



2003 TECHNOLOGY COLLECTION TRENDS IN THE US DEFENSE INDUSTRY

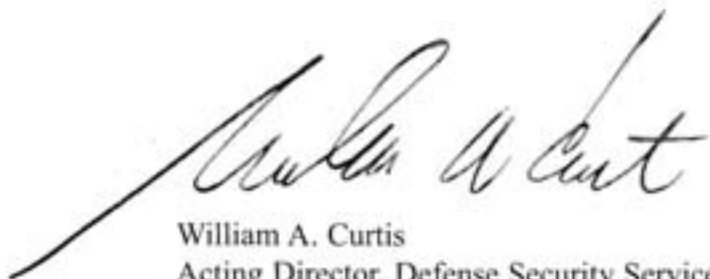


Foreword

The Defense Security Service (DSS) is charged with the mission of assisting the cleared defense industry in the recognition and reporting of foreign contacts and collection attempts, as outlined in the National Industrial Security Program Operating Manual (NISPOM). This annual trends report is made possible by the cumulative effort of cleared defense contractors reporting suspicious activity to their facility security officers and ultimately to DSS.

This publication is designed for use by security officials, cleared contractors, intelligence professionals and DoD policy and decision-makers. It covers some of the most important topics associated with foreign targeting and collection attempts directed at the defense industry, including which technologies are being targeted, how this targeting is accomplished, and where it originates.

The ultimate goal of this publication is to provide individuals and organizations with future trends to improve threat awareness and technology protection related to foreign collection attempts directed at the U.S. defense industry. I strongly encourage the continued reporting of suspicious contact reports to DSS field offices. Prompt reporting of foreign collection attempts is critical to an effective industrial security program.

A handwritten signature in cursive script, appearing to read "William A. Curtis". The signature is written in dark ink and is positioned above the printed name and title.

William A. Curtis
Acting Director, Defense Security Service

Contents

I. Executive Summary	1
A. Reporting Trends	1
B. World Trends	1
C. Technology Interests Trends	1
D. Most Frequently Reported Technology Targets	1
E. Most Frequently Reported Foreign Collection Methods of Operation (MO) ...	1
II. Introduction	3
III. World Collection Trends	4
A. Country Trends: Totals	4
B. Country Trends: Industrial Base Strength	4
C. Worldwide Breakdown by Region	5
D. Foreign Collectors	6
IV. Technology Analysis for Top 10 Categories	8
A. Information Systems	8
B. Sensor & Lasers	11
C. Electronics	14
D. Armaments & Energetic Materials (A&EM)	15
E. Aeronautics	17
F. Marine Systems	19
G. Guidance, Navigation & Vehicle Control (GN&VC)	21
H. Space Systems	23
I. Power Systems	24
J. Manufacturing & Fabrication (M&F)	25
V. Future Trends Assessment	27
VI. Appendix: MO Definitions	28

The 7th Annual Defense Technology Collection Trends publication was prepared by Raj Shekhat and James Norvell, of the DSS Counterintelligence Office (CI). 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 Emeric Butler for design and Marion Todaro for editing.

I. Executive Summary

A. Reporting Trends

In 2002, the DSS/CI Office received 818 suspicious contact reports from cleared contractors, DSS industrial security representatives, and special agents. This represents a 14 percent increase over 2001. There are three major reasons for the climb in reported cases. First, the Internet and e-mail provide foreign entities with fast and efficient methods of communication and collection with relative anonymity. This is supported by the fact that 44 percent of all cases involved an e-mail request for information (RFI), up from 32 percent in 2001. Second, DSS continues to see a sharp rise in foreign nations targeting and utilizing a wide variety of methods as organized collection becomes more complex. Finally, due to the events of September 11, 2001 as well as other terrorist threats and activities in the U.S. and abroad, a heightened sense of awareness among DSS field personnel and cleared defense contractors has yielded an increase in case identifications.

B. Country Trends

In 2002, DSS identified 84 countries associated with suspicious activities. The number of associated countries has increased for 6 consecutive years: from 37 countries in 1997 to 47 in 1998; 56 in 1999; 63 in 2000; 75 in 2001, and finally to 84 in 2002. This represents a 227 percent increase from 1997 to 2002. Countries identified represent every social and political climate and DSS continues to see a broad range of targeting. Also of note, in 2002, the top ten collecting countries accounted for 57 percent of all suspicious activity, while the top five countries represented over 40 percent of all suspicious activity.

C. Technology Interests Trends

In 2002, as reported in previous years, the majority of targeted technologies, including those associated with the Department of Defense (DoD) programs and weapons systems, were covered by the International Traffic of Arms Regulations (ITAR). Foreign entities continue to target weapons components, technical information and emergent technologies more aggressively than complete weapons systems and military equipment. Additionally, suspicious activity in 2002 included the targeting of all 18 militarily critical technology (MCTL) categories.

D. Most Frequently Reported Technology Targets

Technologies generating the most foreign interest in 2002 by frequency of targeting include: Information Systems, Sensors & Lasers, Electronics, A&EMs, Aeronautics Systems, and Marine Systems. Although the top technologies targeted remained relatively the same from 2001 to 2002, Electronics moved ahead of A&EMs and Aeronautics Systems.

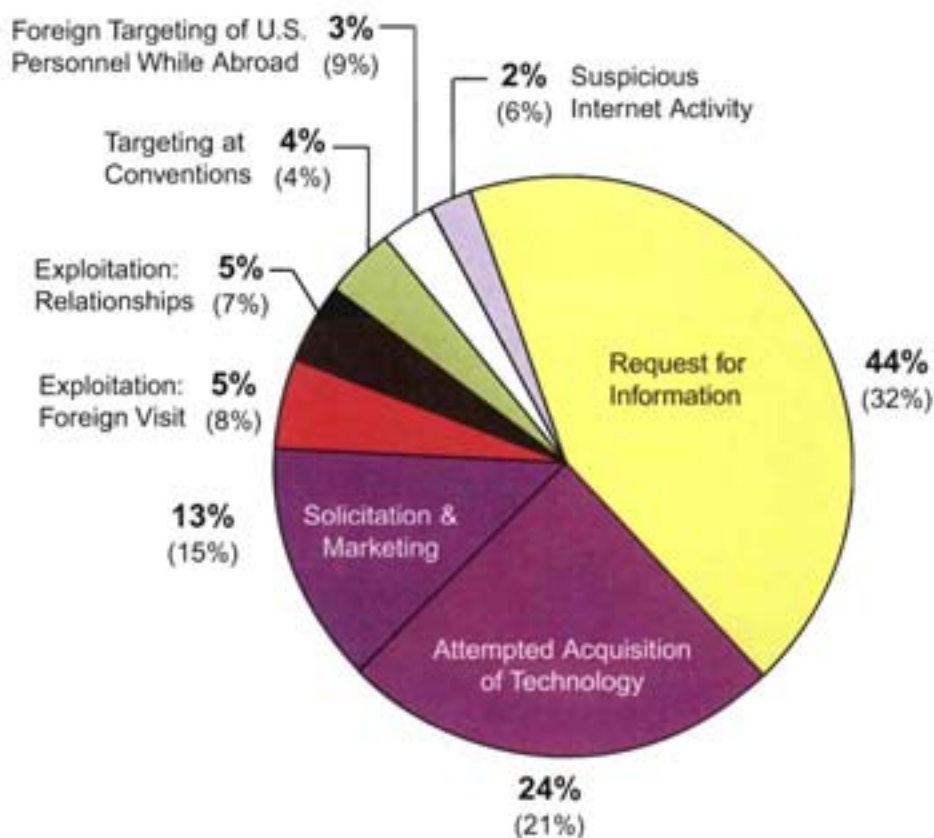
E. Most Frequently Reported Foreign Collection Methods of Operation (MO):

MOs are the techniques employed by a foreign entity to collect intelligence against a given target. Cleared defense companies' reports from 2002 indicate several trends with respect to the variety of MOs employed by foreign entities. MOs associated with potential collection efforts in 2002 are as follows, ranked in order of frequency of occurrence (Note: MOs are defined in detail in the Appendix):

- Request for Information (RFI)
- Attempted Acquisition of Technology

- Solicitation and Marketing Services
- Exploitation of Foreign Visits
- Exploitation of Relationships
- Targeting at Conventions, Seminars, and Exhibits
- Foreign Targeting of U.S. Personnel While Abroad
- Suspicious Internet Activity

Graph 1 Methods of Operation by Foreign Entities in 2002



Note: Percentages in parentheses indicate 2001 values.
 All Charts and Graphs may not total to 100% due to rounding and because MOs representing less than 1% of targeting are not included.

Although foreign entities may use a combination of methodologies, as a particular situation demands, top MOs have remained consistent to those identified in previous years. The overall percentage of RFIs and Attempted Acquisitions increased in 2002, with the top

three MOs having been used in 81 percent of all foreign collection attempts reported to DSS. More detailed information on MOs by specific technology categories is included in the technology section.

II. Introduction

The Defense Security Service (DSS) Counterintelligence (CI) Office has developed the 7th annual trends study as a tool for security professionals. The data and analytical work presented in this study are 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.

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 their possession while performing work on contracts, programs, bids, or research and development efforts.

Based on significant analytical work, this publication provides general information and draws conclusions that help cleared company personnel and DSS personnel recognize and report suspicious foreign activity. Through research presented in this document, DSS enables cleared contractors to enact responsive, threat appropriate, and cost-effective Security Countermeasures (SCM). Moreover, government agencies are encouraged to utilize this reported information to evaluate their own threat environments.

III. World Collection Trends

A. Country Trends: Totals

In 2002, 84 countries were associated with suspicious activities. As the table below illustrates, this number is a 12 percent increase from the number of countries in 2001.

Furthermore, the number of associated countries has increased 6 consecutive years. In 2002, the top ten collecting countries represented 57 percent of all suspicious activity, while the top five accounted for over 40 percent of all suspicious activity.

Table 1 Country Trends

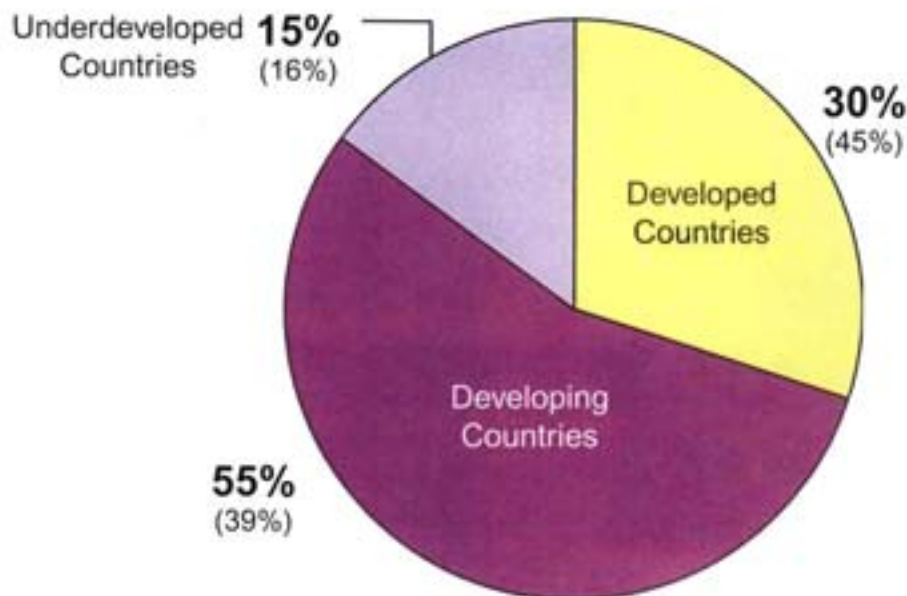
Year	1997	1998	1999	2000	2001	2002
Number of Countries with Identified Collection Involvement	37	47	56	63	75	84

B. Country Trends: Industrial Base Strength

These 84 countries represent every region of the world and every social and political environment. In 2001, the majority of countries targeting cleared contractors were primarily countries with economies and technology industries that were competitive with the United States and with varying degrees of

military capability. In 2002, a new trend is observed, with the majority of collecting nations categorized as still in the development stage. Graph 2 below illustrates this finding. This trend accounts for the fact that components rather than complete defense systems continue to be more heavily targeted. The majority of developing nations are not in a position to build state-of-the-art defense equipment.

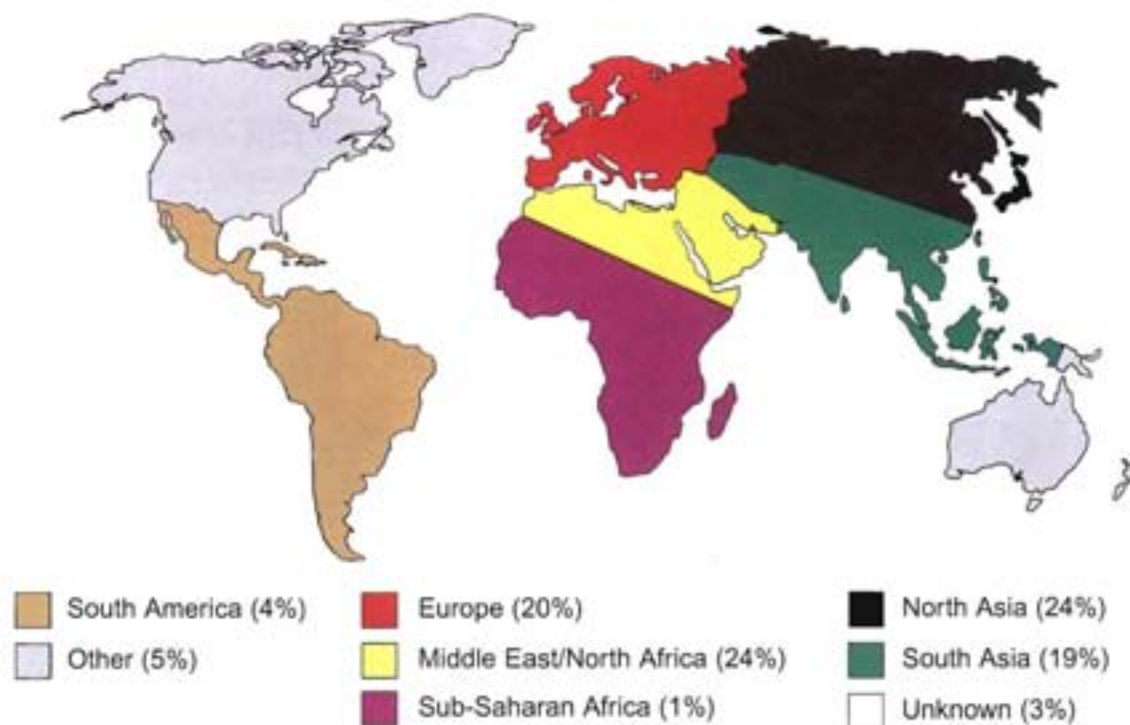
Graph 2 Targeting Based on Foreign Industrial Strength 2002



C. Worldwide Breakdown by Region

Figure 1

Regional Breakdown of Foreign Collection in 2002



The map above reflects the regions where collection efforts originated. The associated percentages indicate the level of collection reported in 2002. The map does not imply national-level support of the collection activity. Collectors may have based their operation in a third country to conceal intentions or identity as the ultimate end-user of collected technology.

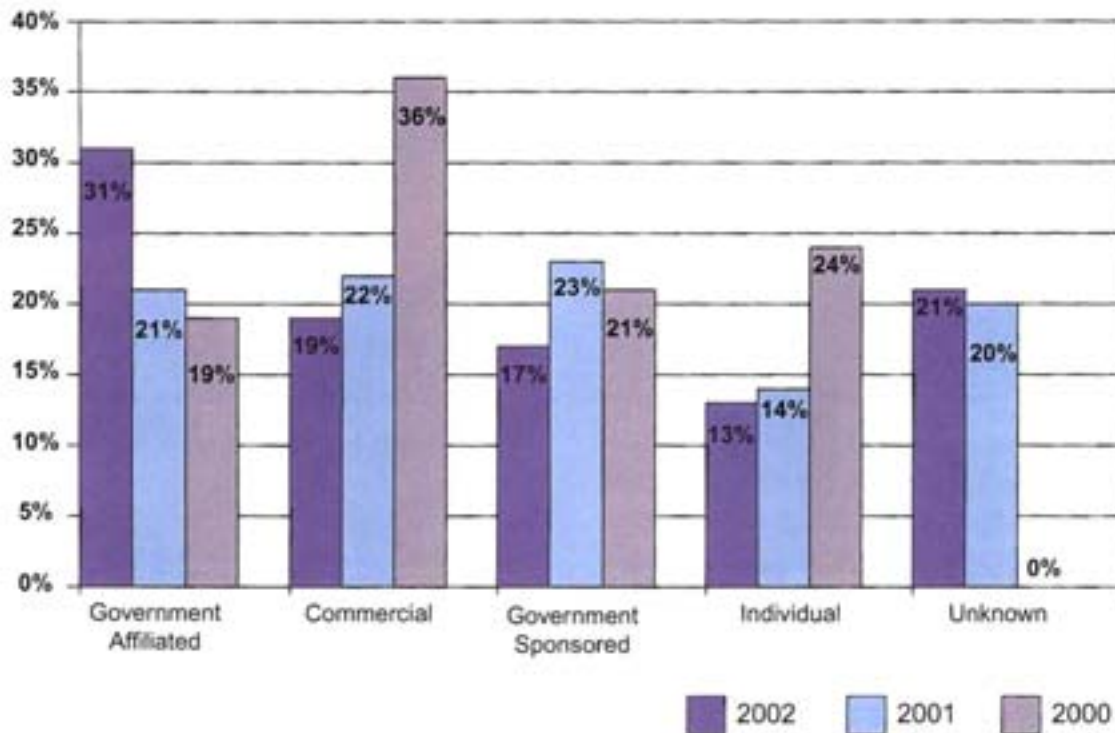
The 2002 sources of targeting outlined in the world map in Figure 1 include North Asia and South Asia, which were presented differently in 2001 as Asia and Eurasia. These two regions are split into North Asia and South Asia to more accurately account for political, religious, and social similarities between countries in Asia. In light of this new reporting methodology, North Asia and South Asia represent a combined 43 percent of all collection in 2002, compared to Asia and Eurasia, which represented a combined 40 percent of all collection in 2001.

Collection within the European region exhibited a comparative decline, falling from 30 per-

cent of total collection in 2001 to 20 percent in 2002. This does not imply a significant decrease in overall targeting by countries within the European category, but rather a more significant increase in targeting from Asian and Middle East/North African nations. The Middle East/ North Africa region increased from 17 percent in 2001 to 24 percent in 2002. In addition, South America showed comparative declines in targeting from 10 percent in 2001 to 4 percent in 2002, and Sub-Saharan Africa also showed comparative declines in targeting from 8 percent in 2001 to 1 percent in 2002.

D. Foreign Collectors

Graph 3
Foreign Collectors of U.S. Technologies



DSS identifies types of collectors after evaluating reported information, conducting extensive research, and assessing relationships and representatives in each incident. Targeting sponsored by foreign governments includes Ministry of Defense, foreign military attachés, and other official government entities. This targeting accounted for 17 percent of all reported cases in 2002, a decrease of 6 percentage points from 2001 reporting. Foreign government-affiliated collection includes research institutes, laboratories, government-funded universities, and contractors representing governments. These types of collectors represent 31 percent of all reported incidents, a significant percentage increase from the 21 percent reported in 2001. (Note: Foreign companies whose work is exclusively or predominantly in support of government

agencies are also included as government affiliates.)

Foreign commercial activities are businesses engaged in the commercial and defense sectors, whose suspicious activity is not associated with foreign governments. Foreign commercial collection has continued to decrease relative to other types of collection from 36 percent in 2000 to 19 percent in 2002. Although corporate collection is attributed to the dual-use nature of many technologies, the rapid decline in commercial collection over the past 3 years is correlated with the increase in government-affiliated collectors. DSS analytical work suggests that the increase in government-affiliated collection is linked with the decrease in commercial collection for two reasons: (1) More accurate

identification of the ultimate end-user, and (2) The large increase in targeting from countries that maintain a strong union with their own (foreign) companies.

Finally, foreign individuals include those individuals for whom DSS has been unable to identify an affiliation because of a lack of information (where only a name or e-mail address is known). The number of reported individual collection attempts has decreased over the last 3 years, as DSS continues to aggressively identify affiliations held by individuals. 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.

Foreign government-related collection represented almost 50 percent of attempts in 2002.

The continued increase in foreign government-affiliated collectors highlights the possibility that governments direct their research institutes, universities, and science and technology academies to develop and acquire desired technologies. As noted earlier, many sensitive military technologies are dual-use, so technological expertise in these areas not only contributes to military superiority but also to a profitable industrial base. In light of this and the findings illustrated in Graph 3 (previous page), foreign government-affiliated collection is expected to rise. DSS expects foreign government-affiliated collection to increase at the expense of direct government-sponsored collection as nations attempt to gather desired information through a more indirect route.



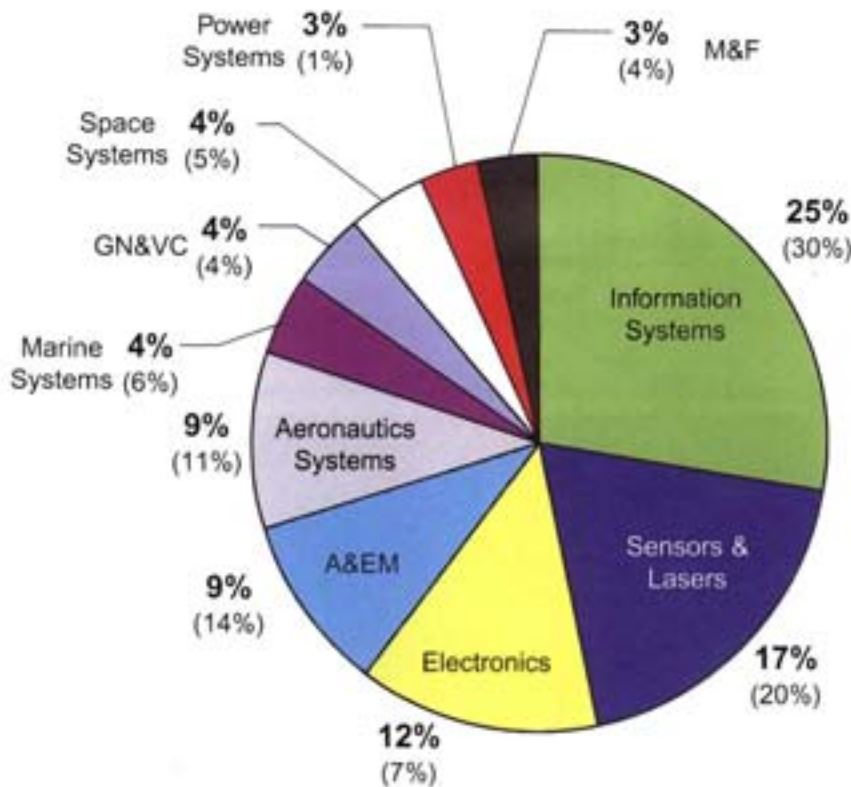
Figure 2: Shipments to the Port of Umm Qasr, Iraq

IV. Technology Analysis for Top 10 Categories

DSS documents and reviews foreign interests in critical U.S. defense technology in 18 categories. The Militarily Critical Technology List (MCTL) is the primary reference for DSS to identify and describe militarily critical technologies and subcategories. The MCTL is a

detailed and structured compendium of the emerging technologies the DoD assesses to be critical to maintaining superior U.S. military capabilities. The MCTL can be found on the Internet at www.dtic.mil/mctl. The following is a detailed look at the top militarily critical technologies targeted in 2002. (Graph 4 breaks down the overall targeting)

Graph 4 Top 10 Technologies Targeted in 2002



A. Information Systems

Overview—Information Systems remained the single most targeted militarily critical technology category, accounting for a quarter of all suspicious collection activity reported to DSS in 2002. Interest in this category, relative to other technologies, decreased by 5 percentage

points from 2001 reporting. However, 58 (70 percent) of the 84 foreign countries associated with suspicious activity in 2002 attempted to collect information systems technology. This is a significant increase from last year, when 44 countries were associated with similar collection activity, and can be partly attributed to an increase in their indigenous military pro-

Collection Incidents for Information Systems Subcategory 1997-2002 (continued)

Information Systems	1997	1998	1999	2000	2001	2002
Intelligent Systems	4	3	0	11	5	28
Modeling and Simulation	5	6	6	12	17	11
Network Switching	4	1	0	1	10	28
Signal Processing	0	1	3	9	20	21
Software Systems	10	15	13	33	27	8
Transmission Systems	5	6	4	29	1	4

Example of Information Systems Collection Attempt

Information systems trend from 2001: targeting of encryption technologies.

Attempted acquisition was the primary method of targeting of encryption devices. Foreign



KG-84 cryptographic devices



KIV-7HS

entities attempted to purchase encryption devices such as the KG-194, KIV-7HS, and the KG-84 (pictured above) without proper export

licenses. Also targeted were submersible and miniature lightweight secure radios. Government affiliated and commercial entities were identified with the majority of targeting in those cases.

In 2002, two individuals were found guilty of attempting to export KIV-7 HS technology to China. The highly publicized arrests followed a 4-month investigation by the Customs Special Agent-in-Charge Office in Baltimore. The technology that these individuals were attempting to export includes the most sensitive items on the U.S. munitions list. The KIV-7HS encryption unit/technology is designed for government use only and cannot be legally exported from the U.S. without first obtaining an export license from the State Department. An undercover Customs agent, posing as the intermediary, engaged in a series of telephone conversations and faxed correspondence with the subject. Correspondence revealed that the subject was affiliated with a Singapore-based company, the buyer of the KIV-7HS units. The subject asked if the undercover agent could obtain the license. After being told by the undercover agent that no license would be approved for export to China and that export to China would be a violation of the Arms Control Export Act, the subject continued to show interest. On August 24, the subject confirmed to the U.S. Customs undercover agent that the KIV-7HS units would be shipped from Los Angeles through Taipei to Singapore, then forwarded to China.

duction capabilities. Fifty-four percent of all collection was government sponsored or affiliated and 12 percent involved commercially related collection.

Modeling and simulation technology was also significantly targeted in 2002. This technology encompasses a wide-range of dual-use applications, ranging from engineering design to flight trainers and simulators. The key elements of this technology involve digital processing to manipulate the data, human systems interface (through which the users inter-



Figure 3: Satellite

act with the data) and the knowledge embedded in the software. Several incidents involved the targeting of Electromagnetic Pulse (EMP) model and simulation software. In one incident, a foreign entity attempted to obtain modeling and simulation software for EMP weapons effects.

Specific targeted technologies included:

- CPU Chips
- EMP Simulation—to analyze HEMP/APM vulnerability/lethality
- Interactive Technical Manuals
- Intercept Technology Platforms (PLS, GSM, CDMA)
- Microwave Technology
- Mobile Computing Devices
- Multiple Encryption Technologies
- Multiple Modeling & Simulating Technologies (electromagnetic pulse)
- Multiple Software Platforms (JOVIAL, GIS)
- Simulator Technology
- Video Tracking System

Table 2

Collection Incidents for Information Systems Subcategory 1997-2002

Information Systems	1997	1998	1999	2000	2001	2002
Command, Control, Communications, Computing, Intelligence (C4 I)	6	5	5	8	24	12
Computer Aided Design, (CAD) Computer Aided Manufacturing (CAM)	1	1	2	4	2	2
High-Performance Computing	2	5	0	3	3	3
Human Systems Interface	0	0	0	0	0	4
Information Security	13	6	2	21	16	7

Graph 5

Methods for Targeting: Information Systems



Note: For all graphs, the 2001 values that are not shown were unavailable

B. Sensors & Lasers

Overview—Sensors & Lasers remained the second most targeted technology category, comprising 17 percent of all suspicious collection activity reported to DSS in 2002. Interest in this category decreased from 2001 by 3 percentage points, compared with other technologies. Moreover, the number of countries targeting sensors and lasers stayed relatively stable from the previous year, with 40 countries reported in 2002 versus 41 countries reported in 2001. Additionally, 50 percent of all collection was government sponsored or affiliated.

Acoustic Sensors remained the most heavily targeted subcategory within Sensors & Lasers, representing almost 68 percent (46 out of 68 total attempts) of collection within the category. Marine passive sonar technology was again the most targeted technology within the Acoustic Sensors' sub-category, accounting for 37 percent. Passive sonar has little commercial application aside from limited academic research and is predominantly used for covert military location of underwater objects that radiate sound, and more specifically for antisubmarine and antisurface warfare.

In addition, air and terrestrial platform

collection quadrupled from 3 attempts in 2001 to 12 attempts 2002. Air platforms are those applications used on aircraft to reduce noise levels and aircraft acoustic vibrations. Terrestrial platforms are seismic acoustic systems for location and identification of petroleum producing features within the earth's crust. Passive acoustic terrestrial systems are included for intruder detection and for the detection and location of target vehicles and direct fire weapons. Air and terrestrial platforms, like other acoustic sensor technologies, are targeted based on military needs.



Figure 4: Ship Radar

DSS noted a sharp decline in reports of targeting against electro-optical sensors. These sensors have military applications that facilitate operations at night or under conditions of limited visibility. This technology is used in night-vision goggles, vehicle drive systems and weapons sights. As reported in 2001, several countries had second and third generation image-intensifier capabilities based on assessed technology transfers. This suggests that the decline in reported targeting of electro-optical sensor technology, in 2002, may in part be a result of countries having

Table 3

Collection Incidents for Sensors & Lasers Subcategory 1997-2002

Sensors and Lasers	1997	1998	1999	2000	2001	2002
Acoustic Sensors	4	18	2	5	41	46
Air and Terrestrial Platforms	N/A	N/A	N/A	N/A	3	12
Marine Passive Sonar	N/A	N/A	N/A	N/A	17	17
Marine Platform	N/A	N/A	N/A	N/A	11	5
Other Acoustic Sensors	N/A	N/A	N/A	N/A	0	7
Electro-Optical Sensors	N/A	N/A	N/A	N/A	0	0
Focal Plane Array/Infrared	8	11	5	5	7	11
Radars	5	8	22	9	20	5
Imagery	5	13	8	3	12	0
Lasers	0	0	4	8	24	4
Other	2	10	5	14	21	0

Note: Acoustic sensors were not subcategorized prior to 2001

sufficiently updated or accepted current second or third generation sensors available to them.

Specific targeted technologies included:

- Mobile Air Defense Radar
- Mine Detection System

- Microwave Radar
- Patriot Radar
- Photo Divide Array Sensor
- TVS 8000 (High-tech Infrared Camera)
- Cargo Inspection System

Example of Sensors & Lasers Collection Attempt

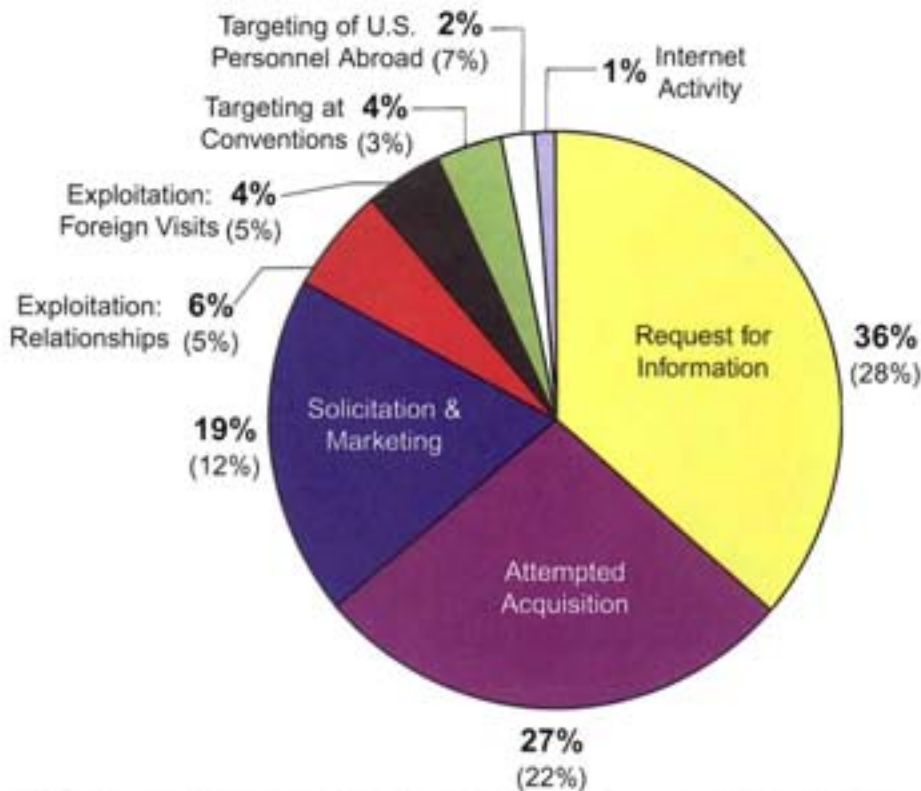
A cleared DoD contractor received an e-mail request from an embargoed nation to purchase several thousand sonobuoys. A sonobuoy is an instrument that is dropped into the ocean (from either an aircraft or ship) to record underwater sounds. It includes a hydrophone and a radio transmitter to send sound signals back to the aircraft or ship. The U.S. Navy uses sonobuoys to detect enemy submarines. The DoD contractor believed the request to be suspicious because of the high number requested. The contractor also suspected that the sonobuoys would be transferred to a third country.



Figure 5: Sonobuoy

Graph 6

Methods for Targeting: Sensors & Lasers



C. Electronics

Overview—Foreign targeting of electronics technologies moved from 5th in 2001 to 3rd most frequently targeted technology in 2002, with 34 countries accounting for 12 percent of all targeting. In 2001, 24 countries targeted electronics technologies, accounting for 7 percent of all targeting. Foreign government and government affiliated entities represented 58 percent of all electronics targeting efforts, followed by commercial entities representing 28 percent and individuals accounting for 10 percent. This remained consistent with 2001 reporting, where 60 percent of electronics targeting was associated with foreign government and government affiliated entities.

The majority of electronic targets fall within the materials/components and fabricated subcategories. Specific targeted technologies included:

- Band Pass Filters
- Combiners
- Monolithic Microwave Integrated Circuit (MMIC) Chips
- Oscillators
- Pin Diodes
- Phase Shifters
- RF Filters
- SP12T Absorptive Switch
- Wave Guides



Figure 6: Electronic Circuit Board

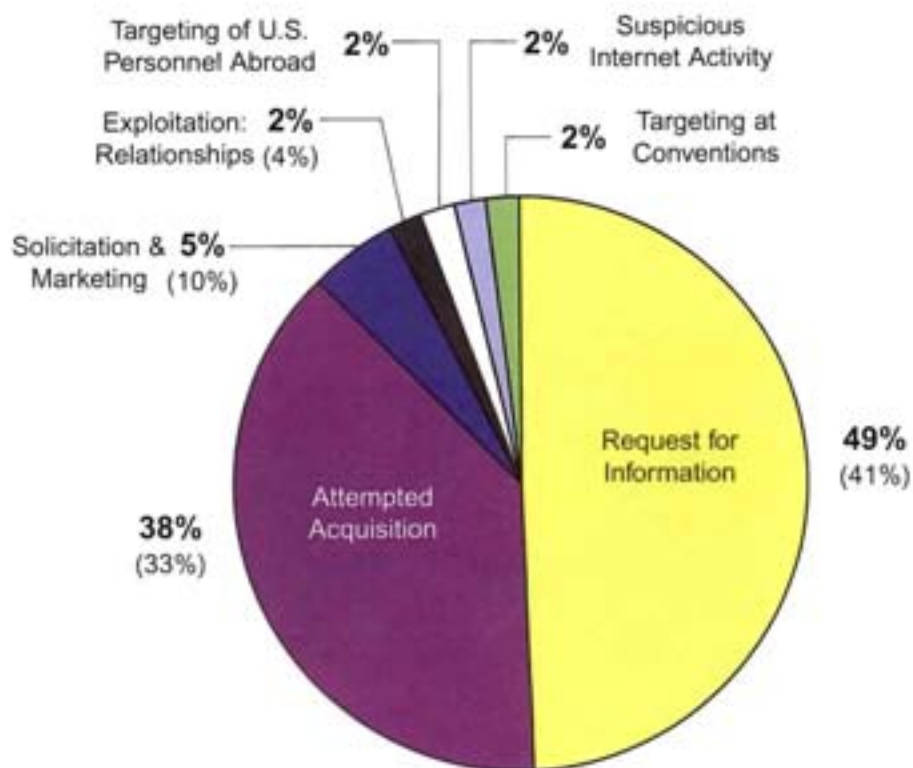
Table 4

Collection Incidents for Electronics Subcategory 1997-2002

Electronics	1997	1998	1999	2000	2001	2002
Materials/components	4	6	12	1	17	50
Fabricated materials	2	3	1	0	5	31
Microelectronics	5	2	4	7	1	1
Optoelectronics	4	1	1	1	2	2

Graph 7

Methods for Targeting: Electronics



D. Armaments & Energetic Materials (A&EMs)

Overview—A&EMs was the 4th most targeted technology, representing 9 percent of all suspicious collection activity reported to DSS in 2002, a decrease, relative to other technologies, of 6 percentage points from 2001 reporting. However, the number of countries targeting A&EMs increased from the previous year, with 29 countries reported in 2002, versus 27 countries reported in 2001. In addition, 36 percent of all 2002 collection of A&EMs was government sponsored or affiliated collection.

There has been a dramatic increase in the pursuit of "smart weapon" design and develop-

ment, with only a few countries currently capable of producing guided and individually targeted multiple-reentry weapons. The extended range and superior level of accuracy of "smart weapons" will continue to make this critical technology a targeted commodity.

U.S. advanced A&EM technology continues to be a major target for foreign collectors worldwide, who are attempting to update and integrate core weapons systems of military, paramilitary and terrorist forces. It is clear from DSS analysis that there is a growing trend towards the A&EM subcategory, General A&EM Targeting, as developing foreign collectors attempt to improve all areas of this critical technology. Analysis supports the

conclusion that developed and, more importantly a larger number of developing countries continue to aggressively target the entire spectrum of A&EMs because of their limited knowledge of these weapons systems.

Specific targeted technologies included:

- Advanced Gun Barrels
- AIM-9X/9M
- Classified Patriot Data
- Crusader Missile

- Explosive Stands for Lab Testing - Nitroglucose, rdx TNT
- Land Attack Standard Missile
- MK 36 Sidewinder Rocket Motor
- MK 38 Machine Gun System
- Missile Data
- Objective Individual Combat Weapon
- TOW2/TOW2A Weight and Propulsion Data

Table 5

Collection Incidents for Armaments & Energetic Materials Subcategory 1997-

Armaments & Energetic Materials	1997	1998	1999	2000	2001	2002
General A&EM targeting	0	0	0	0	28	71
Ammunition, small/medium caliber	0	0	0	0	4	1
Bombs, warheads, large caliber projectiles	5	8	4	16	24	4
Energetic material	0	1	1	1	32	1
Safing arming, fusing, firing	1	1	0	5	9	9
Gun and artillery systems	1	4	4	1	9	3
Mines, countermines, and demolition systems	1	1	0	1	2	3

Example of Armaments & Energetic Materials Collection Attempt



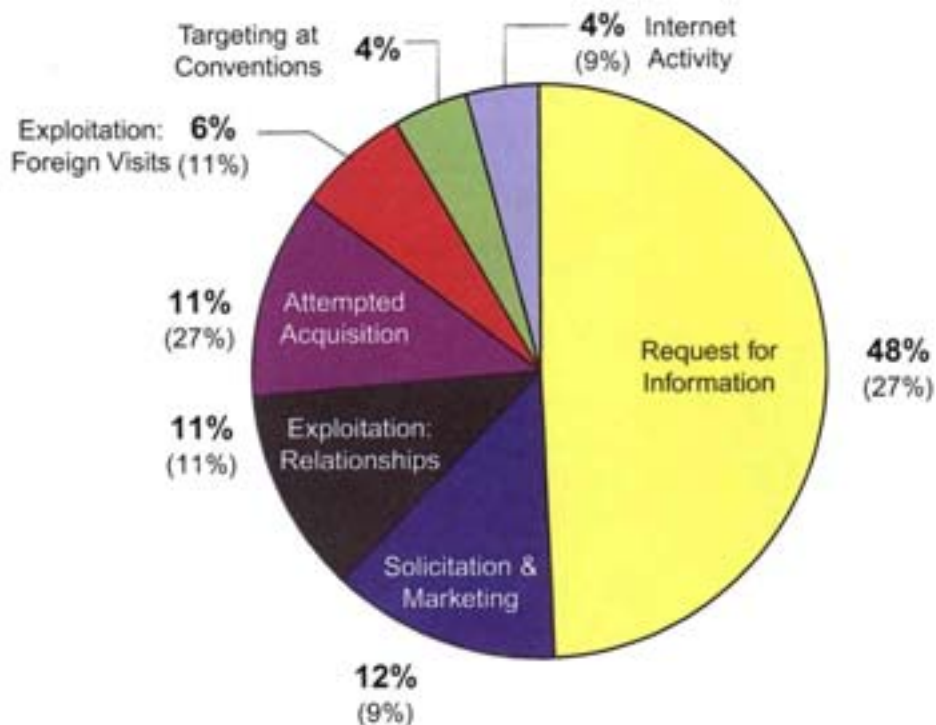
Figure 7: Surface-to-Air Missiles

A cleared contractor in Pennsylvania received e-mail from an embargoed nation requesting information concerning advanced gun-barrel technology. It appears the information was requested in order to prolong the life of gun barrels within the country and was surprisingly requested by a medical professional. Open source research could not find the foreign company; however, open source research associated three separate foreign government defense contractors with a telephone number on the e-mail. These

foreign government contractors were associated with front companies.

Graph 8

Methods for Targeting: Armaments & Energetic Materials



E. Aeronautics Systems

Overview—Aeronautics technology was tied for the 4th most targeted technology, accounting for 9 percent of all 2002 reports. This marked a 2-percentage point decrease, relative to other technologies, from 2001 reporting. Thirty-eight different countries attempted to collect aeronautics technology in 2002. Moreover, 45 percent of all collection was government sponsored or affiliated. The technologies placed in this category include those associated with aircraft, aero-gas turbine engines and the human interface technology

within aeronautics systems. In 2002, there were a total of 92 incidents of aeronautics technology being targeted, including fixed wing aircraft parts and engine technology. In one instance, an embargoed nation requested specific engines for use in their military aircraft.

Specific targeted technologies included:

- Gas Turbine Engines
- F-18
- F-16C/J Blueprints
- Unmanned Aviation Vehicles (UAV)

Table 6

Collection Incidents for Aeronautics Systems Subcategory 1997-2002

Aeronautics	1997	1998	1999	2000	2001	2002
Aircraft, fixed wing	10	5	6	11	46	13
Gas turbine engines	8	5	7	3	7	12
Human (crew systems) interface	1	5	0	1	0	1
Energetic material	3	1	1	4	9	3
Safing arming, fusing, firing	4	4	1	4	21	18



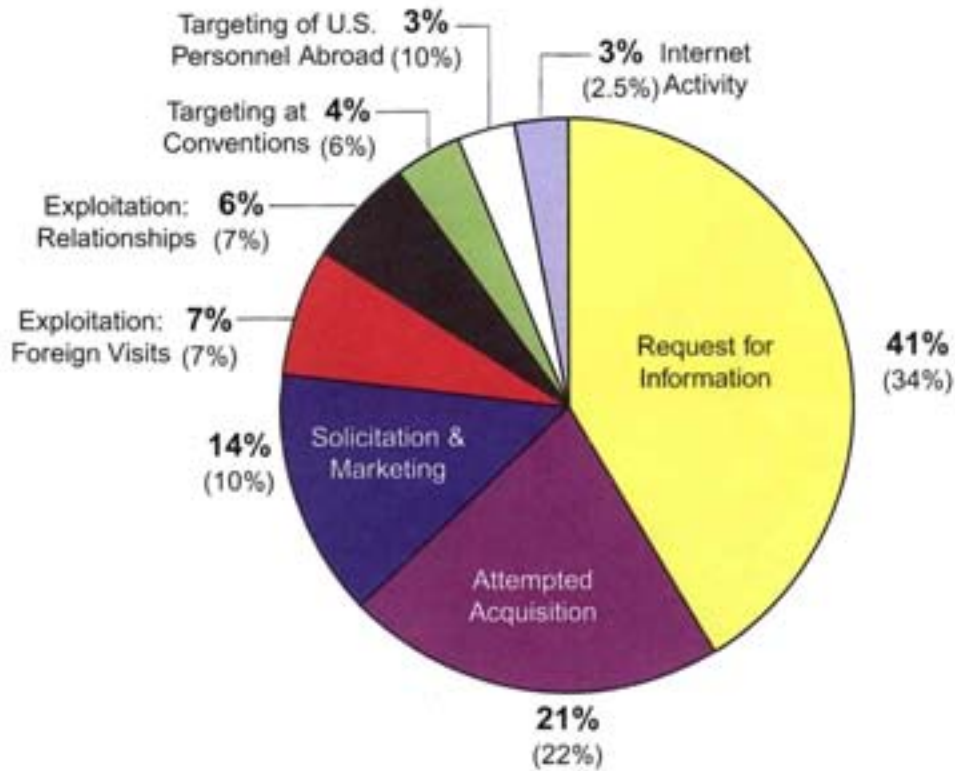
Figure 8: F-15 Eagle

Example of Aeronautics Systems Collection Attempt

An individual from an embargoed country e-mailed a cleared DoD contractor with a request to purchase a "sample" Unmanned Aerial Vehicle (UAV). Depending upon its performance, the individual stated that he might purchase "many more". The individual also requested performance characteristics of the UAV, which were export controlled. The individual involved was identified by DSS in three other unauthorized attempts to obtain export-controlled aeronautics technology from other cleared DoD contractors.

Graph 9

Methods for Targeting: Aeronautics Systems



F. Marine Systems

Overview—Marine Systems was the 6th most frequently targeted technology, representing 4 percent of all 2002 targeting, compared to 6 percent of all 2001 targeting. The number of countries targeting Marine Systems stayed relatively the same, with 25 targeting in 2001 versus 26 targeting in 2002. Furthermore, 30 percent of all collection was government sponsored or affiliated. There were 47 incidents reported to DSS by cleared DoD contractors involving marine technology. The majority of these reported incidents, at least 50 percent, involved RFIs sent via email or letter. In addition, there were several reported incidents involving the outright acquisition of marine technology by foreign entities who

either solicited or applied for employment with DoD contractors.

Specific targeted technologies included:

- Blueprints for Aircraft Carrier
- DD-21
- Electroware Absorption
- Guided Missile Destroyer
- General Information on Ships & Submarines
- Information on Hull Thickness at Specific Points in Ships
- Marine/Hydrographic Surveyor
- Propeller Design
- Turbines on Ships
- Underwater Acoustics
- Unmanned Undersea Vehicles

Table 7

Collection Incidents for Marine Systems Subcategory 1997-2002

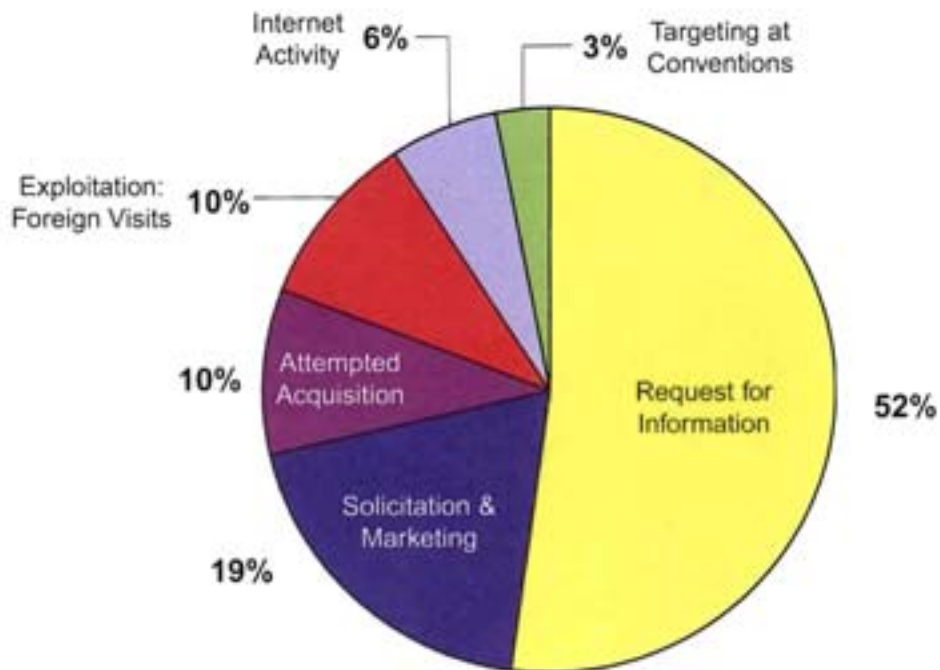
Marine Systems	1997	1998	1999	2000	2001	2002
Propulsors and propulsion system	3	1	0	1	0	3
Signature control and survivability	1	2	2	5	1	1
Subsurface and deep submergence vehicles	2	0	2	3	1	2



Figure 9: Attack Submarine USS Seawolf

Graph 10

Methods for Targeting: Marine Systems



G. Guidance, Navigation, & Vehicle Control (GN&VC)

Overview—GN&VC technology was the 7th most targeted technology, comprising 4 percent of all suspicious collection activity reported to DSS in 2002. Overall interest in this category remained at 4 percent of all collection efforts; however, GN&VC technology was the 10th most targeted in 2001. The total incident number increased from 28 in 2001 to 42 in 2002. Fifteen countries targeted GN&VC technology in 2002, with the top country representing 26 percent (11 of 42) of the total. Furthermore, 44 percent of all collection was government sponsored or affiliated. The number of incidents of targeting has increased from 2001 because military ships, vehicles, and platforms require precision guid-

ed technology and navigation capabilities. DSS expects a continual increase in the targeting of GN&VC technology given that current trends in warfare require increasingly accurate guided long-range systems.

Specific targeted technologies included:

- Avionics System Auto-pilot Technology
- Air Defense Simulator
- GPS Sensors
- GPS Software Simulation Tools
- Gyro Stabilizers
- Inertial Navigation System Technology
- Laser Gyroscopes
- Fiber Optic Inertial Measuring Unit
- Transponders

Example of Guidance, Navigation, & Vehicle Control Collection Attempt

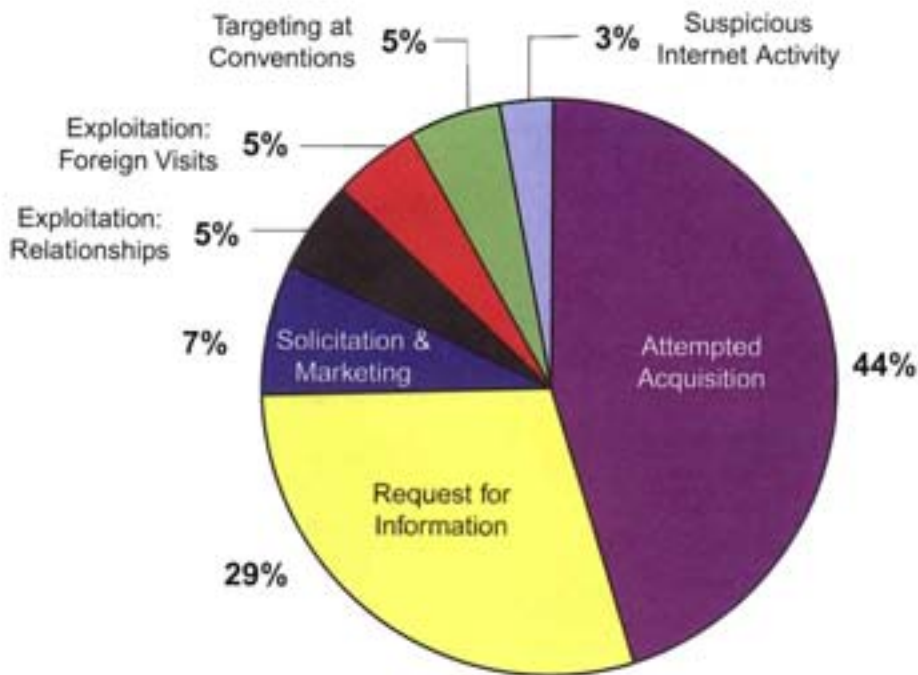


A cleared company received several phone calls to purchase ten, export-controlled ring laser gyroscopes for a foreign company. When asked to provide the names of the end-user, the caller never responded. He left several messages requesting the gyroscopes. Ring laser products are produced for a number of aerospace, land vehicle, marine and space applications.

Figure 10: Ring Laser Gyroscope

Graph 11

Methods for Targeting: Guidance, Navigation, & Vehicle Control



H. Space Systems

Overview—Space Systems technology was the 8th most targeted technology, comprising 4 percent of all suspicious collection activity reported in 2002. Interest in the category decreased slightly, relative to other technologies, by 1 percentage point from 2001 reporting. However, the number of countries targeting Space Systems increased significantly from the previous year, with 23 countries reported in 2002 versus 14 in 2001. Additionally, 67 percent of all collection was government sponsored or affiliated.

Electronic RFIs accounted for 29 percent of all MOs; however, more surprising is the fact that attempted acquisition of space systems technology represented 44 percent of all MOs. As reported last year, the loss of critical information through web site advertising by

cleared U.S. defense contractors is of great concern. More specifically, the sites provide information that includes names of defense contractors, universities researching critical technology, government agencies conducting R&D, and event calendars and locations. DSS analytical work suggests that, as defense contractors continue to provide "directional" information to foreign collectors, attempted acquisition will continue to be the easiest method of operation for accessing sensitive technology.

Specific targeted technologies included:

- GPS Satellite
- Overhead Surveillance Technology
- Satellite Photo Imagery System
- Satellite Information
- Space Component Information

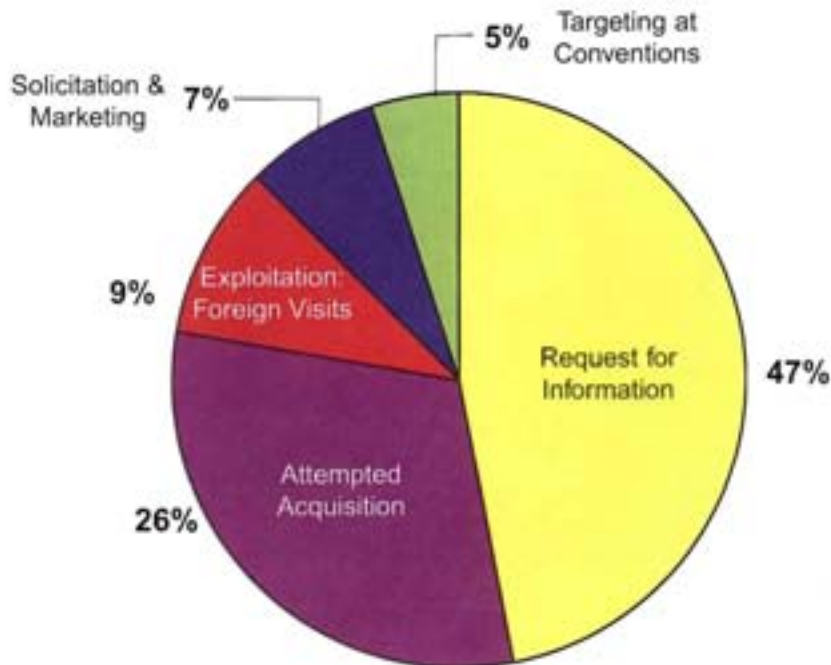
Example of Space Systems Collection Attempt



Figure 11: International Space Station

An e-mail request was sent to a cleared defense contractor from an embargoed nation requesting Global Positioning System (GPS) code signal and performance capabilities for GPS satellites. The e-mail was sent from a faculty member of a foreign state-run university and included the following detailed questions about GPS technology:

- 1) The maximum radial velocity appears when the GPS satellite crosses the horizon. Why?
- 2) The C/A/ code signal on L1 is twice as powerful as the P-code signal on L1. Why?
- 3) What is the role of L3 and L4 in the GPS system?



I. Power Systems

Overview—Power Systems was the 9th most frequently targeted technology in 2002, representing 3 percent of all collection attempts, compared with 1 percent of all attempts in 2001. Additionally, 13 countries targeted power systems in 2002, and 54 percent of all targeting involved government or government affiliated entities, while 34 percent involved commercial entities. Power systems technology includes electric subsystems and systems in literally hundreds of kinds of military equipment. These ongoing applications dictate military requirements for power level, power reliability, ruggedness, packaging and the ability to operate in a wide-range of environments. Technologies targeted within power systems in 2002 included fuel cell technology, batteries, pulse generators and magnets used in power systems.

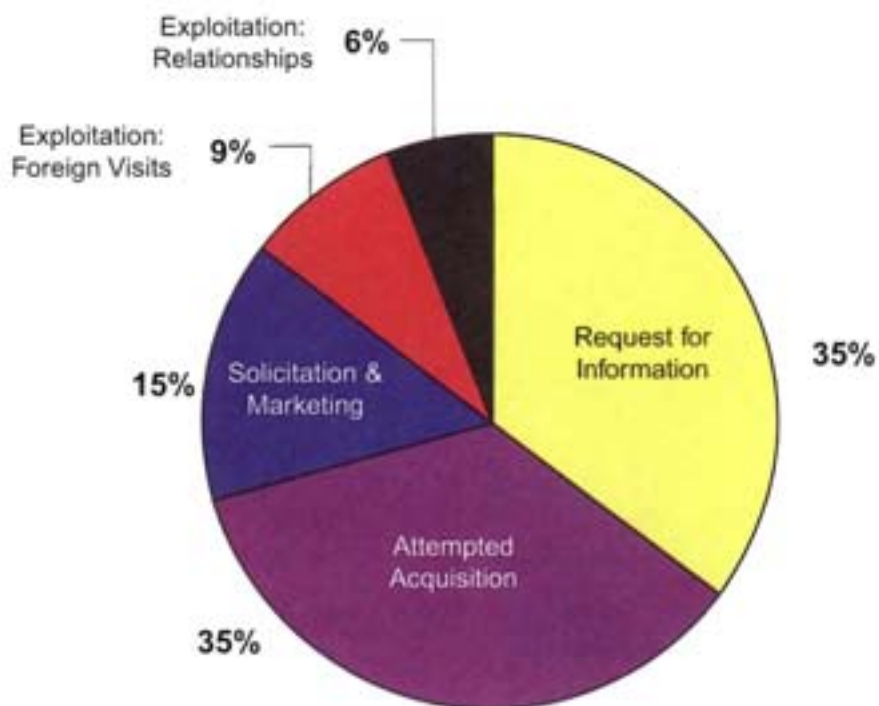
The majority of targeting focused on batteries, including high power lithium, thermal, and hydrogen batteries. The two most prevalent MOs identified with power systems were requests for information and attempted acquisition of technology, each accounting for 35 percent (or a total of 70 percent) of all targeting. Solicitation and marketing of services accounted for 15 percent of the targeting efforts.

Specific targeted technologies included:

- Diesel Systems for Patriot Missile
- Energy Light Battery Cells
- Hydrogen Battery Cells
- Lithium Battery Cells (High-power)
- Magnets (High-power)
- Silver-Zinc Battery Cells

Graph 13

Methods for Targeting: Power Systems



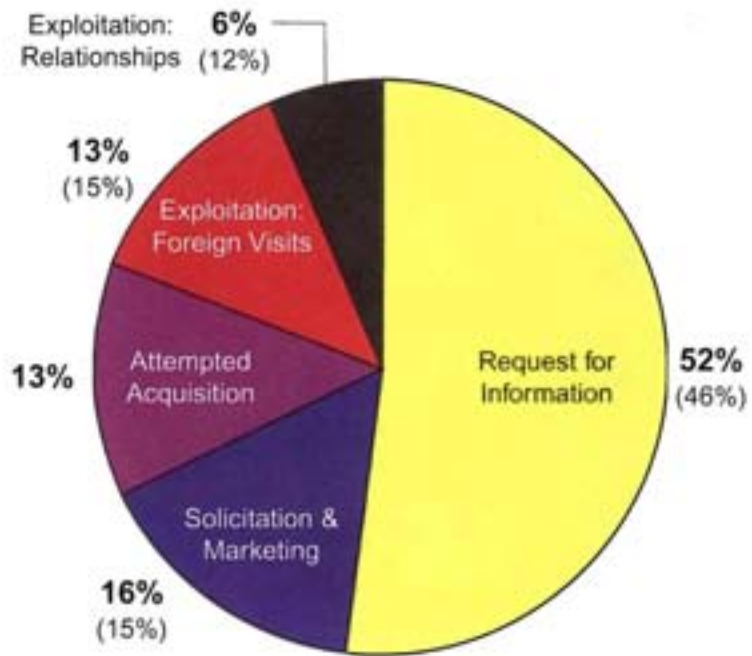
J. Manufacturing & Fabrication (M&F)

Overview—M&F technology was the 10th most targeted technology, comprising 3 percent of all suspicious collection activity reported to DSS in 2002. Interest in the category decreased slightly relative to other technology, by 1 percentage point from 2001 reporting. Additionally, the number of countries targeting M&F technology increased from the previous year, with 18 countries reported in 2002, versus 15 countries reported in 2001. Furthermore, 50 percent of all collection was government sponsored or affiliated.

The most common method of targeting for the technology was through RFIs, which occurred in 52 percent of all attempts in 2002, compared with 46 percent of all attempts in 2001.

Specific targeted technologies included:

- Calibration Technology
- Fabrication Vacuum Vessels
- Pressure Vessels - Kevlar Air Fuel Tanks
- Rocket Motor Case Fabrication Methods



V. Future Trends Assessment

The analytical work presented in this document clearly brings into focus new trends that were seen in 2002. The most significant of these is the substantial increase in targeting by developing nations and the multiple trends that seem to support this demographic shift.

As mentioned in the World Collection Trends section, it is clear that developing nations have become the most significant threat collectors to the U.S. Defense Industry, with over half of all attempted collection originating in developing nations. This is also illustrated in the regional geographic trends where areas with large numbers of developing countries (Asia, Middle East) have shown an increase in collection and regions with primarily developed nations (Europe) have shown declines. It is also important to note that in some cases developing nations may be utilizing developed countries as a base for their targeting operations and vice versa.

Developing nations will continue to produce small arms and ammunition as well as military aircraft, armored vehicles, naval vessels, and even ballistic missiles. Furthermore, these countries aim to integrate newer technologies into their products and hence reduce their dependence upon foreign military hardware. In some cases the belief is that a robust weapons program will reduce the effects of arms embargoes, interruptions in the flow of spare parts, restrictions on the use and resale of foreign weapons, and suppliers' attempts to influence their foreign and domestic policy.

With regard to actual targets, Information Systems and Sensors will most likely remain the two most frequently targeted categories by mostly government or government affiliated

entities in the coming year. Of note, Chemical and Biological Systems fell from the top 10 list of targeted technologies to 12th overall. The current global climate and the high level of interest in development and acquisition of biological and chemical weapons by foreign nations, militaries, and terrorist groups over the last few years does not directly align with the decreasing trend cited in the DSS analysis. Further research suggests that many of the cleared facilities handling biological and chemical systems have ramped up security-levels in light of significant global interest. More importantly, it is possible that foreign groups interested in these technologies may have targeted other nations or already acquired the desired systems.

Another important trend is the significant rise in government-affiliated collection over the last 3 years, with a simultaneous decrease in both commercial and individual targeting compared with other collectors over the same period. As stated earlier, more accurate detection of the real end-user is one reason for the noted trend. However, DSS has seen a sharp increase in targeting by nations that have a clear hand in their foreign companies' operations. These countries tend to be either in the developing stage or close to other hostile nations.

Additionally, there are important observations to note with regard to foreign methods of operation. First, nations targeting U.S. technology will continue to use whatever method is available to them to acquire technology or information. Countries vary in their methods, and, as the number of countries targeting U.S. technology matures, the expectation is that the methods will remain broad. One exception is that the RFI and Attempted Acquisition are two MOs that will continue to be the most

popular MOs. The increase in RFI use is obvious because all countries targeting new technology start at this point; however, the rise in Attempted Acquisition is slightly more of a concern. Foreign entities are able to save significant time and money by acquiring technologies, which cuts out costs associated with research and development. The next step then becomes reproducing the technology.

As noted earlier, advertising and information provided by defense contractors through their

web-sites and in other formats are a major starting point for attempted foreign acquisition. In many cases RFIs can be bypassed in favor of outright acquisition of the desired target. The cleared contractor will likely be the most lucrative target and DSS estimates that reports of suspicious activity will increase from the 818 reported in 2002 despite active security countermeasures taken by these companies.



VI. Appendix: MO Definitions

Request for Information (RFI). A request for information is any request, not sought or encouraged 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 actually been indirectly solicited. 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.

Attempted Acquisition of Technology. This MO involves foreign entities attempting to gain access to sensitive technologies by purchasing U.S. companies and technology. Once a foreign entity gains ownership, control, or influence over a U.S. company with classified contracts, that ownership, control or influence must be mitigated through an insulating instrument approved by the United States Government. If such an approved insulating legal instrument is not implemented, the U.S. company and the foreign investor face the possibility of contract cancellations and loss of future classified contracts.

Solicitation and Marketing of Services. In this MO, consistent with past reporting, foreign individuals with technical backgrounds offer their services to research facilities, academic institutions, and even cleared defense contractors. A number of incidents involved foreign nationals seeking postdoctoral fellowship at cleared universities. Émigrés are continuing to seek employment at companies that are involved in cutting edge technologies.

Exploitation of Foreign Visit. The term "for-

foreign visitor" includes one time visitors, long term visitors (such as exchange employees, official government representatives and students) and frequent visitors (such as foreign sales 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 would request access to facilities or to discuss information outside the scope of approved activities.

Targeting at Conventions. Conventions, seminars and exhibits are rich collection targeting opportunities for foreign collectors. These functions directly link U.S. programs and technologies with knowledgeable personnel. Events provide an opportunity 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 the 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 of Existing Relationships or Joint Ventures. Exploitation of Joint Venture/Research. This MO offers significant collection opportunities for foreign interests. As with frequent foreign 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 product to someone else, they are 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.

Targeting of U.S Personnel Abroad. This MO involves the targeting of U.S. defense contractor employees traveling overseas. The targeting occurs at airports and includes luggage searches, unauthorized use of laptop computers, extensive questioning beyond normal security measures, etc. Other travelers

have received excessively "helpful" service by host government representatives and hotel staffs. Reporting also indicates that traditional FIS collection methods are still used by foreign nations. These measures include surreptitious listening devices, hotel room searches, intrusive inspection of electronic equipment, and positioning of personnel to eavesdrop on conversations.

Internet Activity. Targeting associated with this MO includes exploitation of the Internet (hacking). The majority of the endeavors have been correlated with probing efforts, which account for most of the activity in this category. The computer probes are most likely searching for potential weaknesses in systems for exploitation. In one example, a probing effort that lasted 24 hours originated from a "girls school" in an Asian country. This probing effort was probably masked. The potential exists for users to go to several sites and receive anonymous e-mail addresses. By detecting probes, the cleared companies have already demonstrated they have the security countermeasures in place to thwart attempts to penetrate their computer systems. Although probing a system is not illegal, a crime is committed once a port is breached by an unauthorized entity.