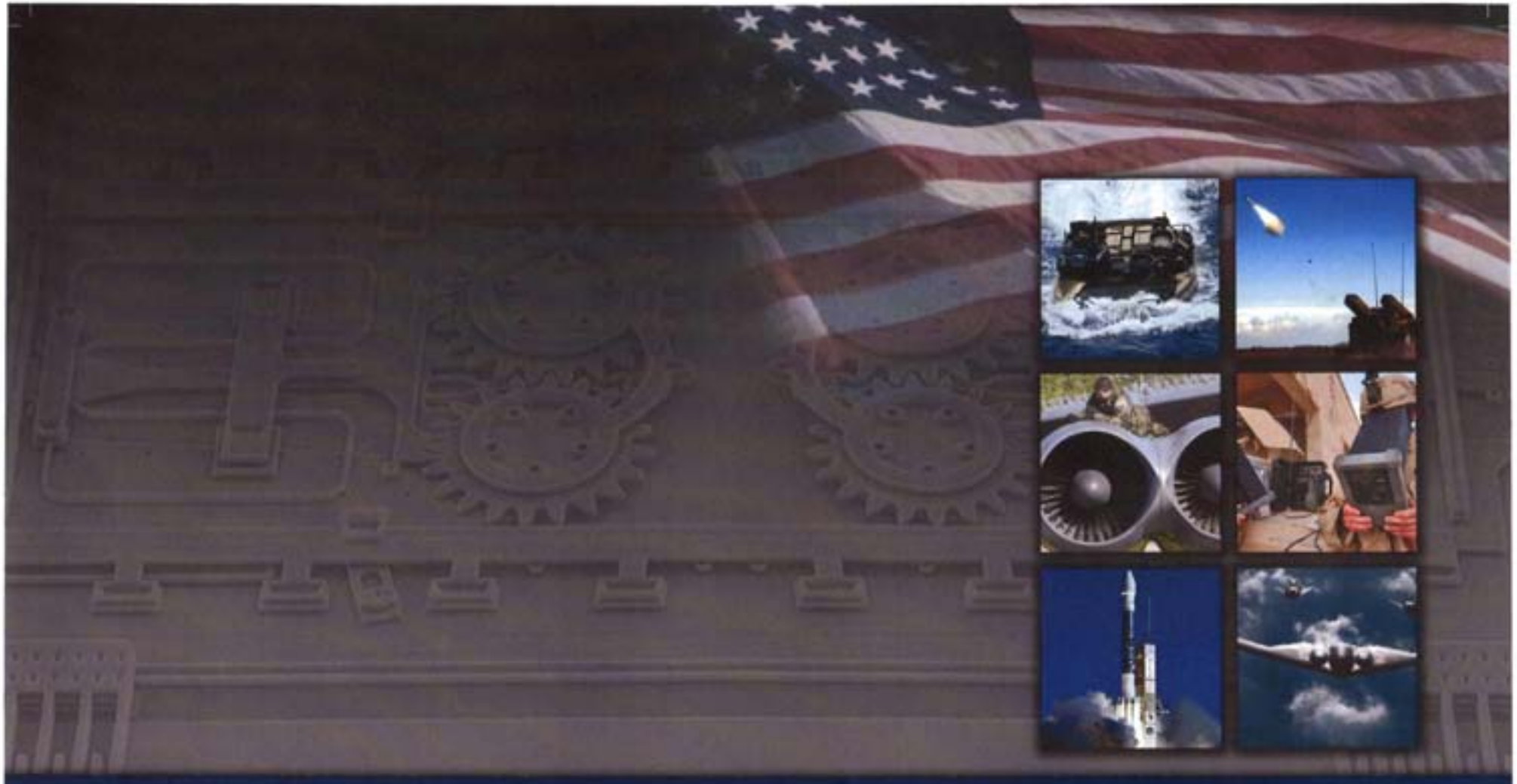


Technology Collection Trends in the U.S. Defense Industry - 2004

Contents

The 8th Annual Defense Technology Collection Trends publication was prepared by the Defense Security Service (DSS) Counterintelligence (CI) Office. Comments 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)/04-S-1594

Foreword

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

DSS intends the results and analysis herein 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 targeting is accomplished, and where it originates.

Our goal for this publication is to provide the community 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 continued reporting of suspicious contact reports to DSS field offices. Prompt reporting of foreign collection activity is critical to an effective industrial security program.

William A. Curtis
Acting Director, Defense Security Service

I. Introduction

The Defense Security Service (DSS) Counterintelligence (CI) Office has produced the 8th annual trends document as a tool for security professionals. The trend and analytical assessments in this publication are based entirely on reports of suspicious foreign activity communicated 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 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 personnel and DSS personnel recognize and report suspicious foreign activity. In addition, DSS aims to improve this document each year from comments and suggestions that are received by the community. Noteworthy changes this year include the Technology Matrix, which was created to provide a detailed snapshot of each technology and the Appendix, which provides indicators and countermeasures complementing the top methods of operation.

Through research presented in this document, DSS enables cleared contractors to enact responsive, threat appropriate, and cost-effective Security Countermeasures (SCM). Furthermore, government agencies are encouraged to use this reported information to evaluate their own threat environments.

II. Executive Summary

A. Reporting Trends

This report is based on an analysis of 1095 suspicious contact reports received in 2003 from cleared contractors, DSS Industrial Security Representatives, and Special Agents. This represents an almost 34 percent increase from 2002 reporting. Targeting is on the rise primarily because the Internet and E-mail provide a fast, efficient, and free method for communication and collection for foreign entities while providing them with relative anonymity. DSS also continues to see a sharp rise in the number of foreign nations targeting and utilizing a wide variety of methods in collection efforts. The global war on terrorism and the operations in Iraq and Afghanistan have reinforced a heightened sense of awareness among DSS field personnel and cleared defense contractors.

B. Country Trends

In 2003, DSS identified 85 countries associated with suspicious activities, one greater than the number of countries reported in 2002, suggesting that the number of countries may have leveled off but not the suspicious targeting. This does not imply the same 85 countries targeted last year. A few countries that targeted in 2002 were not involved in reports of targeting in 2003. Furthermore, in 2003, the top ten collecting countries accounted for 59 percent (57 percent in 2002) of all suspicious activity, while the top five represented 37 percent (40 percent in 2002) of all suspicious activity.

C. Technology Interests Trends

In 2003, as reported in previous years, the majority of targeted technologies, as well as those associated with Department of Defense programs and weapons systems, were covered by International Traffic of Arms Regulations (ITAR). Foreign entities continue to target weapon components, developing technology, and technical information more aggressively than complete weapons systems and military equipment. Additionally, suspicious activity in 2003 included the targeting of all 18 militarily-critical technology categories.

D. Most Frequently Reported Technology Targets

Technologies generating the most foreign interest in 2003 (by frequency of targeting):

- Information Systems – 22%
- Sensors & Lasers – 17%
- Aeronautics Systems – 10%
- Electronics – 9%
- Armaments & Energetic Materials – 9%
- Chemical & Biological Systems – 5%
- Space Systems – 5%
- Marine Systems – 4%
- Materials – 4%
- Guidance Navigation & Vehicle Control – 4%

The ranking of technologies targeted changed only slightly from 2002 with Aeronautics Systems and Chemical & Biological Systems moving up the list of targeted technologies and Power Systems and Manufacturing and Fabrication dropping out of the top ten.

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

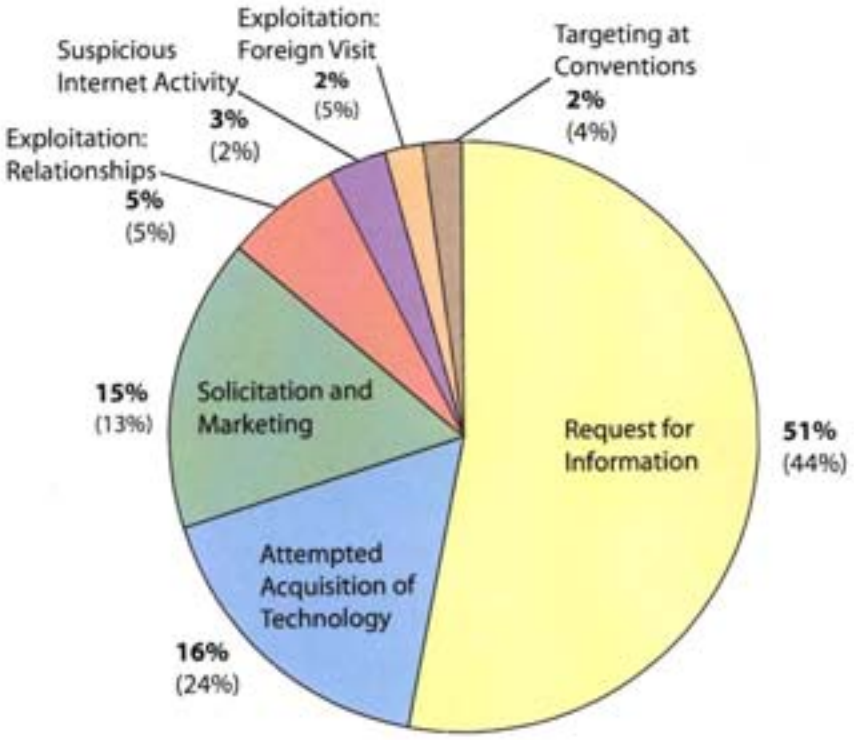
MOs are the techniques utilized by foreign entities in an attempt to collect intelligence, scientific and technical information. The top MOs associated with attempted collection efforts in 2003 (by frequency of targeting):

- Request for Information (RFI) – 51%
- Attempted Acquisition of Technology – 16%
- Solicitation and Marketing Services – 15%
- Exploitation of Relationships – 5%
- Suspicious Internet Activity – 3%
- Exploitation of Foreign Visits – 2%
- Targeting at Conventions, Seminars, and Exhibits – 2%

Although foreign entities may use a combination of methodologies, as a particular situation demands, these top MOs have remained consistent to those identified in previous years. The percentage of RFIs comprised half of all methods used during 2003. The top three MOs were used in 81 percent of all foreign collection attempts reported to DSS.

Graph 1

Methods of Operation by Foreign Entities in 2003



Note: Percentages in parentheses indicate 2002 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.

III. World Collection Trends

Table 1

Country Trends 1997-2003

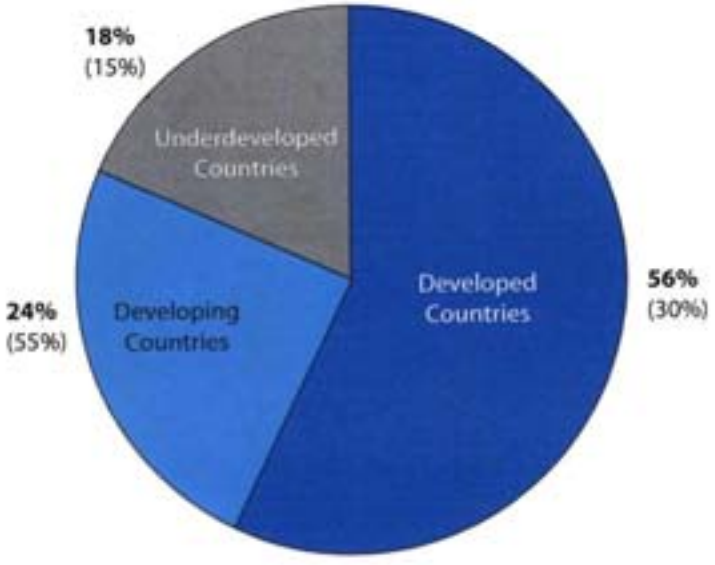
Year	1997	1998	1999	2000	2001	2002	2003
Number of Countries with Identified Collection Involvement	37	47	56	63	75	84	85

A. Country Trends: Industrial Base Strength

These 85 countries represent every region of the world and every social and political environment. In 2002, the trend showed a sharp increase in targeting by developing nations. However, in 2003 and in 2001, the majority of countries targeting cleared contractors were countries with economies and technology industries that were competitive with the United States with varying degrees of military capabilities. Developed countries continue to target complete weapons systems as well as components to fill gaps in undeveloped technology.

Graph 2

Targeting Based on Foreign Industrial Base 2003



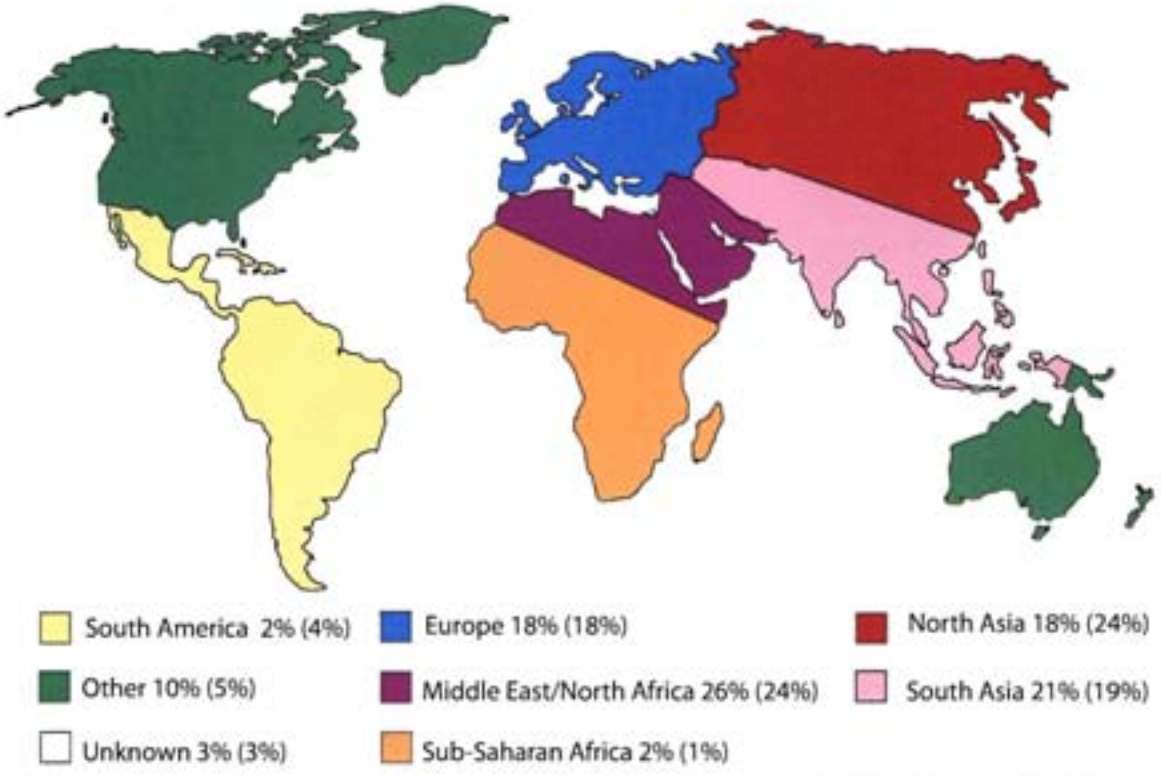
Note: Numbers in parentheses indicate 2002 data.

B. Worldwide Breakdown by Region

The regions in the graphic below are organized to account for political, religious, and social similarities between countries in those parts of the world. The Middle East/North Africa and South Asia areas both showed increases in targeting during 2003. Collection within the North Asia region showed a moderate decline, falling from 24 percent of total collection in 2002 to 18 percent total collection in 2003. This does not imply that all countries within this category reduced targeting—rather that targeting in this region decreased relative to other geographic areas.

Figure 1

Regional Breakdown of Foreign Collection in 2003



The map above reflects the regions where collection efforts originated but 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 associated percentages indicate the level of collection reported in 2003 (2002).

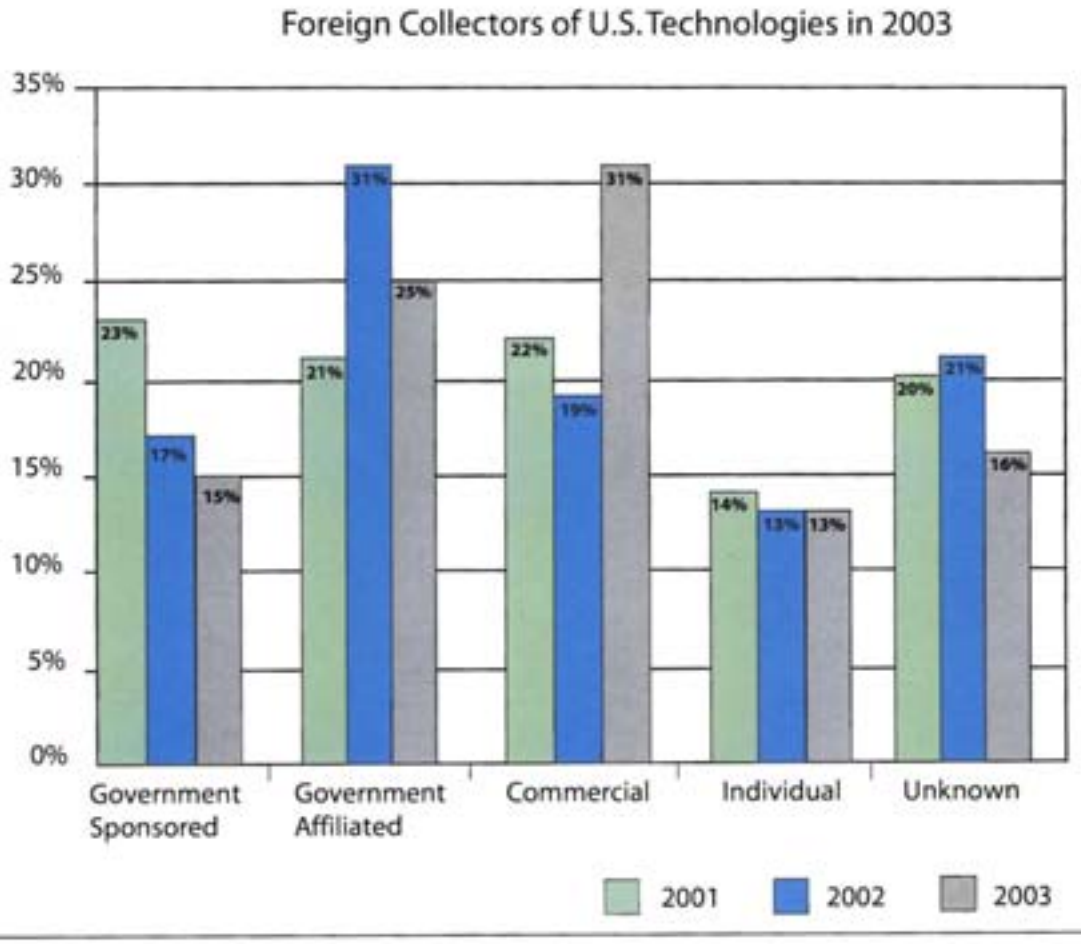
C. Foreign Collectors

DSS identifies types of collectors after evaluating reported information, conducting extensive research, and assessing relationships and representatives in each incident. Foreign government sponsored targeting, which includes Ministry of Defense, Intelligence Officers (including foreign military attachés), and other official government entities accounted for 15 percent of all reported cases in 2003. This represented a 2 percent decrease from 2002 for "traditional" (direct foreign government) targeting. To supplement the three consecutive years of decline in traditional

targeting, foreign nations have relied more heavily on non-traditional collectors (government affiliated and commercial collectors) which accounted for at least 56 percent of all collection in 2003. Foreign government-affiliated collection includes research institutes, laboratories, government-funded universities, and contractors representing governments. (Note: Foreign companies whose work is exclusively or predominantly in support of government agencies are also included as government-affiliates.) Foreign Commercial activities are those companies engaged in business, in the commercial and defense sectors, whose suspicious activity is not identified with a foreign government. Foreign Commercial collection increased significantly from 19 percent in 2002 to 31 percent in 2003. There is a distinct possibility that some of these foreign companies may be servicing government contracts; however, DSS has not seen enough evidence to fully support this claim.

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 was identified as seeking personal financial gain.

Graph 3



IV. Technology Section

DSS documents and reviews foreign interests in critical U.S. defense technology in 18 categories. These Military Critical Technology List (MCTL) technologies are the primary blueprint used by DSS to define categories and subcategories for each technology. The MCTL is a detailed and structured compendium of emerging technologies the Department of Defense (DoD) assess to be critical to maintaining superior U.S. military capabilities.

Table 2

Technology Matrix

Technology	Total Targeting (%)	Foreign Government Targeting (%)	Number of Countries	Top Regions	High Priority Targets Within Category
Information Systems	22% (25%)	32%	63 (47)	South Asia (25%) Middle East/North Africa (17%) Europe (14%)	Algorithms for Various Technologies GIS Technology KA-Band Systems & Power Amplifiers Signal Processing/Time Frequency Data Solid-State Power Amplifiers SX-6 Supercomputer Various Cryptography Technology Various Secure Communication System Various Software Applications/Programs Voice Control Systems
Sensors & Lasers	17% (17%)	43%	46 (40)	South Asia (26%) Middle East/North Africa (20%) North Asia (16%)	Antennas (Coaxial, Fractal Array) High Performance Infrared Systems Laser Frequency Stabilization Technology Mobile Ground Radar Night Vision Technology (Gen3) Solar Thermal System Subsurface Environmental Sensors Thermal Infrared Weapons Systems
Aeronautics	10% (9%)	35%	35 (36)	South Asia (45%) Middle East/North Africa (37%) North Asia (25%)	Automatic Test Simulation Equipment Blade Failure Diagnosis System Blisk Technology Gas Turbine Technology Helicopter Engines Pulse Denotation Rocket Engines Smart Aircraft Control Actuator
Electronics	9% (12%)	24%	32 (37)	North Asia (26%) South Asia (23%) Middle East/North Africa (18%)	Circuit Designs Diplexer Filters Electronic Surveillance Module Load Cell Interface Microwave Engineering Technology Power Magnets Pulse Expander & Compressor Smart Munitions

(Numbers in parentheses indicate 2002 values.)

Table 2

Technology Matrix *(Continued)*

Technology	Total Targeting (%)	Foreign Government Targeting (%)	Number of Countries	Top Regions	High Priority Targets Within Category
Armaments & Energetic Materials	9% (9%)	30%	44 (26)	Europe (42%) South Asia (27%)	Expolsive & Blast Ignition Technology Solid Rocket Propellant Data Supercaviation System Various missile systems
Chemicals & Biological Systems	5% (2%)	29%	40 (23)	Middle East/North Africa (41%) Europe (23%) South Asia (20%)	BioPak Breathing Equipment Bio-testing Kits Environmental Control Systems Microorganism Detection Device
Space Systems	5% (3%)	25%	19 (22)	North Asia (26%) South Asia (23%) Europe (18%)	Cryogenics Power Systems - Electric and Solar Rocket Propulsion and Propellants Space-based Internet Protocol System Spacecraft Navigation and Control (Gyroscopes, Attitude Control Software)
Marine Systems	4% (6%)	40%	34 (24)	Middle East/North Africa (26%) South Asia (23%) North Asia (19%)	Closed Systems Breathing Apparatus Sonobuoys Torpedoes Undersea Acoustic Modeling Undersea Robotics
Materials	4% (2%)	37%	28 (15)	Middle East/North Africa (78%)	Advanced Crystal Technology Aluminum-Silicate Oxide Black Paint (Black Velvet) Cermanic Composites Depleted Uranium Natural Gas Cylinder Technology Polymides/Copolymers Rare Earth Metal Silicone Carbon
Guidance, Navigation & Vehicle Control	4% (4%)	20%	25 (15)	Europe (31%) South Asia (20%) North Asia (19%)	Global Positioning Systems Inertial Navigation Systems Missile Guidance Transponders UAV Autopilot and Flight Control

(Numbers in parentheses indicate 2002 values.)

A. Information Systems

Overview: Targeting directed against information systems technologies decreased by three percent in 2003 relative to other technologies. However, this category continues to be the most frequently targeted. Software systems accounted for almost 50 percent of the suspicious activity within information systems. Of these, roughly one-third were foreign offers to supply software to cleared contractors. The concern in these cases is of malicious code being embedded in the software package. Forty percent of the software requests were associated with military-related systems. In addition, targeting directed against high-performance computing tripled from 2002. The SX-6 supercomputer was an example of this type of targeting in 2003. This technology is a high-speed, high-bandwidth vector supercomputer product with multiple defense applications in addition to industrial, academic, and other government uses.

SX-6 Supercomputer

Table 3

Collection Incidents for Information Systems Subcategory 1997-2003

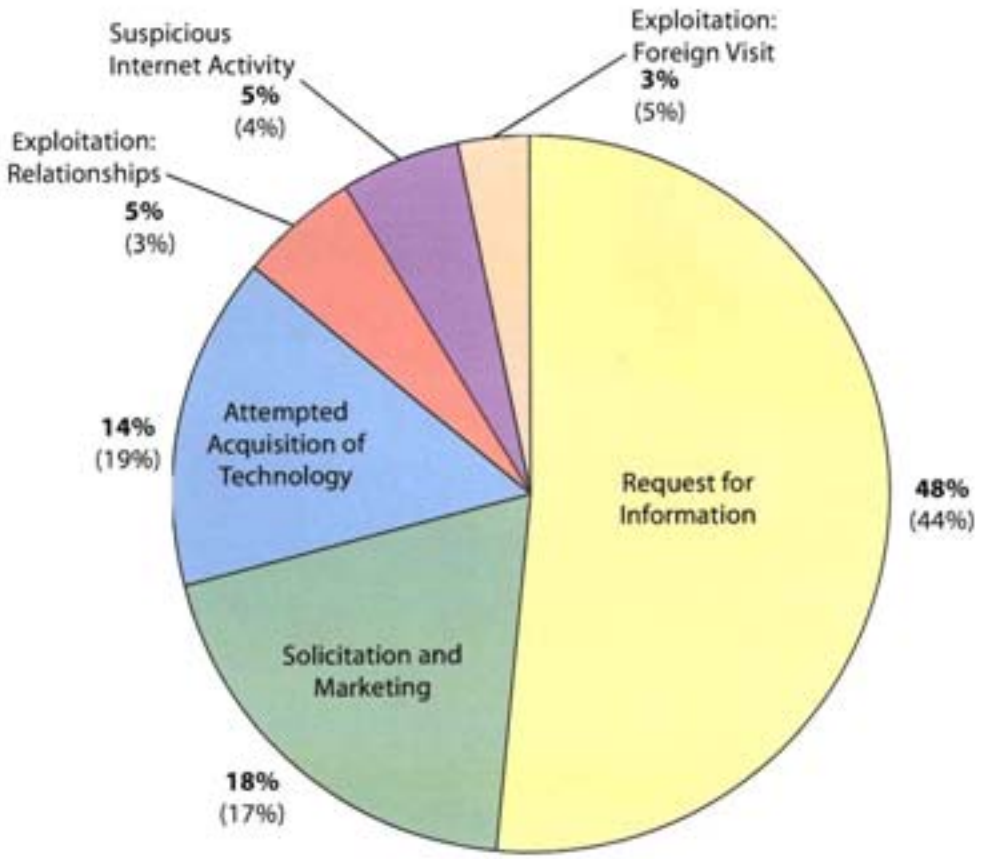
Information Systems	1997	1998	1999	2000	2001	2002	2003
Command, Control, Communications, Computing, Intelligence (C4I)	6	5	5	8	24	12	7
Cumputer Aided Design, (CAD); Computer Aided Manufacturing (CAM)	1	1	2	4	2	2	2
High-Performance Computing	2	5	0	3	3	3	9
Human Systems Interface	0	0	0	0	0	4	4
Information Security	13	6	2	21	16	7	7
Intelligent Systems	4	3	0	11	5	28	6
Modeling and Simulation	5	6	6	12	17	11	3
Network Switching	4	1	0	1	10	28	12
Signal Processing	0	1	3	9	20	21	19
Software Systems	10	15	13	33	27	8	29
Transmission Systems	5	6	4	29	1	4	0

Information Systems Collection Example

Get your free Software…
A European software company contacted a cleared DoD contractor asking if the cleared contractor was interested in beta testing an e-mail encryption software package for free. The foreign company was established in a U.S.-friendly country; however, after careful analysis of company personnel, it was determined that the company was being run from an adversarial country. The names of the company's officers were also associated with other foreign entities that had close associations with elements of the adversarial government's national security apparatus. The cleared company declined the free software offer.

Graph 4

Methods of Operation: Information Systems



B. Sensor and Laser Technology

Overview: Sensors and lasers remained the second most targeted technology category matching collection efforts in 2002 of 17 percent. Foreign collection emphasis focused on sensor platforms placed on UAVs. The number of countries focused on sensor and laser technology increased from 40 to 46. The majority of the entities were associated with North- and South-Asian countries, which together accounted for 42 percent of all reporting. Middle East and North African entities represented another 20 percent of all targeting. The majority of entities were seeking sensors and lasers that would guide weapons to specific targets with pinpoint accuracy. One of the most frequently targeted sensors was the Pan-tilt Zoom Camera, which has a laser rangefinder that provides precise distance measuring capability.

Table 4

Collection Incidents for Sensors & Lasers Subcategory 1997-2003

Sensors and Lasers	1997	1998	1999	2000	2001	2002	2003
Acoustic Sensors	4	18	2	5	41	46	45
Air and Terrestrial Platforms	N/A	N/A	N/A	N/A	3	12	7
Marine Active Sonar	N/A	N/A	N/A	N/A	10	5	11
Marine Passive Sonar	N/A	N/A	N/A	N/A	17	17	4
Marine Platform	N/A	N/A	N/A	N/A	11	5	23
Other Acoustic Sensors	N/A	N/A	N/A	N/A	0	7	0
Electro-Optical Sensors	3	13	3	9	25	2	9
Focal Plane Array/Infrared	8	11	5	5	7	11	10
Radars	5	8	22	9	20	5	3
Imagery	5	13	8	3	12	0	9
Lasers	0	0	4	8	24	4	10
Other	2	10	5	14	21	0	0

Note: Acoustic sensors were not subcategorized prior to 2001.

Night-vision devices and related technologies also experienced an increase in targeting in 2003. Several foreign e-mails seeking to purchase Generation III night-vision devices were sent directly to cleared contractors. These units' light intensification in the 30K to 50K range and their intensification tubes are said to last much longer, provide better viewing clarity, sensitivity, and detection distances. Design and construction is streamlined, making for a much less bulky device.

Generation III Night Vision Device

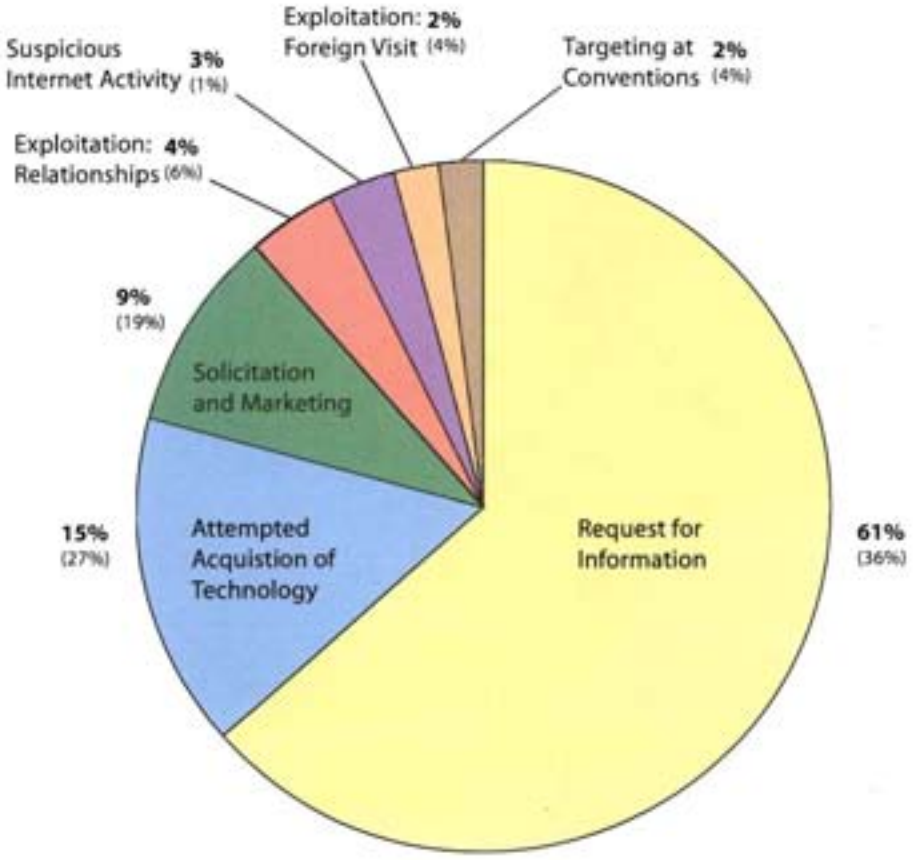
Sensors and Lasers Collection Example

A Middle Eastern company contacted a cleared DoD contractor stating they had a need for a large number of small Pan-Tilt Zoom Cameras. The individual requested information regarding the size, weight, and stabilization characteristics of the camera. He then asked if his company could borrow one of the cameras in order to run tests on it prior to placing their order. He stated he needed all the information within 30 days.

Pan-Tilt Zoom Camera

Graph 5

Methods of Operation: Sensors and Lasers



C. Aeronautics Systems

Overview: Targeting directed against aeronautics-related technologies increased for the first time in three years. Aeronautic systems were the third most frequently targeted technology, representing 10 percent of all 2003 targeting. The most dynamic change occurred with the increased collection of UAV technology. UAVs were a significant element of the U.S. efforts in Afghanistan during Operation Enduring Freedom and in Iraq during Operation Iraqi Freedom. Long viewed as a useful asset for collecting various types of intelligence, these aerial vehicles proved that their worth extended far beyond mere surveillance.

Both Predator and Global Hawk UAVs provided constant imagery to combatant commanders and, in some cases, they actually became combatants. Predator UAVs are capable of carrying Hellfire missiles over the battlefield. If a fleeting target of opportunity emerges, the UAV can be directed to fire its missiles before the target can escape.

South Asian countries led the targeting effort against aeronautics technologies accounting for 45 percent of all reported incidents followed by Middle East/North African Entities (37 percent) and North Asian Entities (25 percent). Almost 50 percent of the targeting involving UAVs was executed by South Asian entities.

Table 5

Collection Incidents for Aeronautics Systems Subcategory 1997-2003

Aeronautics	1997	1998	1999	2000	2001	2002	2003
Aircraft, fixed wing	10	5	6	11	46	13	6
Gas turbine engines	8	5	7	3	7	12	12
Human (crew systems) interfact	1	5	0	1	0	1	3
Helicopters	3	1	1	4	9	3	4
Unmanned aerial vehicles	4	4	1	4	21	18	36

Aeronautics Systems Collection Example

A cleared DoD contractor was contacted by an individual from a foreign country company who stated that he was interested in establishing a joint venture on UAVs. The individual used a miltary rank in his e-mail and stated that his government was interested in making a large purchase. Subsequent e-mail contact suggested the urgent nature of the business and indicated the necessary funding had been approved but the foreign entity needed the technical details of the UAV for their government's purchasing officer in order to tender a bid. A review of DSS records indicated that this country had a history of targeting UAV technology. Additional research revealed that the foreign individual may have had past intelligence connections.

Predator UAV

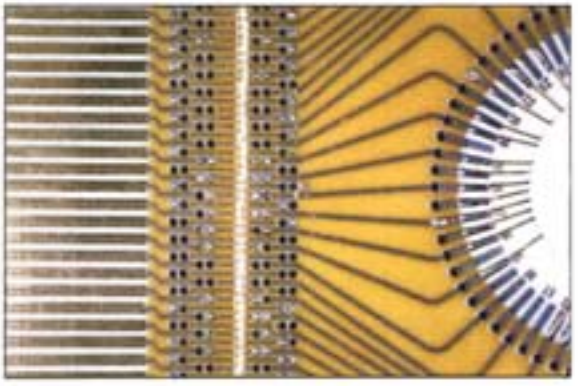
Graph 6

Methods of Operation: Aeronautics Systems

D. Electronics

Overview: In 2003, foreign targeting directed against electronics technology decreased, from 12 to 9 percent relative to other technologies, making it the fourth most popular technology category. The majority of targeting concentrated on electronic components. In one example, a company operating in an embargoed country requested large number of bipolar transistors and transistor chips. The requester wanted the export-controlled chips for use in high-powered radars.

North Asian countries lead the targeting effort for electronics technology, accounting for 26 percent, followed closely by South Asian countries which accounted for 23 percent, and Middle East/North



African countries which represented 18 percent. Countries that possessed modern production facilities were associated with the majority of targeting. What these foreign entities lacked were advanced components to complete their production efforts.

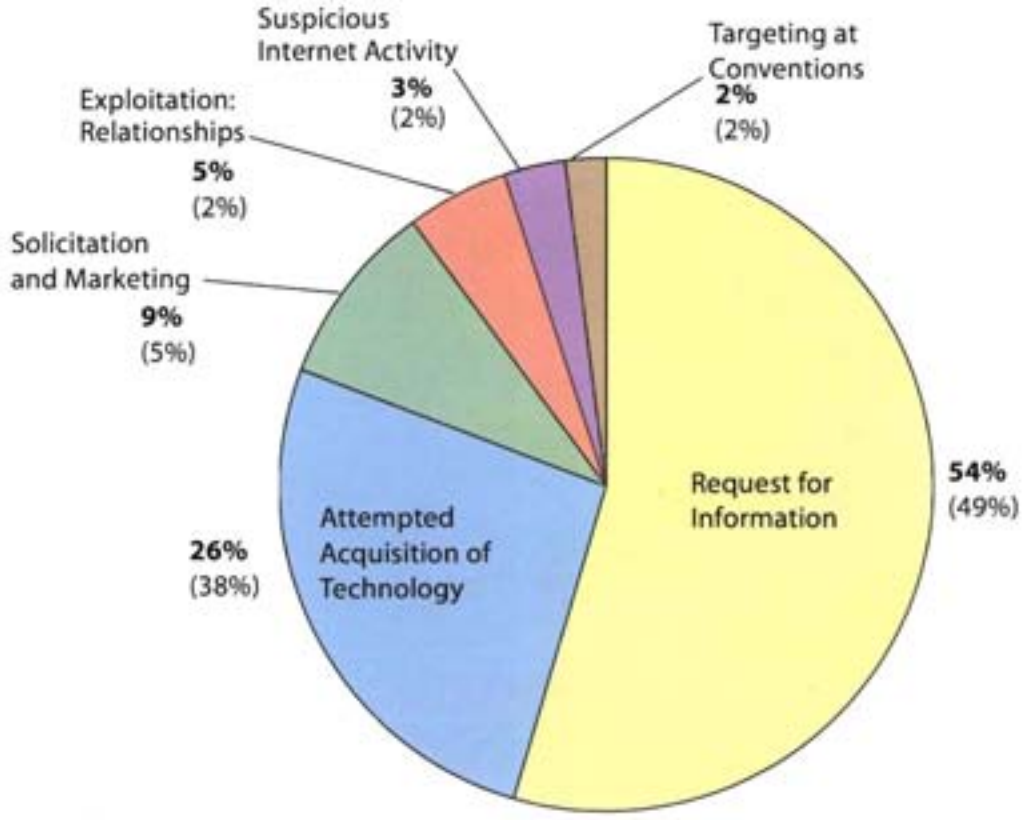
Table 6

Collection Incidents for Electronics Subcategory 1997-2003

Electronics	1997	1998	1999	2000	2001	2002	2003
Materials/components	4	6	12	1	17	50	73
Fabricated materials	2	3	1	0	5	31	3
Microelectronics	5	2	4	7	1	1	8
Optoelectronics	4	1	1	1	2	2	2

Graph 7

Methods of Operation: Electronics



E. Armaments and Energetic Materials

Overview: Targeting against armaments and energetic materials remained at nine percent in 2003. However, targeting directed against the sub-category energetic material increased. Under energetic material, propellant technology was the most frequently targeted.

Several incidents involved foreign entities requesting information on supercavitation from cleared DoD contractors. Supercavitation research is being applied to torpedoes. Using "supercavitation" techniques, the torpedo becomes an underwater missile, capable of reaching its target before the threat can respond. In this approach, the water near the tip of the projectile—or torpedo—literally vaporizes at high speeds, producing a "pocket" in which the weapon can "fly" underwater. Traveling through this vapor pocket dramatically reduces drag, allowing the projectile to reach extremely high velocity for a given input power. Such a weapon would be well-suited for close-range submarine encounters. With multipurpose configurations, it could be used not only for antisubmarine warfare, but also as an antitorpedo weapon, or for defense against high-speed surface craft.

MK-48 Torpedo

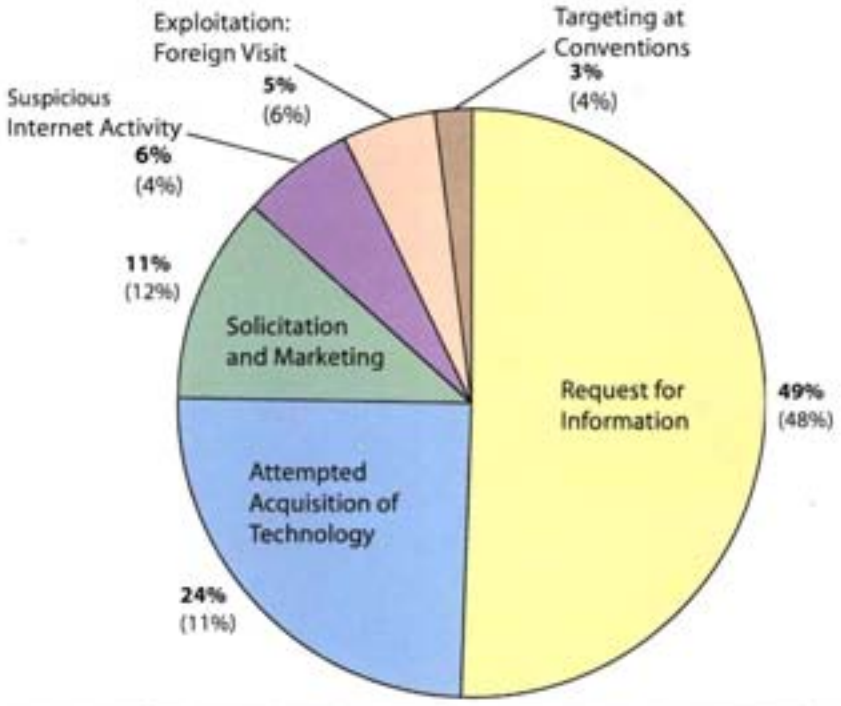
European nations led the targeting effort in 2003 accounting for over 42 percent of all incidents followed by South Asian countries which accounted for 27 percent.

Table 7

Collection Incidents for Armaments and Energetic Materials Subcategory 1997-2003

Armaments and Energetic Materials	1997	1998	1999	2000	2001	2002	2003
General A&EM targeting	0	0	0	0	28	71	42
Ammunition, small/medium caliber	0	0	0	0	4	1	2
Bombs, warheads, large caliber projectiles	5	8	4	16	24	4	0
Energetic material	0	1	1	1	32	1	13
Safing arming, fusing, firing	1	1	0	5	9	9	7
Gun and artillery systems	1	4	4	1	9	3	1
Mines, countermines, and demolition systems	1	1	0	1	2	3	2

Graph 8 Methods of Operation: Armaments and Energetic Materials

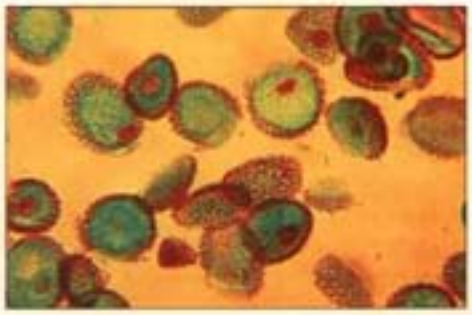


F. Chemical and Biological Systems

Overview: Targeting in 2003 directed against chemical and biological technologies increased to five percent of all targeting. In addition, the number of countries associated with the targeting increased from 23 to 40, with over 41 percent originating from Middle East or North African nations. Several suspicious requests involved foreign efforts to obtain technology capable of detecting biological and chemical agents, as well as requests for general biological and chemical warfare data. It's important to note that no specific requests for biological or chemical material were made to a cleared DoD facility. However, Middle East countries, that have been associated

Chemical and Biological Collection Example

A Middle Eastern scientist who works in the Department of Biology, College of Science at a Middle Eastern university contacted a cleared DoD contractor concerning studies on "Neural Reactions from Chemical and Biological Warfare Agents". The scientist requested reprints of the cleared employees' research. The country is currently embargoed and cannot receive this information.



with developing biological/chemical warfare programs, have made requests for research results on biological and chemical agents.

Graph 9 Methods of Operation: Chemical and Biological Systems

G. Space Systems

Overview: Collection attempts of space-based technology rebounded slightly this year by one percentage point to 5 percent of all targeting. Of the 19 known countries targeting this category, almost half (48 percent) were from Asia. This trend could be attributed to the region's interest in cultivating space based programs and satellite development combined with the need to play catch-up with other nations that have a greater amount of expertise in this technology.

This year saw a significant change in the methods used to target space technologies. In 2002, 26 percent of collection was through attempted acquisition of technology as compared to 12 percent in 2003. While the number of collection attempts through technology acquisition were down, requests for information saw a marked increase from 47 to 62 percent between 2002 and 2003.

Table 8

Space Systems: Targeting Dual Use

Technology	Requester's Stated Use	Possible Use
Space Control Software	Training and Simulation	Spacecraft Control
Power Unit	None given	Satellite or Missile production
High Performance Fiber-Optic Gyro	Automotive Applications	Satellite guidance

Graph 10

Methods of Operation: Space Systems

H. Marine Systems

Targeting associated with marine technology stayed relatively constant from last year at roughly four percent. The number of countries associated with targeting Marine systems increased from 24 in 2002 to 34 in 2003, with Foreign Government targeting accounting for 40 percent of all suspicious incidents. The majority of collection attempts were reported from entities in the Middle East and Asia. The most significant attempts to collect involved undersea technologies such as remotely-operated vehicles, undersea robotics, and supercavitation.

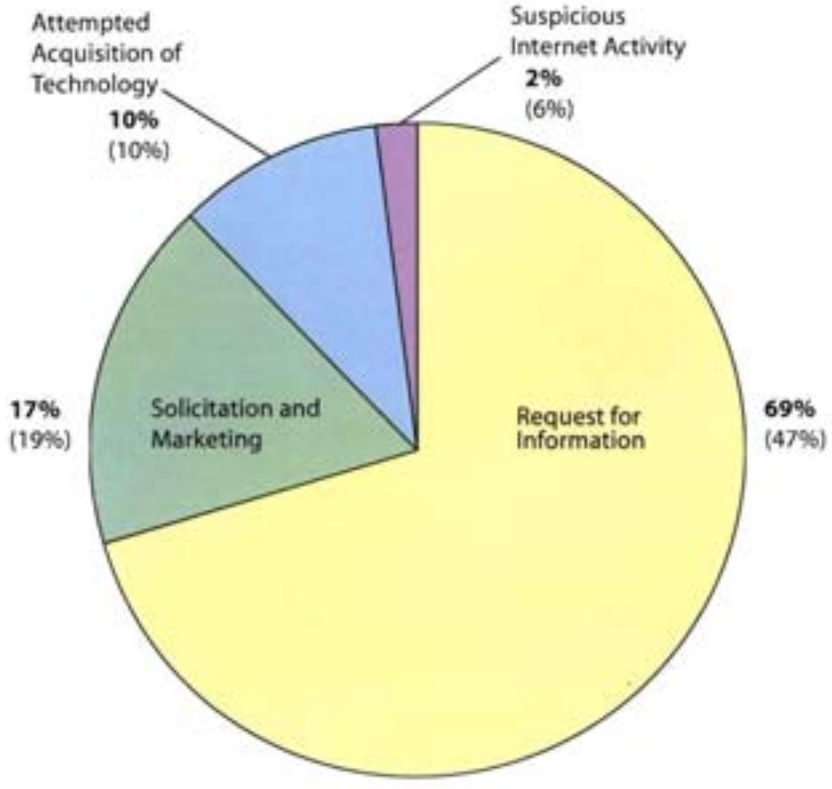
Table 9

Collection Incidents for Marine Systems and Subcategory 1997-2003

Marine Systems	1997	1998	1999	2000	2001	2002	2003
Propulsors and Propulsion system	3	1	0	1	0	3	1
Signature control and survivability	1	2	2	5	1	1	1
Subsurface and deep submergence vehicles	2	0	2	3	1	2	1

Graph 11

Methods of Operation: Marine Systems

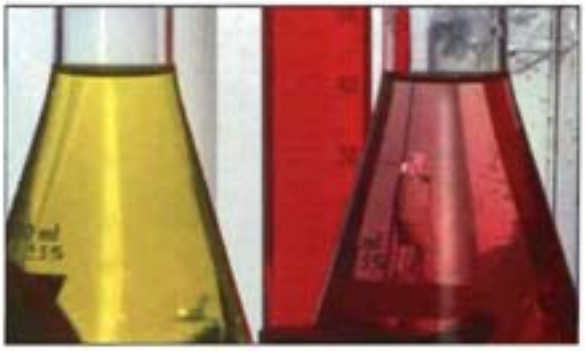


Marine Systems Collection Example

In 2003, there were three suspicious requests for information pertaining to undersea remotely-operated vehicles and undersea robotics. A much cheaper and versatile alternative to manned devices, these technologies are a desirable target.

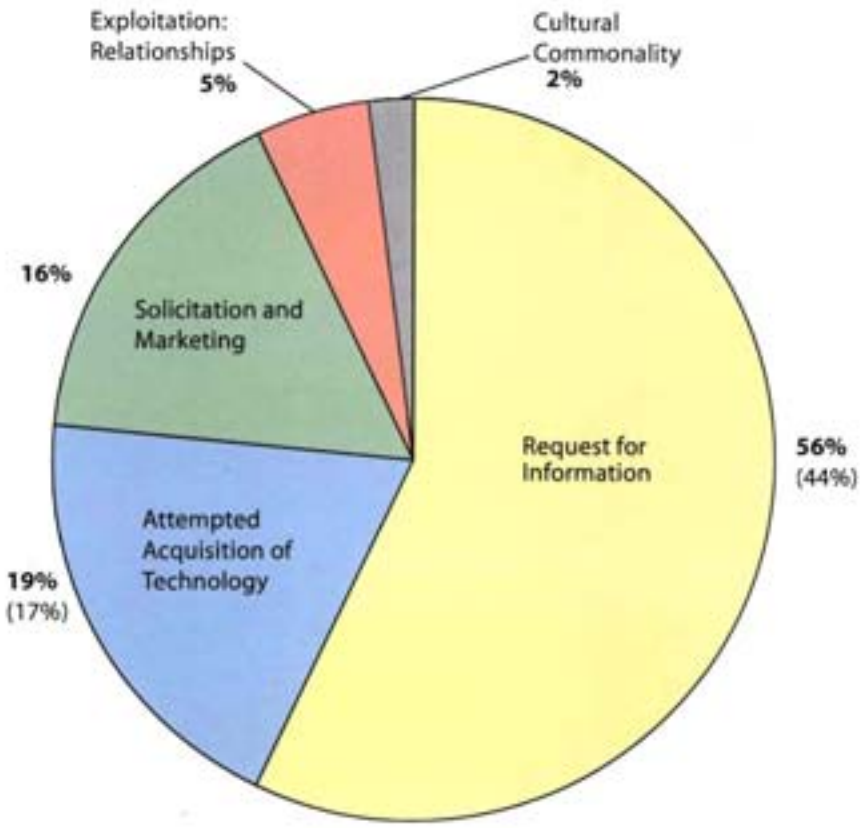
I. Materials

Overview: Targeting directed against material technology increased from two to four percent in 2003. The number of countries interested in material technologies also increased from 15 in 2002 to 28 in 2003. Seventy-eight percent of the countries targeting material technologies were from the Middle East/North African regions. While all industrialized and many developing nations have significant materials capabilities, there are still a host of countries that lack certain production capabilities. Many classes of materials intrinsically have both military and commercial applications. Structural materials are used in a broad range of military applications. An example is ceramics used in body armor and vehicle armor protection. The U.S. also has a strong ceramic matrix composite capability that was frequently targeted in 2003. Several incidents involved cleared DoD contractors being contacted by foreign entities requesting ceramic component technologies including sylramic ceramic composites, nicolon fibers, and silicon carbide fibers.



Graph 12

Methods of Operation: Materials



J. Guidance, Navigation, and Vehicle Control Systems

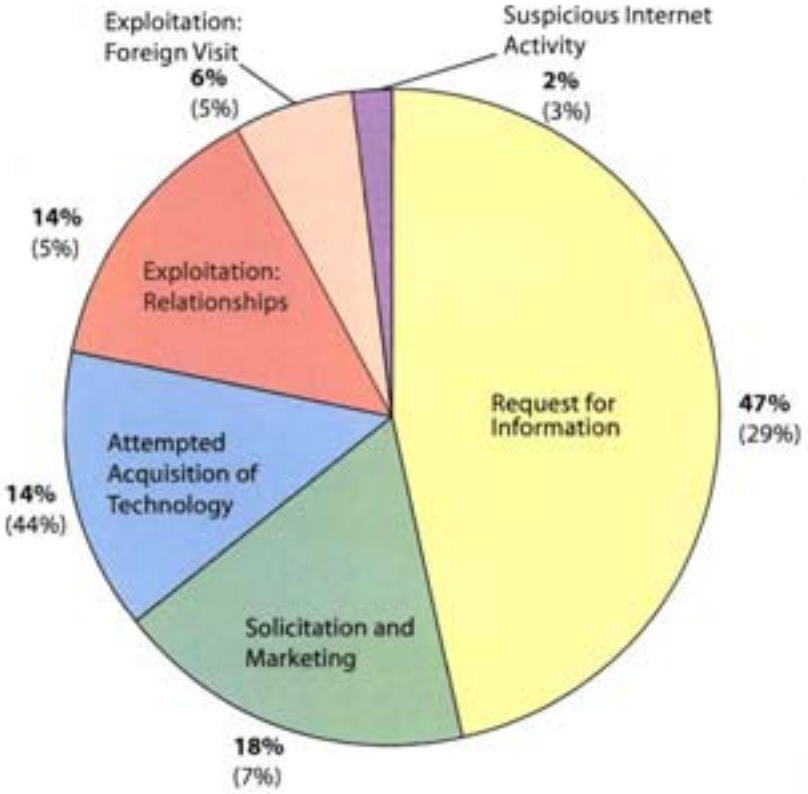
Overview: Targeting of guidance, navigation, and vehicle control systems remained steady during 2003. There was no major increase or decrease in the percentage of reports concerning GN&VC systems. However, the number of countries targeting this technology increased from 15 countries in 2002 to 25 countries in 2003. The majority of collection attempts came from European countries, with 10 countries from this region accounting for 31 percent of reporting. Europe had twice as many countries targeting this technology than any other region. The majority of these attempts involved a clever request for information by first demonstrating a basic familiarity with the technology and then soliciting the contractor to fill in the gaps. These collection attempts could be a means to collect information that would fill technology gaps. Cleared defense industry should be warned that these types of solicitations can be very dangerous as they often appear to be legitimate but can evolve into a very clever elicitation.

Guidance, Navigation, and Vehicle Control Systems Collection Example

Elicitation to Fill a Technology Gap...
A cleared defense contractor received an e-mail from a person identifying himself as an electronic warfare technician and asked about the LANTIRN POD — "I have an idea but I don't know if it's good. Is it possible to have information about the meaning used to switch the wavelength and if it's possible (unclassified) to have block diagrams or some other documentation for this. Thanks alot for your answer."

Graph 13

Methods of Operation: Guidance, Navigation, and Vehicle Control



V. Future Trends Assessment

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

As mentioned in the World Collection Trends section, the bulk of targeting has shifted back toward developed nations with over half of all attempted collection originating in advanced nations. In some cases, developing nations may be utilizing developed countries as a base for their targeting operations and vice versa; however, the evidence does not fully substantiate this claim. It is clear that many of the top countries associated with targeting are now considered among the most developed nations. Although the number of developing countries has increased, the percentage of targeting from developed nations will dominate collection.

With regard to actual targets, information systems and sensors and lasers technologies are firmly established as the two most frequently targeted categories. Of note, chemical and biological systems fell from the top 10 list in 2002, only to return from the 12th to the 6th most frequently targeted technology. 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 is seen in DSS data after an off year in 2002. Cleared facilities handling biological and chemical systems should continue to maintain high security-levels in light of significant global interest.

The increase in targeting of aeronautics systems is primarily due to heavy interest in the UAV. The greatest advertisement for any DoD weapons system is its successful employment in combat. During Operation Enduring Freedom in Afghanistan and Iraqi Freedom, UAV systems proved they could perform multifaceted roles over the battlefield. As a result, collection directed against UAV technology doubled in 2003, a trend that is expected to continue through 2004. Similarly, targeting can be expected to increase on sensor platforms associated with the UAVs.

Another significant trend that is expected to increase is that of targeting by foreign commercial entities. A large number of these companies have close ties to their governments who will ultimately benefit from the advanced technologies. Another concern is foreign commercial companies proliferating DoD technologies to potential U.S. adversaries. Even if a country or entity does not have any nefarious plans, they may not have the means nor the desire to protect the technology from other interested entities or countries.

Consequently an associated trend expected to decline is the targeting by official government entities. One possible explanation for this is that governments have decreased their reliance on Intelligence Officers (IOs) who have been trained in traditional methods of intelligence collection in favor of nontraditional collectors such as scientists at state-sponsored institutes or engineers at commercial entities. This latter group, in most cases, possesses more technical expertise than IOs and knows what types and parts of technologies need to be targeted.

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 request for information (RFI) and attempted acquisition are two MOs that will continue to be the most popular. The increase in RFI again in 2003 to half of all targeting methods is likely to round out at this number. The significant decline in Attempted Acquisition is surprising; however, this could suggest more precise targeting by foreign entities following well-placed RFI inquiries. Foreign entities are able to save significant time and money by acquiring technologies which cuts out

costs associated with research and development. It makes sense to fully determine what technology is needed via RFIs and then focus resources on acquisition of that specific technology. Another possible explanation is that the line distinguishing requests for information and attempted acquisition will continue to blur, moving closer together than in previous years. There may already be indications of this trend due to the fact that the percentage of attempted acquisition decreased by eight percent and the number of RFIs increased by five percent, relative to the other technologies.

Although it was noted last year, it is important to point out that advertising and information provided by defense contractors through their websites and in other formats are the starting point for foreign entities attempting to learn about and acquire defense technology. The cleared contractor will likely be the most lucrative target, and DSS concludes that reports of suspicious activity will continue to increase in 2004—despite active security countermeasures taken by these companies and security professionals.

VI. Appendix: MO Definitions, Indicators, and Countermeasures

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.

RFI	
Indicators	**Countermeasures**
• Technology is ITAR-controlled. • The CDC does not normally conduct business with the foreign requestor. • The request originates from an embargoed country. • The request is unsolicited or unwarranted. • Requestor 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 requestor is fishing for information. • Requestor represents unidentified third party. • The requestor is located in a country with a targeting history directed at the U.S. cleared defense industry. • The requester appears to be "skirting controls." • Several similar requests are made over time.	• Incorporate security into web design and advertising. • Initiate an active monitoring solution of website. • Report request to FSO and report to DSS CI (in several situations, similar requests may have been received by different U.S. cleared facilities). • Ask who requestor represents and why the requestor wants the information.

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.

Attempted Acquisition of U.S. Technology	
Indicators	**Countermeasures**
• Foreign competitors seek a position in the U.S. company that affords access to technology. • Statement 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 mail to non-U.S. addresses.	• Have a technology control plan. • Request a threat assessment from DSS or the program office whose work the contractor performs. • Scrutinize employees hired at the behest of foreign entity.

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 fellowships at cleared universities or attempting to gain employment at companies that are involved in cutting-edge technologies.

Solicitation and Marketing of Services	
Indicators	**Countermeasures**
• Offer to provide offshore software support on defense-related projects. • Invitation to cultural exchange, individual-to-individual exchange or ambassador program. • Offer to act as sales or purchasing agent in foreign country. • Foreign "scientist" seeks employment associated with sensitive defense technologies. • Foreign government- and business-sponsored internships.	• Report suspicious activities to FSO and DSS. • Report names of foreign scientists and engineers whose solicitation concerns classified or controlled research technologies. • Obtain recommendations and assess risks posed by software support in a foreign land. • Receive State Department travel briefings before departing on an exchange or ambassador program.

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 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 requests access to facilities or discusses information outside the scope of approved activities.

Exploitation: Foreign Visit	
Indicators	**Countermeasures**
• Foreign Liaison Officer or embassy official attempts to conceal official identities during a supposedly commercial visit. • Hidden agendas as 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 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 response. • Visitor claims business interest but lacks experience researching and developing this technology. (Remember: Discussion of export-controlled technology also requires an export license.)	• Brief country threat to all employees involved with the foreign visit. Request intelligence country threat assessments. • 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. • Develop or improve a Technology Control Plan incorporating above recommendations. • 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 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 at Exhibits, Conventions, and Seminars	
Indicators	**Countermeasures**
• Topics at seminars and conventions deal with classified or controlled technologies and/or applications. • Country or organization sponsoring seminar or conference has tried unsuccessfully to visit the facility. • Receive invitation to brief or lecture in a foreign country with all expenses paid. • Requests for presentation summary 6-12 months before seminar. • Photography and filming appear suspicious. • Attendees wear false name tags. • Casual conversation and discussions during and after events that appears aimed at future contact/relations.	• Have a technology control plan for any items and proprietary information brought overseas. • Be aware of follow-up requests after a show. • 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.

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 products 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.

Exploitation: Relationships	
Indicators	**Countermeasures**
• Resident foreign representatives — Fax documents to an embassy or another country in a foreign language — Want to access the local area network (LAN) — Want unrestricted access to the facility — Single out company personnel to elicit • Enticing U.S. contractors to provide large amounts of technical data as part of the bidding process, only to have the contract canceled. • Potential technology-sharing agreements during the joint venture are one-sided. • Foreign organization sends more foreign representatives than is necessary for the project. • New employees hired from the foreign parent company or its foreign partners ask to access classified or export-controlled data.	• Have technology control plan or very detailed Standard Practice Procedure. • Review all documents being faxed or mailed and have someone to translate. • 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. 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 foreign intelligence service (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 accounts for the majority of 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 that 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.

Exploitation of Internet	
Indicators	**Countermeasures**
• Computer probes are most likely searching for potential weaknesses in systems. • Network attacks originated from foreign Internet service providers. • Attacks last over a period of a day. • Several hundred attempts to access are made using multiple passwords.	• Have 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 security alert status.