TARGETING U.S. TECHNOLOGIES:

"A TREND ANALYSIS OF REPORTING FROM DEFENSE INDUSTRY"

2008

DEFENSE SECURITY SERVICE

TABLE OF CONTENTS

In the interests of readability and ease of comprehension, the editors have deferred the conventional stylistic use of repeated acronyms in favor of a full exposition of terms as they are first used within each specific section.

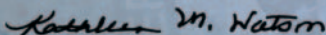# TABLES AND FIGURES

TABLES

FIGURES

PREFACE

Targeting U.S. Technologies:
A Trend Analysis of Reporting from Defense Industry

The Defense Security Service (DSS) is chartered to work in partnership with defense industry to protect critical technologies and information. An essential component of that effort is a requirement for defense contractors, who have access to classified material or "Cleared Defense Contractors," to identify and report suspicious contacts and potential collection attempts, as outlined in the National Industrial Security Program Operating Manual (NISPOM). DSS publishes this annual report based on an analysis of those Suspicious Contact Reports (SCRs) that DSS considers indicative of efforts by entities to target defense-related information and personnel.

This publication is intended to assist security officials, cleared defense contractors, intelligence professionals, and Department of Defense policymakers and decision makers assess the technology collection threat and implement appropriate security countermeasures. Based on analysis of SCRs received from defense industry, this publication identifies the most frequently targeted U.S. technologies, reflects the most common collection methods utilized, identifies entities attempting the collection, and identifies the regions where these collection efforts originate.

DSS encourages all Facility Security Officers to use information in this report to supplement security awareness and education programs at their facilities. In addition to increasing threat awareness within the industrial base, the additional SCRs generated by robust training efforts further contribute to the integrity of this annual analytical product. Timely submission of SCRs to DSS field offices is critical to an effective Industrial Security Program.

This document would not be possible without the strong support of Facility Security Officers within the U.S. cleared defense industry. DSS thanks the employees of the U.S. cleared defense industry for their continued support of the NISPOM and their contributions to this annual publication.

KATHLEEN M. WATSON
Director
Defense Security Service

EXECUTIVE SUMMARY

A. Key Findings

In response to Department of Defense (DoD) guidance, DSS publishes this report to detail and analyze possible foreign targeting of information and technologies developed or maintained within the Cleared Defense Contractor (CDC) community. The principal substance of this report is drawn from DSS analysis of suspicious contacts with foreign entities as reported by the CDC community during fiscal years 2006 and 2007 (FY06-FY07). The following constitutes key findings based on DSS analysis of data received from the defense industry during FY06-FY07:

- The number of reports DSS receives from CDCs detailing foreign contacts evaluated as "suspicious" continues to grow exponentially. This is likely attributable in part to the explosive growth of the Internet and the ever-increasing opportunity it affords for uninhibited and unfiltered global contact, but it is also likely indicative of hostile entities' increased exploitation of the Internet to target critical defense technologies. Enhanced CDC threat awareness is also partially responsible for increased recognition and reporting of suspicious incidents.

- Contacts originating from the East Asia and the Pacific region constitute, by far, the greatest number of suspicious contacts attributable to a specific region of origin. The nature and disproportionate extent of these contacts suggest a concerted effort to exploit contact for competitive, economic, and military advantage.

- DSS identified a shift in the affiliation of the entities making suspicious contacts. In most region-specific analyses, the majority of contacts originated from commercial entities vice those affiliated with governmental entities. This is likely a purposeful attempt to make the contacts seem more innocuous by using non-governmental entities as surrogate collectors for interested government or government affiliated entities. It also likely reflects the growing and increasingly interconnected global economy.

- Exploitation of cyberspace as a vehicle for surreptitious access to information resident on CDC data systems is a growing concern, and it constitutes a significant portion of contacts that DSS deems "suspicious." The ability to field effective security countermeasures to oppose this persistent threat and to mitigate the ability of hostile elements to control the information battlefield requires constant diligence.

B. Regional Collection Trends

According to the U.S. State Department, there are 200 independent countries in the world. In FY06-FY07, entities within over half of these countries attempted, at least once, to acquire U.S. defense technologies or information in a suspicious manner. DSS organized these

attempts into the State Department's six regional groupings (See Reference Map for information about the countries within the State Department's regional bureaus). For FY06-FY07, the six regions DSS most frequently affiliated with Suspicious Contact Reports were in descending order of occurrence:

REGIONS

- East Asia and the Pacific
- Near East
- Europe and Eurasia
- South and Central Asia
- Western Hemisphere
- Africa
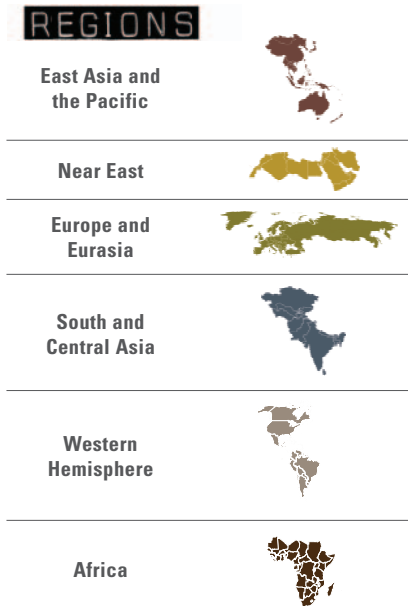
Also, five percent of traditional collection attempts were from entities of unknown origin. It is noteworthy that the regions affiliated with the suspicious requests may not always be the ultimate end user of the targeted technology. Collectors may use anonymous proxies or base their collection activity in another region to conceal their intentions or the identity of the ultimate end-user.

Reporting and analysis indicated "East Asia and the Pacific" as the region of the world most actively attempting to illegally acquire U.S. defense technologies. This region was responsible for 36 percent of traditional collection attempts in FY06-FY07 and is

historically the most active collector. This area had the largest portion of overall reporting with a slight increase from 30 percent to 36 percent from previous years. Although reporting from "East Asia and the Pacific" increased, reporting from the other regions either stayed constant or slightly decreased.

Once again, in FY06-FY07, the "Near East" region was the second most active area with 20 percent of the reporting, followed by "Europe and Eurasia" and "South and Central Asia" with 17 and 16 percent respectively. (Note: The minimal number suspicious contacts reports from the remaining two regions, Africa and the Western Hemisphere regions, did not justify inclusion in this year's report of most prolific collectors.)

Additionally throughout FY06-FY07, the most suspicious cyber entities had Internet Protocol (IP) addresses suggesting origination in the following regions, listed in descending order:

REGIONS

- East Asia and the Pacific
- Europe and Eurasia
- Unknown Region
- Near East
- South and Central Asia
- Western Hemisphere
- Africa

C. Cyber Trends

In recognition of an increasingly pervasive threat, this report includes a section specific to the use of cyberspace as a collection medium. Of the cyber incidents defense industry reported to DSS, the reports detailed entities targeting controlled unclassified information on unclassified industry networks; however, DSS is concerned that the lack of reporting detailing attacks against classified networks may lead to a false sense of security. The defense industry should continue to take precautions to secure both their classified and unclassified networks.

In FY06-FY07, DSS observed 52 percent of reportable incidents involving attempts to intrude or "hack" into the defense industrial base's computer systems or networks originated from East Asia and the Pacific Internet Protocol (IP) addresses. Despite having IP addresses specific to identifiable regions, DSS analysts categorize 96 percent of all affiliations within a collector's region as being of "Unknown" affiliation. These affiliations remain difficult to ascertain because of the nature of the IP addresses (e.g. governmental, academic, private, etc.), and because users likely mask or conceal their true identities through anonymous proxies. In FY06-FY07, cyber entities appeared most interested in targeting "Information Systems" technology, and their preferred method of operation was "Attempted Intrusion" with 61 percent of all reported cyber incidents falling into this category.

D. Collector Affiliations

DSS analyzes each SCR to determine the collector's affiliation and ascertain which foreign entity is targeting U.S. technology. For example, a SCR classified as "Government"

means the suspicious activity is affiliated with or acting on behalf of a foreign government or agency. Other collector affiliations include "Commercial," "Individual," and "Government Associated" entities. In FY06-FY07, DSS assessed "Commercial" entities as the top collectors of U.S. technology. This represented a five percent increase during fiscal years 2004 and 2005 (FY04-FY05), resulting in "Commercial" entities replacing "Government Associated" entities as the top collector entity affiliation category. This significant increase is likely the result of foreign entities seeking to privatize research and development in an effort to shift the focus from collection efforts emanating from or being associated with governmental entities.

E. Methods of Operations

Once DSS recognizes the region of origin and collector affiliation, it is important to understand how the suspicious entity attempts to collect the restricted information. From identification and analysis of Methods of Operation (MO), or modus operandi, DSS identifies the most prevalent collection techniques and indicators, and recommends countermeasures for the cleared defense industry to negate the MO's effectiveness.

In FY06-FY07, the top four collection MOs represented over 70 percent of all foreign collection attempts:

METHODS

Request for Information (RFI)	@
Attempted Acquisition of Controlled Technology	
Solicitation and Marketing of Services	☎
Suspicious Internet Activity	http//:www

TECHNOLOGIES

Information Systems	
Aeronautics	
Sensors	
Lasers and Optics	
Armaments and Energetic Materials	
Electronics	
Space Systems	
Marine Systems	
Positioning, Navigation, and Time Technology	
Materials and Processing Technology	

Sustaining the top position, "RFI" dropped 12 percent from FY04-FY05, while "Suspicious Internet Activity" increased by five percent. As in FY04-FY05, "RFI" and "Attempted Acquisition of Controlled Technology" continued to remain the top two MOs during this time period.

F. Targeted Technologies

DSS analyzes foreign interest in U.S. defense technology in terms of the 20 categories in the Developing Science and Technologies List (DSTL). Identification of which technologies suspicious elements are targeting for acquisition is a critical analytic objective. Understanding collection priorities allows the U.S. cleared defense industry to establish security countermeasures to help mitigate the loss of technology and classified information.

DSS analysis of FY06-FY07 SCRs indicated the following technologies, listed in order of foreign entity interest, represented probable collection priorities:

This listing is generally consistent with previous years' assessments. Suspicious entities in FY06-FY07 continued to target "Information Systems" technology most frequently, registering a five percent increase in the number of SCRs involving that technology. The remaining nine categories also showed small increases, demonstrating continued interest in these technologies, but DSS believes the increases in reporting are attributable in part to enhanced awareness and sensitivity of defense industry to report suspicious incidents involving these known targets of foreign interest.

BACKGROUND

Department of Defense (DoD) Instruction, 5200.39, dated July 16, 2008, requires DSS to publish a report detailing suspicious contacts occurring within the Cleared Defense Contractor (CDC) community indicative of a foreign threat to personnel, information, and technologies resident in the U.S. cleared defense industrial base. Per the instruction, DSS provides appropriate dissemination of these reports to the DoD Counterintelligence (CI) community, national entities, and the CDC community to assist in general threat awareness, to identify specific technologies at risk, and to aid in the application of appropriate threat countermeasures. DSS receives and analyzes Suspicious Contact Reports (SCRs) from CDCs in accordance with reporting requirements as defined in Chapter 1, Section 3, of the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, dated February 28, 2006. Based on an analysis of these SCRs, DSS prepared this report, "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry."

In a departure from previous annually produced studies covering a single fiscal year (FY), this report is based on data acquired over two fiscal years, FY2006 and FY2007. Accordingly, DSS did not prepare a report in 2007 specific to information based on FY2006 reporting. Future iterations of this report will revert to production on an annual basis.

This trends report covers information regarding the most prolific foreign entities by region targeting the CDC community during FY06-FY07 as compared to previous years. In this report, DSS used U.S. Department of State

regional bureaus to identify the countries that comprise the foreign regions. The report includes statistical and trends analysis on foreign regional affiliations, the traditional methods foreign entities in regional areas used to target the CDC community, and the specific technology sectors that they targeted. Each section also contains an analytical assessment forecasting potential future activities against the CDC community.

This trends report also provides specific information on cyber threats faced by the CDC community. Historically, DSS has included suspicious cyber activity as a subcategory within the regional collection trends; however, based on increased reporting of cyber attacks on the CDC community, DSS has determined a separate section is warranted to address this growing threat.

This report is published as part of DSS's ongoing effort to enhance awareness of foreign entities targeting the U.S. cleared industrial base and to encourage reporting of such incidents as they occur. It illuminates the entities' modus operandi to acquire information concerning specific technologies, identifies at-risk technologies, and projects estimates of foreign collectors' likely future activities. This report is also intended as a ready reference tool for the use of security professionals in their efforts to detect, deter, mitigate, or neutralize the effects of foreign targeting.

A. Scope/Methodology

This report is based primarily on suspicious contact reporting DSS collected from the CDC

community, but it also includes reference to all-source intelligence community reporting. While DSS analyzes all SCRs received from industry, only those that DSS determined to represent a potential CI concern form the basis of this report. DSS received a total of 4,897 reports from the CDC community in FY06-FY07. Through analytical processes and application of the DSS foreign intelligence threat assessment methodology, DSS determined 2,269 of these reports either posed a potential CI threat to the CDC community, or represented a link to elements DSS determined as hostile to U.S. interests.

In order to conduct accurate statistical analysis on FY06-FY07 data, DSS compiled FY04-FY05 data to create a comparable data set. All trends, statistics and analysis found in this report represent a comparison between the data sets encompassing these respective two-year time periods.

DSS analyzes foreign interest in U.S. defense technology in terms of the 20 categories in the Developing Science and Technologies List (DSTL). The DSTL is a compendium of science and technology capabilities being developed worldwide that have the potential to significantly enhance or degrade U.S. military capabilities in the future. The DSTL serves as a template for DSS to define categories and subcategories for each technology. Identification of said technologies is a critical analytic objective.

As noted, DSS categorizes and culls SCRs to determine if they have a CI nexus or pose a potential CI threat to the cleared defense community. DSS analysts scrutinize the SCRs examining the critical U.S. technology, the targeting entity, the methods of operation, the relationships to previous reporting from the

CDC community, and all-source Intelligence Community (IC) information.

B. Explanation of Estimative Language

DSS adopted the IC estimative language standard for use in the DSS "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry." The use of synonymous phraseology such as "we judge," "we assess," or "we estimate," as well as terms such as "likely," or "indicate," represents our efforts to convey an analytical assessment or judgment. These assessments, based on incomplete or at times fragmentary information, are not a fact, proof, nor do they represent empirically-based certainty or knowledge. Some analytical judgments are directly based on collected information; others rest on previous judgments, both of which serve as building blocks. In either type of judgment, we do not have "evidence" showing something to be a fact or that definitively links two items or issues.

Intelligence judgments pertaining to "likelihood" are intended to reflect the DSS's sense of the probability of a development, event, or trend. Assigning precise numerical ratings to such judgments would imply more rigor than we intend. The chart below provides a rough idea of the relationship of terms to each other.

Remote	Unlikely	Even Chance	Probably Likely	Almost Certainly
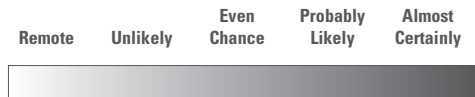
We do not intend the term "unlikely" to imply an event will not happen. We use "probably" and "likely" to indicate there is a greater than even chance. We use words such as "we cannot dismiss," "we cannot rule out," and "we cannot discount" to reflect unlikely — or even remote — events whose consequences are such that it warrants mentioning. Words such as "may" and "suggest" are used to reflect situations in which we are unable to assess the likelihood generally because relevant information is nonexistent, sketchy, or fragmented.

In addition to using words within a judgment to convey degrees of likelihood, we also ascribe "high," "moderate," or "low" confidence levels based on the scope and quality of information supporting our judgments.

CYBER
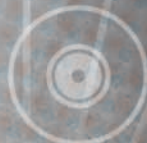
CYBER

1. Overview

DSS analysis of reports from defense industry indicates increased targeting of cleared industry unclassified computer networks. In FY06-FY07, the number of reports of Suspicious Cyber Activity (SCA) received from cleared industry significantly increased to 229 reports as compared to the 80 reports from FY04-FY05. Attempted computer intrusions and associated cyber-based activities represent an attractive, relatively low-risk option for many foreign entities seeking to further their Research and Development (R&D) programs and emulate U.S. technological advances. DSS refers identifiable computer network intrusion activity to law enforcement and operational counterintelligence agencies for further investigation.

2. Regions of Origin

FY06-FY07 cleared industry reporting indicates that entities in the East Asia and Pacific region were the most active collectors, accounting for 52 percent of all SCA reporting. Reporting indicates the likelihood that entities in this region are targeting the defense industrial base to further their own R&D programs as well as to improve their command, control, communications, and intelligence operations. The Europe and Eurasia region was the second most active collector, accounting for 21 percent of all SCA reporting. This percentage shows a slight increase over FY04-FY05 reporting which ranked collector entities from that region at 16 percent. Although DSS makes every attempt at attribution, for much of the SCA reporting the actual origin of the activity remains

undetermined or unknown. Such reports comprised the third largest category of SCA reporting. *Analyst Comments: It is likely this increase in reporting directly reflects both the Cleared Defense Contractors' (CDCs) increased cyber awareness and propensity to report, as well as traditional collectors' increased use of the cyber-based exploitation tactics. (Confidence Level: High)*

COUNTRIES OF ORIGIN

TABLE 1

Region	FY 2006-2007 Percent	FY 2004-2005 Percent
East Asia Pacific	52	57
Europe and Eurasia	21	16
Unknown	18	9
Near East	4	12
South and Central Asia	4	3

The chart above identifies the targeting entities' possible region of origin and is based solely on DSS analysis of SCRs. This chart does not necessarily represent regional-sponsorship for the cyber activity.

3. Collector Affiliations

DSS identifies SCA collectors after evaluating reported information, conducting research, and attempting to make correlations with historical collection attempts. When at all possible, DSS uses Internet Protocol (IP) as a baseline for determination of SCA reporting. When additional information is available, DSS analysts compare technical data such as file names and specific network intrusion methodologies to determine regional origin and organizational affiliation. Although so-called

AFFILIATIONS

FIGURE 1

Number of Cases
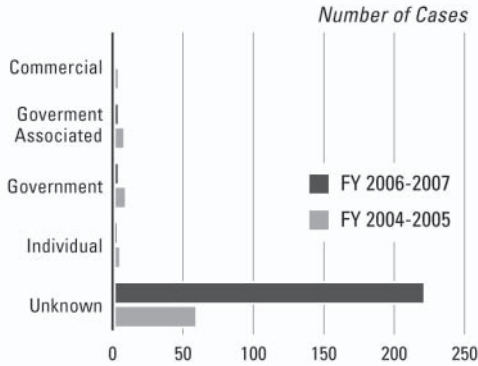
cyber "hacktivists," various transnational actors and a variety of entities unique to a particular geographic region, are behind some of these attempts, the nature of cyberspace makes it extremely difficult to attribute the collection attempts to specific government or commercial affiliations. For example, foreign entities can easily mask IP addresses, utilize freely available anonymous proxies, or launch attacks from any of the open WiFi hotspots across the globe. These resources, particularly with the increased availability of open anonymous proxies and the ease with which IP can be masked, complicate the security and counterintelligence community's ability to determine positive affiliation within a region of origin. In 96 percent of the events reported in FY06-FY07, DSS could not conclusively determine positive affiliation of the entity behind the SCA.

4. Method of Operations

Cyber collectors employed "Attempted Intrusions" as the most common Method of Operation (MO). In FY06-FY07, this MO characterized 61 percent of all Suspicious Contact Reports (SCRs). Many of these attempts to gain unauthorized access to CDC networks were through socially-engineered emails with malicious payloads, or software, to exploit popular commercial software programs. The second most prevalent MO was "Confirmed Intrusion" activity. In FY06-FY07, 24 percent of all cyber SCRs were confirmed penetrations of the CDC's unclassified network.

In FY06-FY07, the remaining 15 percent of cyber SCRs included potential pre-attack reconnaissance, "botnet" activity (a botnet is a general term to refer to a collection of compromised computers, called "zombie computers," running malicious software under a common command and control infrastructure), suspected denial-of-service attacks, and firewall logs.

METHODS OF OPERATION

FIGURE 2

FY 2006-2007
Percent
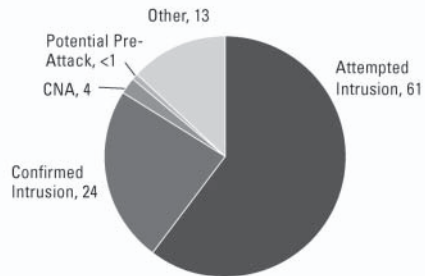
5. Targeted Technologies

FY06-FY07 industry reporting indicated foreign entities targeted all 20 technologies on the Developing Science and Technologies List. Cyber collectors most frequently sought "Information Systems" technology, accounting for over 40 percent of all cyber-related collection attempts. "Armaments and Energetic Materials" represented the second most targeted category of technology, accounting for nine percent of all SCA reporting. East Asia and Pacific regional collector entities were the most active collectors of this technology. "Aeronautics" technology was the third most targeted category of

TARGETED TECHNOLOGIES

TABLE 2

Developing Science and Technologies List (DSTL) Codes	FY 2006-2007		FY 2004-2005	
	Number of Cases	Percent	Number of Cases	Percent
Aeronautics	22	7	5	5
Armaments and Energetic Materials	26	9	8	8
Biological	6	2	1	1
Biomedical	2	1		
Chemical	4	1	1	1
Directed and Kinetic Energy	1	<1		
Energy Systems	1	<1		
Electronics	18	6	7	7
Ground Systems	1	<1		
Information Systems	131	43	23	24
Laser and Optics	19	6	5	5
Manufacturing and Fabrication	1	<1	2	2
Marine Systems	12	4	18	19
Materials and Processing	6	2		
Nuclear	3	1	2	2
Positioning, Navigation, and Time	2	1		
Sensors	15	5	9	9
Signature Control	1	<1	1	1
Space Systems	17	6	1	1
Weapons Effects	3	1		
Unknown	12	4	15	15

technology, accounting for seven percent of all SCA reporting.

6. Analytical Forecast

It is highly likely the amount of cyber targeting and attacks on unclassified networks will increase in the coming years. The availability of attack tools and the ease with which networks can be successfully exploited make cyber targeting an attractive MO for collectors with the technical ability to access and manipulate CDC's networks. It is likely that the number of network intrusion attempts will increase due to a growing awareness of the threat, propensity to report on the part of the CDC, as well as the development and fielding of enhanced detection methods. Furthermore, as the complexity of computer networks and the increased globalization of the defense industry increases, cyber targeting and collection will likely pose increasing challenges for defense industry to identify and counter. (Confidence Level: High)

EAST ASIA AND THE PACIFIC

EAST ASIA AND THE PACIFIC

1. Overview

As was the case in previous assessments, entities from the East Asia and the Pacific region retained their status in FY06-FY07 as the most prolific collectors of U.S. technology, far outstripping collection efforts emanating from the Near East region, the second most frequently noted collector. However, there was a significant change in the frequency of which kind of entity, within the region, originated the contact. In FY04-FY05, most Suspicious Contact Reports (SCRs) originated from "Government" entities located in the region. In FY06-FY07, however, "Commercial" entities dominated as the region's most active collectors. East Asia and the Pacific entities used "Attempted Acquisition of Controlled Technology" as the predominant Method of Operation (MO) to gain restricted information. Also during this reporting period, East Asia and Pacific entities focused their collection efforts on "Information Systems" technology, especially targeting various components of military "Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance" (C4ISR) applications.

2. Collector Affiliations

DSS analysis of the 696 SCRs associated with actors in the East Asia and Pacific region revealed that "Commercial" entities in the region surpassed "Government" affiliated collectors as the preeminent entities attempting acquisition of restricted, classified, and proprietary technology.

AFFILIATIONS

FIGURE 3
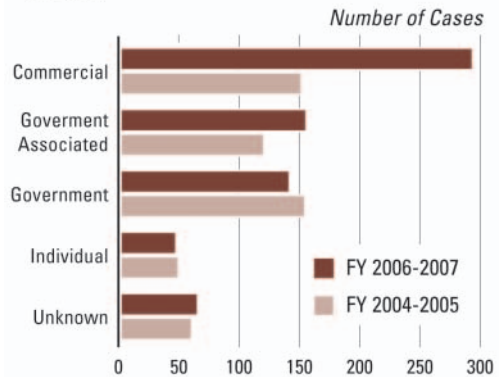
During FY06-FY07 "Commercial" collection within the East Asia and the Pacific region accounted for 42 percent of all SCR reporting. This category's significant increase over FY04-FY05 figures drove a concomitant change in the overall standings of collector affiliations, with "Commercial" affiliations replacing "Government" as the most commonly encountered collector-entity. In fact, the "Government" collector category, despite consistent collector reporting, fell from first to the third position in the hierarchy slightly behind "Government Affiliated" entities. "Commercial" collection attempts often mirrored "Government" collection efforts as an effective way for surrogate collectors to meet government collection requirements. The increase is also partially due to the rise of "Commercial" non-traditional collectors such as post-graduate and graduate students applying for positions in U.S. cleared industry. *Analyst Comment: We cannot*

rule out the increase of non-traditional collectors based on increased participation in the global marketplace, but the shift in collector affiliation is more likely due to governmental entities' successful use of legitimate and illicit front companies as surrogates to acquire controlled technologies. It is likely that commercial affiliations increased as third party countries, within the East Asia and Pacific region, used smaller commercial venues as surrogates to navigate around restrictive import / export procedures. (Confidence Level: Moderate)

3. Methods of Operation

In FY06-FY07, the top three East Asia and Pacific collection MOs remained unchanged from FY04-FY05, but the order of precedence changed. Cleared Defense Contractors (CDCs) reported the most frequent MO was "Attempted Acquisition of Controlled Technology," reflected in 35 percent of the SCRs. "Request for Information" (RFI) dropped to second at 28 percent of reporting, while "Solicitation and Marketing of Services" remained as the third most active method of choice. Also, a common

collection trend was to combine the MOs of "Attempted Acquisition of Technology" or "RFI" with "Exploitation of a Foreign Visit (CONUS)." For example, often a visiting delegation would request additional classified information during a visit to the CDC. *Analyst Comment: This moderate increase of attempted acquisition of controlled technology was likely attributable in part to the influx of engineers into CDCs as part of joint memorandums of agreement giving direct access to U.S. technology. It is likely these collectors are no longer just seeking information but are attempting to procure specific items for development in various military and civilian programs. (Confidence Level: High)*

4. Targeted Technologies

The East Asia and Pacific top five targeted technologies did not change significantly from FY04-FY05. Most of the technology categories remained the same or saw a slight increase in reporting; however, "Armaments and Energetic Materials" technology dropped from the second position to the fifth position. "Information Systems" technology retained its prominent

METHODS OF OPERATION

FIGURE 4

FY 2006-2007
Percent

- Other, 8
- Targeting at Convention, Exposition, Seminar; 6
- Exploitation of a Foreign Visit CONUS, 10
- Solicitation of Marketing Services, 13
- Attempted Acquisition of Controlled Technology, 35
- Request for Information, 28

FY 2004-2005
Percent

- Other, 7
- Exploitation of Relationships, 5
- Exploitation of a Foreign Visit CONUS, 8
- Solicitation of Marketing Services, 10
- Request for Information, 42
- Attempted Acquisition of Controlled Technology, 28

TARGETED TECHNOLOGIES

TABLE 3

Developing Science and Technologies List (DSTL) Codes	FY 2006-2007		FY 2004-2005	
	Number of Cases	Percent	Number of Cases	Percent
Aeronautics	91	11	53	9
Armaments and Energetic Materials	64	8	57	9
Biological	12	1	12	2
Biomedical	3	<1	2	<1
Chemical	10	1	17	3
Directed and Kinetic Energy	3	<1	3	<1
Energy Systems	7	1	14	2
Electronics	52	6	40	7
Ground Systems	11	1	5	<1
Information Systems	186	23	133	22
Laser and Optics	90	11	53	9
Manufacturing and Fabrication	24	3	9	1
Marine Systems	49	6	22	4
Materials and Processing	14	2	18	3
Nuclear	5	1	5	<1
Positioning, Navigation, and Time	38	5	16	3
Sensors	101	12	54	9
Signature Control	7	1	28	5
Space Systems	34	4	45	7
Weapons Effects	7	1	2	<1
Unknown	15	2	25	4

position as the most sought-after technology, consistent with the collection focus on C4ISR and military systems technologies. Each of the top five targeted technology areas represented ongoing "Commercial" and "Government" efforts to modernize and develop R&D programs. *Analyst Comment: This increase of information systems is likely attributable to collectors focusing on R&D shortcomings and desiring to modernize aging military and C4ISR capabilities. (Confidence Level: High)*

5. Analytical Forecast

Entities originating from East Asia and the Pacific region are highly likely to remain focused on acquiring advanced technologies to strengthen their indigenous R&D programs. With increased military systems technology collection efforts, government and government affiliated collectors are likely to apply pressure on commercial entities to continue and increase their collection efforts. Also, given the trade restrictions in the East Asia and the Pacific region, collection attempts are likely to be more subtle via third party commercial collectors as a means to skirt import / export restrictions. Commercial entities, through joint agreements and potential purchase of U.S. companies, are highly likely to engage in dual-use technology acquisition. Technology acquisitions will likely focus on areas of R&D shortcomings, especially C4ISR technology and its subset, Unmanned Aerial Vehicle (UAV) technology. As the region with the most active collectors, it will be critical for defense contractors to clearly identify technology end users to protect their products from reverse engineering and exploitation. Countering this prolific threat will require the highest degree of awareness and diligence within the U.S. cleared industry. (Confidence Level: High)

NEAR EAST

NEAR EAST

1. Overview

With 453 reports, entities originating from the Near East region remained the second most prolific collectors of U.S. technology in FY06-FY07. "Government Associated" and "Commercial" collectors continued to dominate industry reports, followed closely by "Government" collection attempts. Entities primarily sought technologies that involved "Information Systems;" however, regional collectors also focused on "Aeronautics" and "Sensors" technology. The preferred collection style, or Methods of Operation (MO), for this region was "Request for Information" (RFI) distantly followed by "Attempted Acquisition of Controlled Technology" and "Solicitation and Marketing of Services" in second and third place, respectively. The collectors in this region represented a vast spectrum, ranging from students and business entrepreneurs to full-fledged government operators.

2. Collector Affiliations

As noted, contacts originated from an array of collectors in the Near East region. As was the case in FY04-FY05 reporting, DSS assessed "Government Associated" entities as being the most frequently noted collectors, representing 34 percent of the reports. However, potentially the most significant change noted in FY06-FY07 reporting was the five percent increase in affiliations assessed as emanating from "Commercial" entities, placing that affiliation in a virtual tie with the formerly dominant "Government Associated"

AFFILIATIONS

FIGURE 5   Number of Cases

Categories: Commercial, Government Associated, Government, Individual, Unknown

Legend: FY 2006-2007, FY 2004-2005

Axis: 0, 50, 100, 150, 200
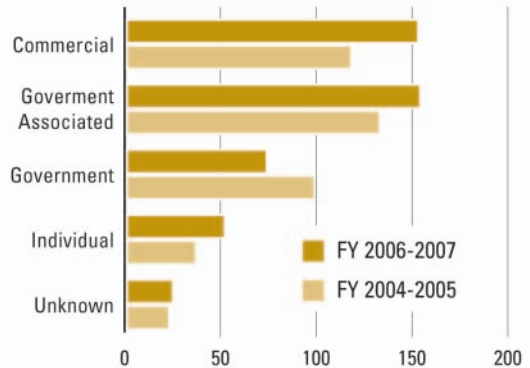
category of collectors. *Analyst Comment: The increase of commercial entities is likely due to collusion between commercial entities and government associated entities to ascertain leading-edge technology from the U.S. defense industry. It is highly likely commercial entities, such as universities, public agencies, and R&D centers, are affiliated with these government associated collectors. Consequently, it is also likely the government monitors all external communications through various government offices and such communications are transmitted only with official approval. (Confidence Level: Moderate)*

3. Methods of Operation

Collection entities in this region continue to favor "RFI" as the most common collection technique of choice due to its low-risk, high-gain properties. Collectors also

METHODS OF OPERATION

FIGURE 6

FY 2006-2007
Percent

Exploitation of Relationships, 6
Other, 6
Exploitation of a Foreign Visit CONUS, 7
Solicitation of Marketing Services, 10
Request for Information, 37
Attempted Acquisition of Controlled Technology, 34

FY 2004-2005
Percent

Exploitation of Relationships, 5
Other, 11
Exploitation of a Foreign Visit CONUS, 5
Solicitation of Marketing Services, 9
Request for Information, 41
Attempted Acquisition of Controlled Technology, 29

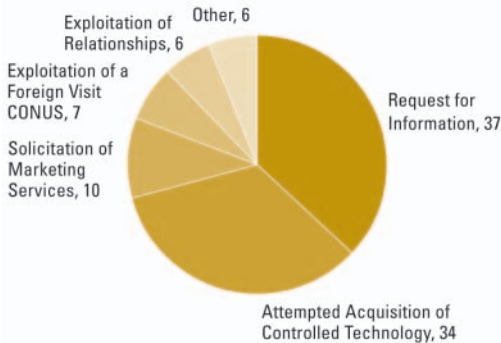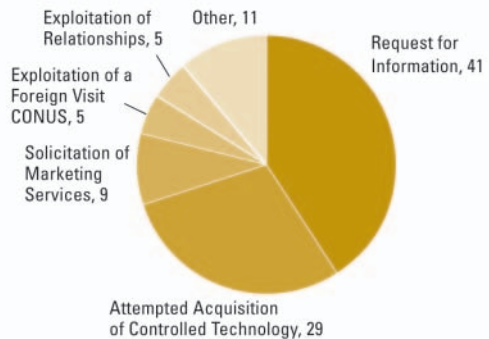continued to use "Attempted Acquisition of Controlled Technology" in their efforts to exploit U.S. cleared defense contractors (CDCs) for desirable information. While "RFI" continues to be a popular method, other collectors attempt to acquire or divert U.S. controlled technology via a neutral country. *Analyst Comment: It is highly likely Near East entities will continue to rely on non-traditional collectors and all available avenues of approach in their efforts to target U.S. technology. This direct targeting increases the number of targets of opportunity and is likely to increase the success rate for acquiring sensitive, classified, and export-controlled U.S. technology. (Confidence Level: High)*

4. Targeted Technologies

Near East entities continued to steadily target "Information Systems." An increased interest in "Aeronautics" and "Sensors" technology was also noticed with a particular focus on Unmanned Aerial Vehicles (UAVs)

and associated systems. Since FY04-FY05, the number of UAVs fielded in the Iraq war increased over five-fold, with a concomitant increase in interest from Near East entities. As UAV technology evolves with ever-increasing efficiency and effectiveness, the desire to obtain these emerging technologies will also increase, as well as their associated bundled-weapons platforms. The wars in Iraq and Afghanistan have also generated an increased focus on the acquisition of cutting edge technologies related to "Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance" (C4ISR) programs, especially as they relate to war-fighting capabilities. *Analyst Comment: As defense industry continues to make advances in the aeronautics field, it is highly likely that entities will pursue aggressive collection attempts in this area. Collectors are highly likely to target these aeronautical systems, especially UAVs, because UAVs have a substantial, continuing role in R&D. In addition, it is likely that media reports from the War on Terrorism*

TARGETED TECHNOLOGIES

TABLE 4

Developing Science and Technologies List (DSTL) Codes	FY 2006-2007		FY 2004-2005	
	Number of Cases	Percent	Number of Cases	Percent
Aeronautics	68	12	46	9
Armaments and Energetic Materials	50	9	40	8
Biological	12	2	18	3
Biomedical	6	1	4	1
Chemical	17	3	24	5
Directed and Kinetic Energy	4	1	5	1
Energy Systems	16	3	6	1
Electronics	30	5	52	10
Ground Systems	10	2	5	1
Information Systems	121	22	116	22
Laser and Optics	37	7	41	8
Manufacturing and Fabrication	28	5	14	3
Marine Systems	8	1	15	3
Materials and Processing	27	5	20	4
Nuclear	5	1	3	<1
Positioning, Navigation, and Time	18	3	12	2
Sensors	56	10	59	11
Signature Control	7	1	21	4
Space Systems	15	3	11	2
Weapons Effects	1	<1	1	<1
Unknown	10	2	13	2

highlight and increase focus on aeronautic system capabilities. Suspicious entities are also concerned with platform efficiency, extended flight duration, and R&D related C4ISR programs. (Confidence Level: High)

5. Analytical Forecast

Entities originating from the Near East region will likely continue to collect on U.S. products in order to develop their own force multipliers as well as to improve existing technology. It is highly likely they will continue to use email RFIs in their attempt to acquire sensitive U.S. technology. Furthermore, channeling such requests through other nations to avoid export regulations is also likely to continue as a targeting method. As this region becomes more volatile, it is highly likely entities will continue to focus their collection on government related technologies such as information systems and aeronautics technology, especially in the areas of C4ISR systems and UAVs respectively. (Confidence Level: High)

EUROPE AND EURASIA
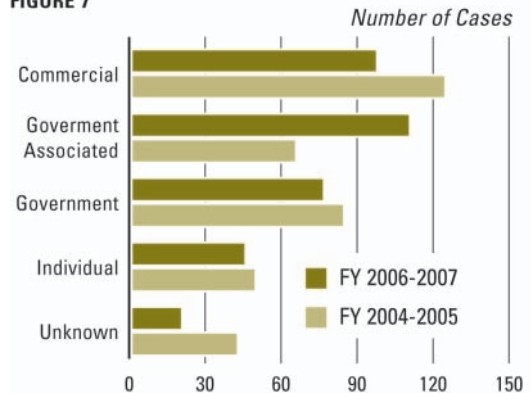
EUROPE AND EURASIA

1. Overview

In FY06-FY07, the Europe and Eurasia region ranked as the third most common originator of contacts assessed as being possible attempts to acquire sensitive information or restricted technology from Cleared Defense Contractors (CDCs). The 348 reported incidents in FY06-FY07 represented a nominal decrease over FY04-FY05 figures when DSS attributed 364 collection attempts to that region. Defense industry reporting indicated "Government Associated" and "Commercial" entities were responsible for the majority of the targeting efforts. These entities used "Request for Information" (RFI) as the predominant Method of Operation (MO) to procure restricted, classified, and proprietary technology. Furthermore, Europe and Eurasia actors focused their collection efforts on "Information Systems" technology, especially information communications sub-category.

2. Collector Affiliations

In FY06-FY07, defense industry reporting indicated "Government Associated" and "Commercial" collectors were responsible for the majority of the targeting efforts. These two affiliation categories were responsible for a combined total of 60 percent of all Europe and Eurasia collection efforts. *Analyst Comment: Although DSS noted overall increases from other regions in the use of commercial affiliations, the increase in the government associated category of collectors emanating*

AFFILIATIONS

FIGURE 7

Number of Cases

Commercial
Government Associated
Government
Individual
Unknown

FY 2006-2007
FY 2004-2005

0 30 60 90 120 150

from Europe and Eurasia is likely associated with government officials publicly elevating military development to a national task. (Confidence Level: Moderate)

3. Methods of Operation

In FY06-FY07, the top three MOs Europe and Eurasia collectors used accounted for nearly 80 percent of all reported incidents involving suspicious entities. The top three MOs for FY06-FY07 were "RFI," "Attempted Acquisition of Technology," and "Solicitation and Marketing of Services." Entities originating from Europe and Eurasia continued their use of "RFI" as a preferred collection MO, although it registered a decrease from 47 percent in FY04-FY05 to 36 percent in FY06-FY07. Conversely, "Attempted Acquisition

METHODS OF OPERATION

FIGURE 8

FY 2006-2007
Percent

Exploitation of Relationships, 4
Other, 9
Targeting at a Convention, Exposition, Seminar; 8
Solicitation of Marketing Services, 13
Request for Information, 36
Attempted Acquisition of Controlled Technology, 30

FY 2004-2005
Percent

Other, 8
Exploitation of Relationships, 6
Exploitation of a Foreign Visit CONUS, 9
Solicitation of Marketing Services, 12
Request for Information, 47
Attempted Acquisition of Controlled Technology, 18

of Controlled Technology" significantly increased to 30 percent while "Soliciting and Marketing of Services" nominally increased to 13 percent. *Analyst Comment: Europe and Eurasia actors are highly unlikely to change their collection techniques. The exponential growth of the Internet and use of email accounts have all but eliminated national boundaries, making RFI a virtually risk-free option. (Confidence Level: High)*

4. Targeted Technologies

Europe and Eurasia top five targeted technologies did not change significantly from FY04-FY05. Most of the categories remained the same, except for "Electronics Technology" which fell from fifth to sixth position in the hierarchy. "Information Systems" technology remained the most sought after technology with collection focused on the information communications sub-category. Interestingly, "Aeronautics Technology" saw a moderate increase, which is likely attributed with Europe

and Eurasia entities aggressively pursuing aircraft / aviation industry technology, specifically focusing on unmanned aerial vehicle technology and components.

TARGETED TECHNOLOGIES

TABLE 5

Developing Science and Technologies List (DSTL) Codes	FY 2006-2007		FY 2004-2005	
	Number of Cases	Percent	Number of Cases	Percent
Aeronautics	78	18	51	11
Armaments and Energetic Materials	37	8	55	12
Biological	11	3	13	3
Biomedical	2	<1	4	1
Chemical	10	2	14	3
Directed and Kinetic Energy	3	1	1	<1
Energy Systems	3	1	4	1
Electronics	21	5	45	9
Ground Systems	6	1	2	<1
Information Systems	98	22	80	17
Laser and Optics	46	10	32	7
Manufacturing and Fabrication	4	1	6	1
Marine Systems	16	4	15	3
Materials and Processing	9	2	15	3
Nuclear	3	1	3	1
Positioning, Navigation, and Time	19	4	15	3
Sensors	51	12	53	11
Signature Control	2	<1	22	5
Space Systems	13	3	16	3
Weapons Effects	1	<1	1	<1
Unknown	6	1	28	6

5. Analytical Forecast

Entities originating from Europe and Eurasia will likely remain focused on acquiring advanced technologies to strengthen their R&D programs. The desire to rejuvenate indigenous defense industries are likely to lead government associated and commercial entities to seek out business ventures with U.S. companies in an effort to acquire desirable western technologies. Additionally, Europe and Eurasia actors will continue to pursue dual-use technologies that have the potential to assist in the development of advanced weapon systems or improve upon Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) applications. (Confidence Level: Moderate)

SOUTH AND CENTRAL ASIA
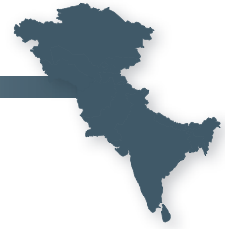
SOUTH AND CENTRAL ASIA

1. Overview

The South and Central Asia region remained the fourth most prolific region for technology collection in FY06-FY07. "Commercial" collectors continued to dominate industry reports, consistent with the trend in other regions. Collectors sought "Information Systems" technology most frequently, followed by "Lasers and Optics," "Sensor Systems," and "Aeronautics" technology. Industry reporting of the primary Methods of Operation (MOs) also mirrored the hierarchy noted in the other regions, with "Attempted Acquisition of Technology" in the top position followed by "Request for Information" (RFI) and "Solicitation and Marketing of Services."

2. Collector Affiliations

From the 348 reports validated by DSS as having met the suspicious contact threshold, the most dramatic trend was the significant rise in the number of contacts emanating from "Commercial" affiliated entities. These entities accounted for 52 percent of the reported contacts, a change from 39 percent in FY04-FY05. "Individual" contacts, not otherwise associated with "Commercial" or "Government" entities, also rose to 25 percent, nearly doubling the amount of reports from FY04-FY05 and accounting for a quarter of overall contacts in FY06-FY07. "Government" and "Government Associated" entities dropped to 10 percent and 11 percent respectively over the same time. "Government Associated" affiliations were three times less active than the

AFFILIATIONS

FIGURE 9

Number of Cases

FY 2006-2007
FY 2004-2005
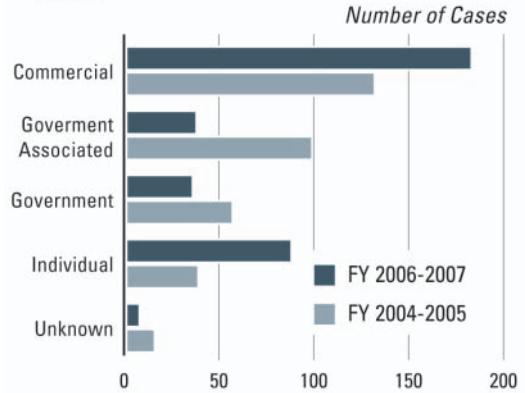
previous time period, a significant decrease from FY04-FY05. *Analyst Comment: The increase of commercial and corresponding drop in government and government associated contacts mirrors a trend that DSS observed for FY06-FY07. This trend is likely attributable to the shift in the global market economy for third world countries and increased international access to the Internet. This access allows smaller commercial entities to enter the international technology acquisition arena on a larger scale and finally join in specific modernization efforts. (Confidence Level: Moderate)*
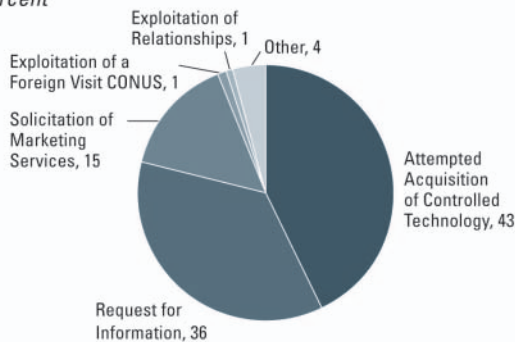
3. Methods of Operation

DSS analysis noted a parallel between the rising status of "Commercial" entities as the most active collector affiliations, and the concomitant emergence of the "Attempted
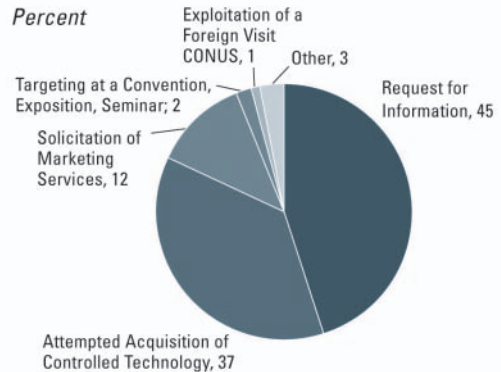
METHODS OF OPERATION

FIGURE 10

FY 2006-2007
Percent

Exploitation of Relationships, 1
Other, 4
Exploitation of a Foreign Visit CONUS, 1
Solicitation of Marketing Services, 15
Attempted Acquisition of Controlled Technology, 43
Request for Information, 36

FY 2004-2005
Percent

Exploitation of a Foreign Visit CONUS, 1
Other, 3
Targeting at a Convention, Exposition, Seminar; 2
Solicitation of Marketing Services, 12
Request for Information, 45
Attempted Acquisition of Controlled Technology, 37

Acquisition of Controlled Technology" technique as the most common MO of choice. While "Government Affiliated" collector entities most commonly employ "RFI" as a means to acquire information, "Commercial" collectors tend to prefer attempts designed to actually acquire the technology itself, purportedly to further their own business interests. As a result, in FY06-FY07, the rise of "Attempted Acquisition of Controlled Technologies" over the "RFI" method was a complete reversal of MOs from FY04-FY05. The third most prolific MO, "Solicitation and Marketing of Services" also rose slightly, but paled in comparison to the "Attempted Acquisition of Controlled Technology" MO. *Analyst Comment: The changes in MO that industry reported in FY06-FY07 reflect the difference between government entities seeking technology for R&D purposes and commercial entities seeking technologies for sales. As the commercial entities continue to fulfill local technology contracts, the push to acquire controlled technologies will likely grow more aggressive. (Confidence Level: Moderate)*

4. Targeted Technologies

Over the last four years, suspicious targeting emanating from South and Central Asia has remained relatively static with only nominal increases among the top four most sought-after technologies. Regional entities continued to seek "Information Systems" technologies, specifically "Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance" (C4ISR) systems as the premier type of technology, accounting for almost a quarter of all reports. "Lasers and Optics," specifically laser target designators and laser range finders, remained in second place; however, "Lasers and Optics" was only seven percent below "Information Systems" technologies. "Sensors" technology remained in third place and was focused on Improvised Explosive Device (IED), motion sensors, and intrusion detection sensors. "Aeronautics" technology remained in fourth place with a focus on Unmanned Arial Vehicles (UAVs) and associated systems. The increase in the top four technologies was a result of the

TARGETED TECHNOLOGIES

TABLE 6

Developing Science and Technologies List (DSTL) Codes	FY 2006-2007		FY 2004-2005	
	Number of Cases	Percent	Number of Cases	Percent
Aeronautics	49	12	40	10
Armaments and Energetic Materials	28	7	32	8
Biological	5	1	6	2
Biomedical	4	1	5	1
Chemical	3	1	14	4
Directed and Kinetic Energy	1	<1	4	1
Energy Systems	2	<1	5	1
Electronics	34	8	34	9
Ground Systems	10	2	6	2
Information Systems	84	21	67	17
Laser and Optics	59	14	48	12
Manufacturing and Fabrication	7	2	3	<1
Marine Systems	9	2	3	<1
Materials and Processing	14	3	22	6
Nuclear	3	1	1	<1
Positioning, Navigation, and Time	4	1	7	2
Sensors	55	14	41	10
Signature Control	5	1	31	8
Space Systems	30	7	23	6
Weapons Effects			1	<1
Unknown	1	<1	4	1

virtual elimination of "Chemical," "Materials and Processing," and "Signature Control" technology. *Analyst Comment: Entities from the South and Central Asia region continued their pursuit of economic and military modernization efforts to counter growing regional insurgencies. It is likely this targeting will drive these entities to seek state-of-the-art technologies (C4ISR, targeting, and detections systems) for their militaries and law enforcement organizations. (Confidence Level: Moderate)*

5. Analytical Forecast

The use of commercial collectors as the most frequently noted entities initiating contact is highly likely to continue as a trend into the next year. The entities using attempted acquisition of controlled technologies as their MO of choice will continue to grow as the regional commercial and military entities are exposed to new technologies as cooperation and contact with NATO partners expands. Information systems technology, specifically C4ISR systems, will likely remain the primary focus for technology collection, while lasers and optics technology acquisition attempts are also likely to grow concurrently with the attempts to acquire C4ISR systems. Collection against aeronautics technology, in the form of UAV systems, is likely to surpass collection of sensors technology, as NATO and Coalition forces continue to champion UAV systems as an integral component of C4ISR systems for its high-value, multi-tasking capabilities. (Confidence Level: Moderate)

CASE STUDIES

CASE STUDIES

A suspected representative of a foreign firm contacted via email a defense contractor employee, working on military grade technologies for a cleared U.S. defense company; however, DSS noted that the requestor's company's name did not match the incoming email address. The email correspondent claimed his company had an "urgent requirement" for military-grade technology developed at the contractor facility and wanted to establish a business relationship. Subsequent analysis revealed that the email address the correspondent used was associated with a second foreign company having a history of end-user certificate fraud.

A representative of a foreign research center contacted a cleared U.S. defense facility and provided product design schematics in an apparent attempt to justify obtaining export-controlled materials. A review of the research center's schematics revealed that they were associated with a military critical technology program. At first, the research center denied that the product in the schematics had any military applications; but when challenged, they eventually recanted and admitted the

product design could indeed be used for military purposes. Despite this exposed deception, the foreign firm's representatives continued to maintain they had no intention of utilizing the final product for such purposes.

A cleared U.S. defense company reported receiving multiple deceptive emails with attachments that (when opened) resulted in malicious software being automatically installed on the company's internal computer system. Numerous employees within this cleared defense company were victims of this ruse. Following the extraction and analysis of one of the malicious payloads, cleared U.S. defense analysts discovered additional malicious codes embedded in .gif and .jpg image files in the software.

Over several months, a foreign firm repeatedly contacted an employee of a U.S. cleared defense company, cultivating his assistance to procure components for the foreign firm's use. Although the contact began with a seemingly innocuous request for non-export controlled components, the foreign firm

later amended its list to include dual-use export controlled items. The foreign company eventually shared the contractor employee's contact information with multiple sections inside the foreign firm, resulting in a flood of additional requests to the same contractor employee. Within a month, this same foreign firm shifted focus to a second cleared defense company, requesting technology of interest to the military research and development efforts of the foreign firm's country of origin.

An individual apparently posing as a foreign student contacted an employee working for a cleared U.S. defense company performing aerodynamics research, asking for what amounted to classified information on the cleared defense company's UAV applications. The foreign "student," supposedly an aerodynamics major at a major foreign university, also inquired about the possibility of an intern position in the company's aerodynamics research branch. The "student's" requested information and research interests related to classified and export restricted technology actively sought by the student's country of origin.

An engineering team from a U.S. defense contractor participated in an exchange with a foreign counterpart team during which approved, unclassified technical

information was shared between participants. Following the exchange program's completion, representatives of the U.S. company discovered several export-restricted documents among a large volume of printed materials that the foreign engineer team left on-site. Upon further review of the printed materials the foreign engineers left, the U.S. company representatives discovered the foreign team had acquired a large amount of open source information on military programs clearly outside the scope of the unclassified contract with the cleared U.S. defense company.

OUTLOOK

A. Conclusion

Breaking the suspicious requests into regions, the current two-year trends show the ranking of regions remained constant; however, the percentages changed. DSS found that the region with the largest number of suspicious contacts, East Asia and the Pacific, increased from 30 to 36 percent when compared to statistics from FY04-FY05. DSS noted these East Asia and the Pacific collection efforts were almost twice as frequent as those reports emanating from the Near East, the second largest foreign collector of U.S. technology. After these collectors, Europe and Eurasian and South and Central Asia entities completed the hierarchy of most frequently encountered collectors. The aforementioned top collectors targeted U.S. technology, specifically "Information Systems," representing a 23 percent focus of collection activities.

This collection period saw a shift in collectors from entities associated with governmental entities to those linked to commercial enterprises. The most prolific entities continued to utilize "Commercial" collectors to acquire U.S. technology with that category of collector affiliation responsible for almost 40 percent of Suspicious Contact Reports (SCRs). Reporting indicated the governments from the East Asia and Pacific and Near East regions used both legitimate commercial entities and illicit front companies in attempts to acquire controlled technologies. Meanwhile, South and Central Asia collectors were more inclined to use less-traditional collectors, such as students, to gain access to restricted U.S. technology. The top collectors also relied heavily on "Government Associated" entities

to target U.S. technology with contacts from that category representing 24 percent of the collection effort.

In FY06-FY07, the top collectors used "Request for Information" (RFI) and "Attempted Acquisition of Controlled Technology" as the main Methods of Operation (MO) to acquire U.S. technology. Entities utilizing these MOs as well as "Solicitation and Marketing of Services" were responsible for over 70 percent of all collection attempts. This was also consistent from entities within the specific regions, as "RFI" and "Attempted Acquisition of Controlled Technology" continued regionally as the top collection MOs. The top collectors also used the "Suspicious Internet Activity" MO to collect U.S. technology. This MO significantly increased from four to 10 percent to occupy the position as the fourth most frequently encountered collection technique.

During FY06-FY07, reporting from the most prolific collectors also included those reports with a cyber nexus. Suspicious entities with IP addresses originating in the East Asia and the Pacific region represented 52 percent of the cyber collection effort, greatly outdistancing Europe and Eurasia as the second-ranking region-specific origin of such incidents. DSS and Intelligence Community reporting indicated that East Asia and the Pacific cyber collectors were targeting Cleared Defense Contractor (CDC) networks for R&D and "Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance" (C4ISR) programs in support of their "Information Systems" collection effort. Similarly, the most prolific cyber collectors targeted "Information Systems"

as the most popular cyber technology with 43 percent of suspicious contact activity focused on acquisition of information applying to that discipline. To gain this technology, collectors used the "Attempted Intrusion" MO the most, constituting 61 percent of the cyber collection effort against this technology. Due to the nature of IP addresses and the use of anonymous proxies, cyber collectors often conceal their identities. This makes it difficult to positively ascertain the collector's true affiliation. In FY06-FY07, DSS analysis could only attribute four percent of cyber related SCRs to entities within specific regions of origin. Although it is difficult to discover true cyber affiliations, network attacks and attempted intrusions continue to grow with the expansion of the global marketplace and technological advancements.

B. Forecast

As contractor personnel become more sensitized to the threat, it is highly likely the number of SCRs from CDCs, including cyber incidents, will increase proportionately. Similarly, as the defense industry engages emerging third world markets, the use of less-traditional collectors is also highly likely to increase, along with a concurrent increase in the number of suspicious contacts.

Information systems technology, particularly C4ISR systems, is highly likely to remain a priority technology target for the most prolific collectors. This also includes increased collection against modeling and simulation technology. Weapons technology developments, particularly missile and missile defense technologies, are likely to continue as collection priorities for entities for the Near East and Europe and Eurasian regions; while lasers and optics, materials and processing, and naval technologies are likely priority targets for the

East Asia and the Pacific region. Aeronautics technologies, especially advanced UAV systems, are likely to continue as a major focus for all foreign collectors.

Suspicious entities are highly likely to increase their use of the Internet against defense contractors as a relatively low-risk, high-gain technique, offering illicit collectors the opportunity to acquire sensitive and proprietary information stored on U.S. computer networks. Internet targeting can also be used as a tool to identify targets of opportunity not readily apparent to potential collectors, allowing hostile elements to focus their collection efforts and design targeting plans employing the full range of collection techniques.

It is highly likely foreign commercial entities will increase their attempts to purchase CDC developed technologies, as well as pursue joint commercial endeavors in order to gain access to sensitive U.S. technology. These endeavors are likely to complicate the U.S. security and counterintelligence communities' ability to distinguish between legitimate global business practices and attempts at illegal acquisition of U.S. technologies. Furthermore, nearly all collectors will continue attempts to acquire any and all U.S. dual-use technologies regardless of their significance in order to advance their own technological bases with both commercial and military applications. This multi-dimensional threat environment will almost certainly require innovative and pro-active vigilance on the part of U.S. defense security personnel and cleared contractors. (Confidence Level: High)

REFERENCE MAP
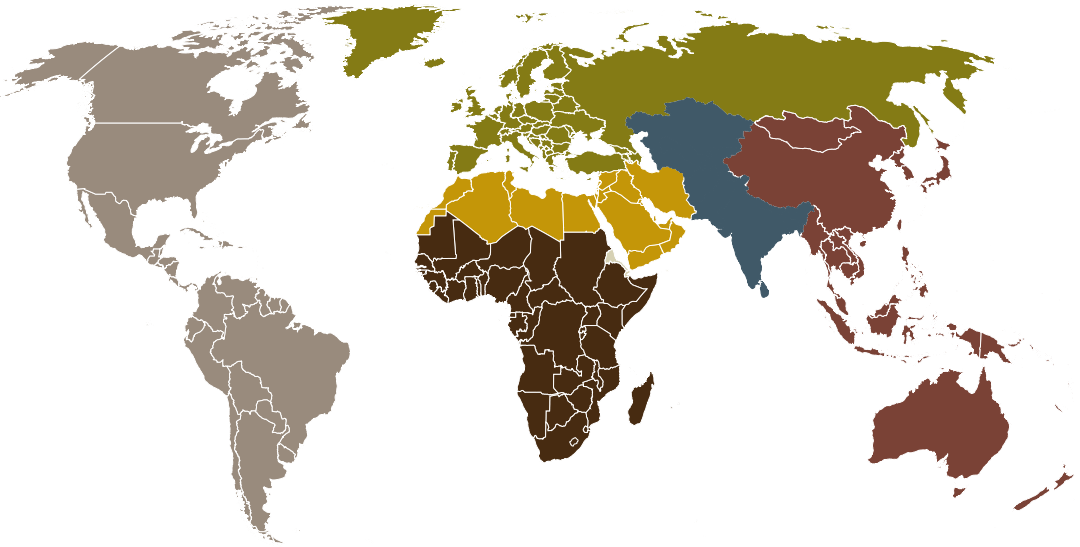
Retrieved from U.S. Department of State, http://www.state.gov/countries/, on 19 Dec 08

AFRICA	EAST ASIA AND THE PACIFIC	EUROPE AND EURASIA	NEAR EAST	SOUTH AND CENTRAL ASIA	WESTERN HEMISPHERE
Angola	Australia	Albania	Algeria	Afghanistan	Antigua and Barbuda
Benin	Brunei	Andorra	Bahrain	Bangladesh	Argentina
Botswana	Burma	Armenia	Egypt	Bhutan	Aruba
Burkina Faso	Cambodia	Austria	Iran	India	Bahamas, The
Burundi	China	Azerbaijan	Iraq	Kazakhstan	Barbados
Cameroon	Fiji	Belarus	Israel	Kyrgyz Republic	Belize
Cape Verde	Indonesia	Belgium	Jordan	Maldives	Bermuda
Central African Republic	Japan	Bosnia and Herzegovina	Kuwait	Nepal	Bolivia
Chad	Kiribati	Bulgaria	Lebanon	Pakistan	Brazil
Comoros	Korea, North	Croatia	Libya	Sri Lanka	Canada
Congo, Democratic Republic of the	Korea, South	Cyprus	Morocco	Tajikistan	Cayman Islands
Congo, Republic of the	Laos	Czech Republic	Oman	Turkmenistan	Chile
Cote d'Ivoire	Malaysia	Denmark	Palestinian Territories	Uzbekistan	Colombia
Djibouti	Marshall Islands	Estonia	Qatar		Costa Rica
Equatorial Guinea	Micronesia	European Union	Saudi Arabia		Cuba
Eritrea	Mongolia	Finland	Syria		Dominica
Ethiopia	Nauru	France	Tunisia		Dominican Republic
Gabon	New Zealand	Georgia	United Arab Emirates		Ecuador
Gambia, The	Palau	Germany	Yemen		El Salvador
Ghana	Papua New Guinea	Greece			Grenada
Guinea	Philippines	Greenland			Guatemala
Guinea-Bissau	Samoa	Holy See			Guyana
Kenya	Singapore	Hungary			Haiti
Lesotho	Solomon Islands	Iceland			Honduras
Liberia	Taiwan	Ireland			Jamaica
Madagascar	Thailand	Italy			Mexico
Malawi	Timor-Leste	Kosovo			Netherlands Antilles
Mali	Tonga	Latvia			Nicaragua
Mauritania	Tuvalu	Liechtenstein			Panama
Mauritius	Vanuatu	Lithuania			Paraguay
Mozambique	Vietnam	Luxembourg			Peru
Namibia		Macedonia			St. Kitts and Nevis
Niger		Malta			St. Lucia
Nigeria		Moldova			St. Vincent and the Grenadines
Rwanda		Monaco			Suriname
Sao Tome and Principe		Montenegro			Trinidad and Tobago
Senegal		Netherlands			United States
Seychelles		Norway			Uruguay
Sierra Leone		Poland			Venezuela
Somalia		Portugal			
South Africa		Romania			
Sudan		Russia			
Swaziland		San Marino			
Tanzania		Serbia			
Togo		Slovakia			
Uganda		Slovenia			
Zambia		Spain			
Zimbabwe		Sweden			
		Switzerland			
		Turkey			
		Ukraine			
		United Kingdom			

Retrieved from U.S. Department of State, http://www.state.gov/countries/, on 19 Dec 08

FEEDBACK FORM

(U) Comments or questions pertaining to this publication should be addressed to Defense Security Service, ATTN: CI Directorate, 1340 Braddock Place, Alexandria, VA 22314.
Web Site: http://www.dss.mil

Cleared Defense Contractor Name: _____
CAGE Code: _____

Point of Contact: _____
Address: _____
Email/Phone: _____

Issue: _____
_____
_____
_____
_____
_____
_____
_____
_____

Discussion: _____
_____
_____
_____
_____
_____
_____
_____
_____

Recommendation: _____
_____
_____
_____
_____
_____
_____
_____
_____