy or another country in a language other than English; repeatedly request access to the local area network (LAN); want unrestricted access to the facility; single out company per sonnel to develop as possible sources of infor mation • Enticing U.S. contractor to provide large amounts of technical data as part of the bidding process, only to have the contract cancelled • Potential technology-sharing agreements during the joint venture are one-sided • Foreign organization sends more foreign repre sentatives than are necessary for the project • New employees hired from the foreign parent company or its foreign partners asks to access classified or export-controlled data	• Have a Technology Control Plan or very detailed Standard Practice Procedure • Review all documents being faxed or mailed and have someone reliable translate foreign language correspondence • Provide foreign representatives with stand-alone computers • Share minimum amount of information appropriate to the scope of the joint venture/research • Extensively educate employees on the scope of the project and how to deal with and report elicitation • Refuse to accept unnecessary foreign representatives into the facility

Targeting of U.S. Personnel Abroad. This MO involves the targeting of U.S. defense contractor employees traveling overseas. Targeting occurs at airports and includes luggage searches, unauthorized use of laptop computers, extensive questioning beyond the normal security measures, etc. Other travelers have received excessively "helpful" service by host government representatives and hotel staffs. Reporting also indicates that traditional foreign intelligence service (FIS) collection methods are still used by foreign nations. Some methods include surreptitious listening devices, hotel room searches, intrusive inspection of electronic equipment, and positioning of personnel to eavesdrop on conversations.

Targeting of U.S. Personnel Abroad	
Indicators	**Countermeasure**
• Specific and direct questions by unknown and/or suspicious persons regarding personal and professional information • Activities that indicate possible surveillance • Appearance that hotel room and personal items have been searched or accessed • Confiscation of computers or media at official control points • Repeatedly identified for official questioning • Assignment to the same area (room or floor) of hotel on multiple visits	• Complete a pre-travel security briefing and don't publicize travel plans • Maintain control of sensitive information/documents and media/equipment • Keep hotel room doors closed and locked. Note how the room looks when you go out • Limit sensitive discussions • Don't use computer or fax equipment at foreign hotels or business centers for sensitive matters • Ignore or deflect intrusive or suspect inquires or conversations about professional or personal matters • Keep unwanted (no longer needed) sensitive material until it can be disposed of securely

Suspicious Internet Activity. Targeting associated with this MO includes exploitation of the internet (hacking). The majority of the endeavors have been correlated with probing efforts. The computer probes are most likely searching for potential weaknesses in systems for exploitation. In one example, an internet probing effort of a contractor's unclassified network lasted over 24 hours. The original source of the attack was likely masked, but the probes were traced to IP addresses allocated to a "girl's school" in an East Asian country. This probing effort was very likely obfuscated by the entity conducting the probes in order to deter network security administrators from determining the true identity of the entity. The potential exists for users to go to several websites and receive anonymous e-mail addresses. In detecting these probes, the cleared companies have already demonstrated they have the security countermeasures in place to thwart attempts to penetrate their computer systems. Although the probing of a system in not illegal, a crime is committed once a port is breached by an unauthorized entity.

Internet Activity	
Indicators	**Countermeasure**
• Computer probes and emails with attachments known to carry viruses and other computer exploits • Network attacks originated from foreign Internet Protocol (IP) address or Internet Service Provider (ISP) • Attacks last over a period of a day or more • Several hundred, if not thousands of attempts are made using multiple passwords and/or scripts	• Have a firewall monitoring software that logs all intrusion attempts and any malicious activity • Have appropriate level of protection in place to repel such an attack • When a probe is noted, heighten network security alert status