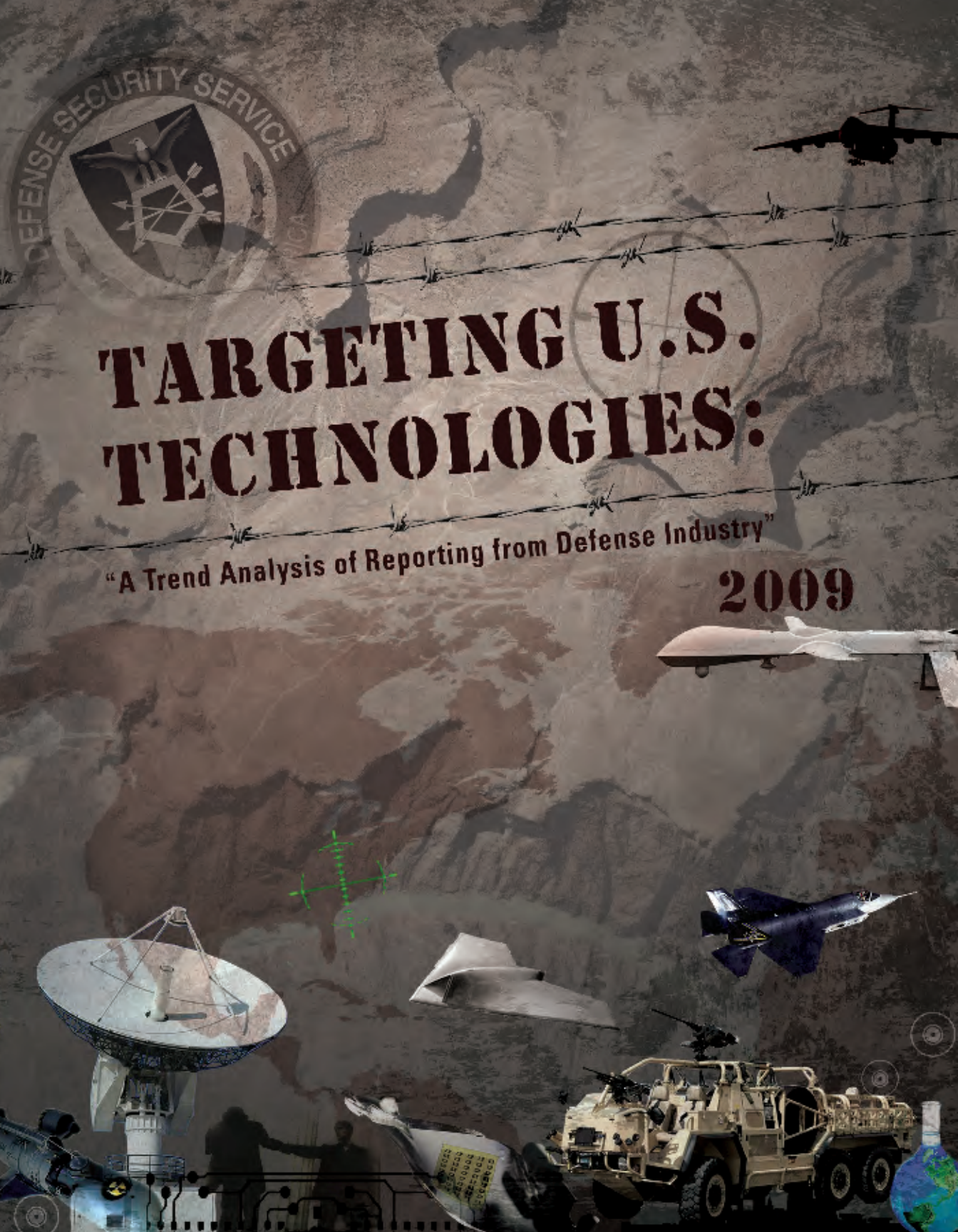


TARGETING U.S. TECHNOLOGIES:

"A Trend Analysis of Reporting from Defense Industry"

2009

Produced by Defense Security Office
Counterintelligence Directorate

Contributors:
Mr. Thomas Badoud, Mr. Timothy Deerr, Ms. Sara DeWitz, and Mr. John Parsons

http://www.dss.mil

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

United States defense-related technologies and information are under attack: each day, every hour, and from multiple sources. The attack is pervasive, relentless, and unfortunately, at times successful. As a result, the United States' technical lead, competitive edge, and strategic military advantage are at risk; and our national security interests could be compromised. Defeating this attack requires knowledge of the threat and diligence on the part of all personnel charged with protecting classified information, to deter or neutralize its effect.

The Defense Security Service (DSS) works with defense industry to protect critical technologies and information. Defense contractors with access to classified material are required to identify and report suspicious contacts and potential collection attempts as mandated in the National Industrial Security Program Operating Manual (NISPOM). DSS publishes this annual report based on an analysis of suspicious contact reports (SCRs) that DSS considers indicative of efforts to target defense-related information.

Security officials, cleared defense contractors, intelligence professionals, and Department of Defense policy and decision makers can use information in this publication to assess the technology collection threat and develop and implement appropriate measures to mitigate its effect. DSS analysts examine information obtained from SCRs to identify the most frequently targeted technologies, assess the most common collection methods, explore possible motivations and affiliations of those attempting the collection, and identify the locations where these collection threats originate. If we are to be relevant and effective in defeating this threat, it is incumbent upon cleared defense contractors to report all incidents indicative of targeting. It is our hope that the information and analysis in this report will inform and encourage such reporting.

DSS encourages all Facility Security Officers to use the information in this report to supplement security awareness and education programs at their facilities. In addition to increasing threat awareness within the industrial base, robust training efforts contribute to additional SCRs and further contribute to the integrity of this 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 United States cleared defense industry. DSS thanks the employees and companies of the United States cleared defense industry for their continued support of the NISPOM and their contributions to this annual publication.

Kathleen M. Watson

KATHLEEN M. WATSON
Director
Defense Security Service

EXECUTIVE SUMMARY

A. KEY FINDINGS

The Defense Security Service (DSS) presents the 2009 "Targeting U.S. Technologies" report in summation of defense industry reporting for fiscal year 2008 (FY08). This report analyzes possible foreign targeting of information and technologies developed or maintained within the cleared defense contractor (CDC) community. It offers a single perspective of the threat as viewed through the admittedly narrow, but nonetheless relevant, window of defense industry's unsolicited contact with foreign entities interested in defense programs and technologies. The substance of this report is drawn from DSS analysis of suspicious contact reports (SCRs) received from industry. These reports describe suspicious foreign activity targeting U.S. personnel, technologies, classified information, and export controlled products. The following constitutes key findings based on DSS analysis of FY08 data as compared to the previous year's reporting:

- **East Asia and Pacific-originated contacts continued to generate the greatest number of suspicious reports attributable to a specific region of origin.** For the fifth year in a row, reporting with an East Asia and Pacific nexus far exceeded those from any other region suggesting a continuing, concerted, and growing effort to exploit contacts within United States industry for competitive, economic, and military advantage.

- **Aggressive collection attempts by commercial actors continued to surge.** In FY08, commercial entities attempted to collect defense technology at a rate nearly double that of governmental or individual collector affiliations. This trend likely represents a purposeful attempt to make the contacts seem more innocuous, shifting focus from government collectors to commercial or non-traditional entities.

- **Collectors continued bold and overt exploitation of the Internet to acquire information via direct requests.** Facilitated by ever increasing world wide connectivity, the ease of inundating industry with overt email requests and webpage submissions made direct requests a premier vehicle for solicitation and/or collection. While not all direct requests for information or services represent organized collection attempts, exploitation of this medium provides collectors an efficient, low-cost, high-gain opportunity to acquire classified or restricted information.

- **Unmanned aerial vehicle (UAV) technology has emerged as a priority target of aggressive collectors from multiple regions.** In FY08, DSS noticed a significant increase in exploitation attempts against UAV systems and technologies at CDCs. Targeting of UAVs is non-region specific, broadly based, and spans all phases of research, development, and deployment. It is highly likely that this interest and probable targeting is the direct result of a growing and increasingly competitive world market for UAV systems.

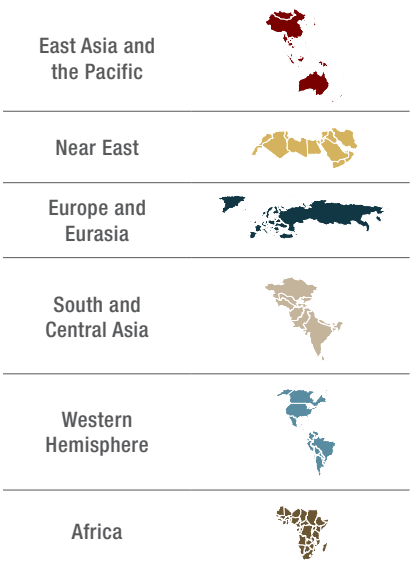
B. REGIONAL COLLECTION TRENDS

According to the U.S. State Department, there are 194 independent countries in the world. In FY08, entities in over half of these countries attempted, at least once, to illicitly acquire United States defense technologies or information. DSS organized information about 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).

Concurrently, DSS examined SCRs received from the defense industry in FY08 to determine which represented matters of confirmed or probable counterintelligence (CI) concern. Where possible, analysts affiliated relevant reports with specific regions of origin assessing the geographic association of the requestor. For FY08, the regions most frequently affiliated with validated or probable reports of CI concern were, in descending order of occurrence:

REGIONAL TRENDS

FIGURE 1



A comparison to FY07 data reveals no major changes in this hierarchy; with East Asia and the Pacific and Near East entities remaining the most prolific collectors of United States technology or information. As in previous years, East Asia and the Pacific collectors continued to dominate collection efforts in terms of sheer volume. The desire to maintain and dominate a regional military capability, while enhancing political and economic influence, likely drives intense collection priorities from East Asia and Pacific entities. This modernization campaign relies heavily on exploiting United States technical advancements. Countering this threat to United States defense industry will require the highest degree of cooperation, education, awareness, and vigilance.

This reporting period also witnessed a number of SCRs emanating from the Near East region. While Near East entities were the second most prolific regional collectors, the volume did not approach the deluge of reporting emanating from East Asia and the Pacific collectors. To counter international trade restrictions and embargoes imposed on various actors in this region, Near East collectors used widely cast and varied approaches to target United States technology, frequently engaging non-traditional collectors, such as students at American universities, to illicitly gather information and attempt to acquire technology. Given rising trends related to this region, suspicious requests from Near East entities are not likely to abate in the near future.

Despite Europe and Eurasia's geo-political significance and economic status as a rival in the technical marketplace, attempts to acquire defense-related technologies emanating from this region failed to keep pace with collection attempts noted from either the East Asia and Pacific region or the Near East region. When DSS first compiled comparative statistics in 2004, European and Eurasian collectors ranked second only

to East Asia and the Pacific entities. Since then, SCRs with European and Eurasian nexes have declined steadily, relegating the region to the third position in the hierarchy of collectors, an almost 40 percent decrease from reports in 2004.

The reasons for this relative decline remain largely conjectural, but DSS reporting indicates that European and Eurasian collectors may be simply less dependent on overt contacts with United States industry to keep pace with technical advancements. Although many European and Eurasian research and development (R&D) programs are robust and favorably positioned to satisfy the majority of their own technical requirements, intelligence community reporting indicates that this indigenous R&D capacity does not diminish an appetite for U.S. military and dual-use technologies. More sinisterly, it may suggest that Europe and Eurasia collectors do not need to use high-profile collection techniques because their covert collection methodologies are already efficient and effective as to render the more blatant, overt requests largely supplemental to other collection competencies. It is noteworthy that even though their overt collection efforts have declined, European and Eurasian cyber actors remain some of the most active targeters of United States technology.

C. COLLECTOR AFFILIATIONS

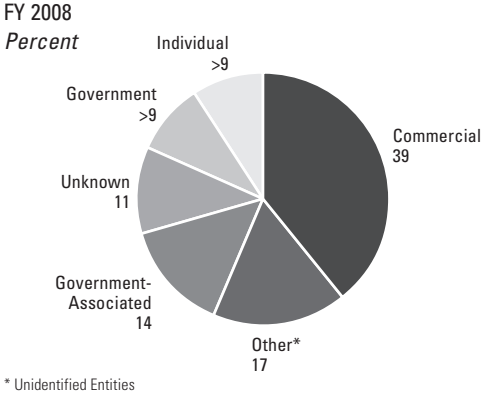
DSS analyzes each SCR to determine the collector's affiliation in an attempt to ascertain which foreign entity is targeting United States technology. The examples below describe a sampling of collectors resident within a region of origin:

- Government: Ministry of Defense, foreign military attachés, or branches of the military
- Government Affiliated: Research institutes, laboratories, government-funded universities, or contractors representing a government agency
- Commercial: Businesses in the commercial and defense sectors
- Individual: Persons seeking financial gain, persons avoiding traditional export procedures, or persons purportedly seeking academic or research information

As in FY07, commercial entities represented the top collectors of United States technology, outstripping government affiliated entities as the most frequently observed collector category. While affected by the explosive growth of the worldwide marketplace and the ease with which commercial entities make inquiries through the Internet, the growing preeminence of commercial collectors is likely attributable, at least in part, to a conscious effort on the part of foreign governments to mask interest using commercial surrogates to obtain information designed to enhance a specific regions' technical or economic competitive posture. The collector affiliations suspicious entities most frequently used are represented in the figure below:

COLLECTOR AFFILIATIONS

FIGURE 2



* Unidentified Entities

D. METHODS OF OPERATION

Once DSS identifies the requestor's region of origin, as well as the collector's probable affiliation, DSS assesses the methods of operation (MOs) that the suspicious entity employs to acquire information or technology. Analysis of MOs assists CDC personnel in recognizing suspicious entity attempts to acquire sensitive defense-related information and aids in the application of appropriate countermeasures to mitigate or negate effectiveness.

In FY08, the top four collection MOs were used in 80 percent of all foreign collection attempts. The MOs suspicious entities most frequently utilized were, in descending order of occurrence:

METHODS OF OPERATION

FIGURE 3

Direct Request
Email requests for information, webcard purchase requests, price quote requests, phone calls, or marketing surveys

Suspicious Internet Activity
Confirmed intrusion, attempted intrusion, computer network attack, potential pre-attack, or spam

Solicitation and Seeking Employment
Offering technical and business services to CDCs, resume submissions, or sales offers

Foreign Visits and Targeting
Suspicious activity at a convention, unannounced visit to a CDC, solicitations to attend a convention, offers of paid travel to a seminar, targeting of travelers, questions beyond scope, or overt search and seizure

Exploitation of direct requests continued to be the most common technique that foreign entities used in attempting to acquire information in FY08. Of note, suspicious Internet activity was second only to direct request as a technique of choice, emphasizing the growing significance of that MO to facilitate foreign collection of defense-related information and technology.

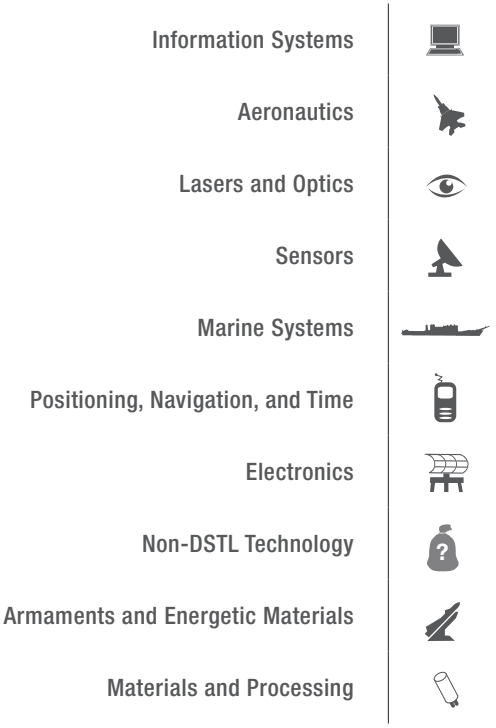
E. TARGETED TECHNOLOGIES

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

DSS analysis of FY08 SCRs indicated the following technologies, listed in descending order of foreign entity interest, represented probable collection priorities:

TARGETED TECHNOLOGIES

FIGURE 4



This listing is generally consistent with previous years' assessments. In FY08, suspicious entities continued to target information systems technology most frequently, as they had in FY07. The remaining technical categories retained their relative positions in the hierarchy, but interest in aeronautic technology saw the largest increase, owing primarily to growing interest in the acquisition of information and technologies identifiable with unmanned aerial vehicles (UAVs).

F. SPECIAL FOCUS AREA: TARGETING UAVS

This report contains a section focused on the increasing prominence of UAVs as an emerging collection target. Technically diverse, UAVs can range from small, hand-launched planes to armed high-altitude long-endurance vehicles. The UAV market also continues to expand as developers continually offer updated systems and, concomitantly, the global UAV demand increases. This cyclical dynamic drives intense requirements for the information related to state-of-the-art developments in the field. As a world leader in UAV R&D, the United States defense industry is at risk of intensive foreign-originated efforts to acquire UAV-related technologies or information. Given this targeting focus on UAV platforms and systems, it is highly likely that the imperative for economic or military advantage will continue to make defense industry UAV-related technologies primary collection priorities.

BACKGROUND

Department of Defense (DoD) Instruction, 5200.39, dated July 16, 2008, requires DSS to publish a classified report, as well as an unclassified companion 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 United States cleared defense industrial base. In accordance with this instruction, DSS disseminates 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 stated in Chapter 1, Section 3 of the National Industrial Security Program Operating Manual, 5220.22-M, dated February 28, 2006. Based on an analysis of these SCRs, DSS prepared this report.

This trends report covers information regarding the most prolific foreign collectors targeting the CDC community during fiscal year 2008 (FY08) as compared to the previous fiscal year. The report includes statistical and trends analysis on foreign collector affiliations, the traditional methods foreign entities 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 unmanned aerial vehicle (UAV) technology acquisition in United States cleared defense industry. DSS has determined a separate section is warranted to address this growing collection area. This section provides a definition of UAV systems that foreign collectors target, analysis based on reporting from defense industry, and the UAV collector methodology.

This report is published as part of the agency's ongoing effort to enhance awareness of foreign entities targeting the United States' cleared defense industry 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

DSS provides statistical and trends analysis on the foreign entity threat posed to the CDC community over the past fiscal year as compared to the previous year. The report is based on suspicious contact reporting DSS collected from the CDC community, and also includes reference to all-source Intelligence Community (IC) reporting. While DSS analyzes all SCRs received from industry, only those DSS determined to represent a potential CI concern in FY08 form the basis of this report. Through analytical processes and application of the DSS foreign intelligence threat assessment methodology, DSS determined over 32 percent of these reports reflected a potential CI threat to the CDC community or represented a link to elements DSS determined as hostile to United States' interests.

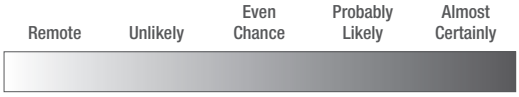
DSS analyzes foreign interest in United States defense technology in terms of the 20 categories in the Developing Science and Technologies List (DSTL). The DSTL is a compendium of science and technology capabilities being developed worldwide that have the potential to significantly enhance or degrade United States 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 United States technology, the targeting entity, the methods of operation, the relationships to previous reporting from the CDC community, and all-source IC information.

B. EXPLANATION OF ESTIMATIVE LANGUAGE & ANALYTIC CONFIDENCE

DSS adopted the IC estimative language standard for use in this report. The use of synonymous phraseology such as "we judge," "we assess," or "we estimate," as well as terms such as "likely," or "indicate," represent an effort by DSS 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 based directly on collected information; others rest on previous judgments, both of which serve as building blocks. In either type of judgment, DSS does not have "evidence" showing something to be a fact or that definitively links two items or issues.

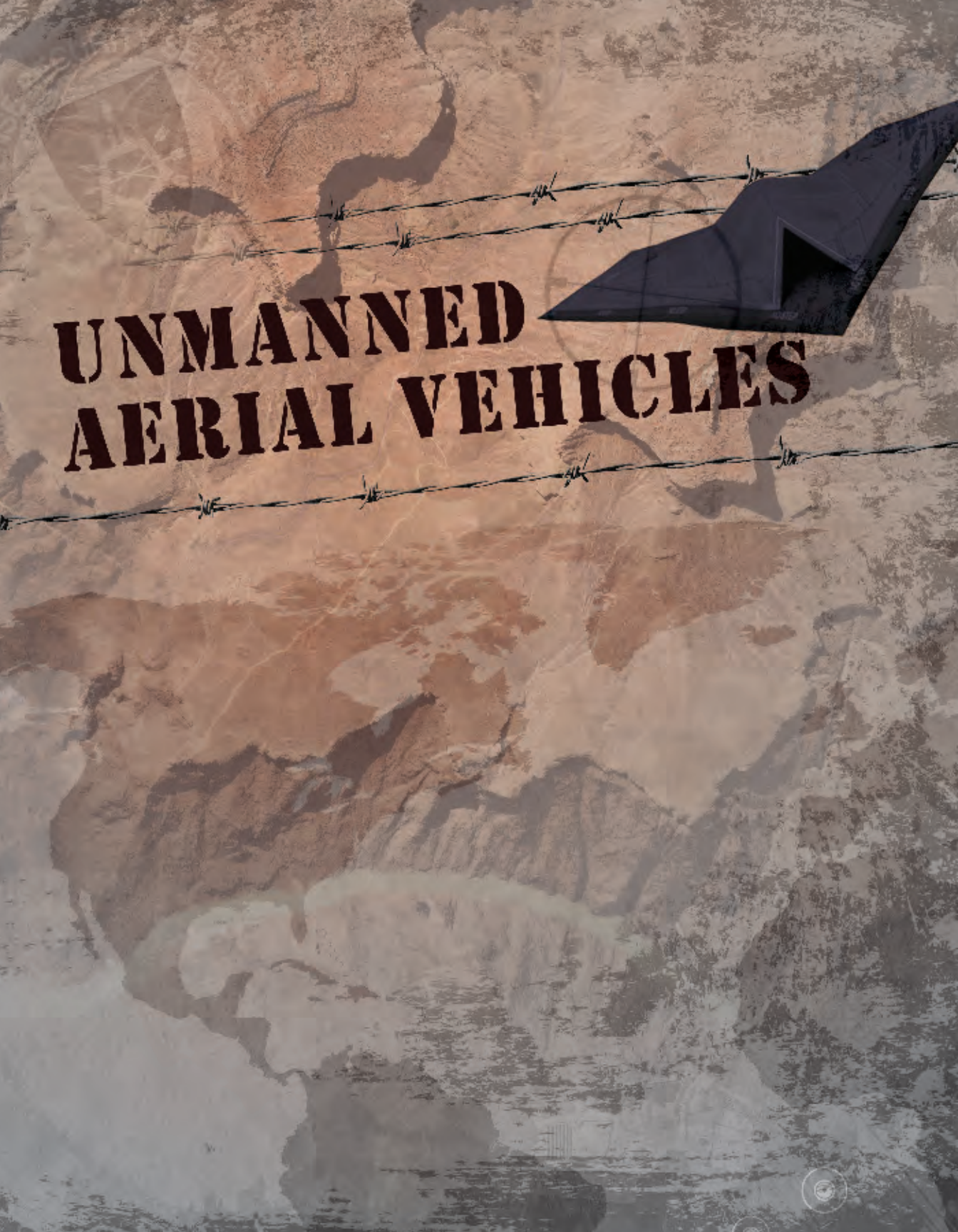
Intelligence judgments pertaining to "likelihood" are intended to reflect the Agency's sense of the probability of a development, event, or trend. Assigning precise numerical ratings to such judgments would imply more rigor than DSS intends. The chart below provides a rough idea of the relationship of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



DSS does not intend the term "unlikely" to imply an event will not happen. It uses "probably" and "likely" to indicate there is a greater than even chance. DSS uses 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 DSS is 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, DSS also ascribes analytic confidence levels based on the scope and quality of information supporting DSS judgments:

- High Confidence: Indicates judgments are based on high-quality information, or the nature of the issue makes it possible to render a solid judgment.
- Moderate Confidence: Indicates the information can be interpreted in various ways, DSS has alternative views, or the information is credible and plausible but not corroborated sufficiently to warrant a higher level of confidence.
- Low Confidence: Indicates the information is scant, questionable, or highly fragmented, making solid analytic inferences difficult, or that DSS has significant concerns or problems with the sources.


UNMANNED
AERIAL VEHICLES

SPECIAL FOCUS AREA: TARGETING UNMANNED AERIAL VEHICLES

1. OVERVIEW

The worldwide use of unmanned aerial vehicles (UAV) for reconnaissance, surveillance and target acquisition (RSTA) has risen steadily over the past 25 years, as countries place increasing emphasis on the acquisition of UAV capabilities to acquire parity or maintain strategic or tactical advantage.

As a world leader in UAV research and development (R&D), the United States industrial sector is at risk of intensive foreign-originated efforts to acquire UAV-related technologies or information resident at cleared defense contractor (CDC) facilities. CDCs should be aware of the intensity of this burgeoning threat and be prepared to institute appropriate measures to counter its effect. This special interest report is intended to contribute to that effort.

Currently, approximately 50 countries are involved with more than 100 different UAV acquisition and/or development programs. An overview of UAV R&D and production efforts reveals an unprecedented level of worldwide activity (See Figure 5):

- Near East entities continue to be the world leader in UAV exports and have made progress in the development of lethal UAVs.
- South and Central Asia collectors are leading importers of UAV technology and have started their own fledging development programs.

WHAT IS A UAV SYSTEM?

A UAV system usually consists of one or more aerial vehicles (AVs); a ground control station (GCS); a ground tracking unit; and AV launch, recovery, and support equipment. The AV flies within the atmosphere under its own power, performs a mission, and has the ability to return. A simple propeller-driven, fixed-wing AV, minus data links and payload, can cost as little as $5,000. Adding camera payloads and data links to transmit the camera pictures may increase the price anywhere from $350,000 to $1,000,000. Adding a GCS data processor, a ground tracking unit, ground maintenance support equipment, and extra payload packages may increase the system cost to as much as $25 million.[1]

In the more advanced systems, two-way data links provide payload management and vehicle command control as long as it stays within radio line-of-sight (LOS) of the ground tracking unit. The data links also transmit payload-derived reconnaissance data to the GCS. UAV navigation is derived from an internal navigation system coupled to a global positioning system receiver. Many United States UAVs are equipped with a return-to-home function that automatically routes the AV back to its home station or a predetermined location if the AV loses LOS with the ground tracking unit. The payloads or sensor packages available for use on UAVs include:

- Day-only television
- Low-light television
- Infrared line scan
- Thermal imagers
- Synthetic-aperture radar
- Moving-target-indicating radar

- East Asia and the Pacific entities desire to be major exporters of UAV platforms. Also, their indigenous programs are robust, but often lack operational success further creating pressure to obtain foreign technology.
- European and Eurasian entities aggressively pursue joint ventures and technology transfers to aid indigenous R&D efforts.
- African collectors have successfully marketed their systems to third-party buyers.

The UAV market continues to expand as a greater number of developers offer updated systems and the global demand increases. This competitive dynamic drives intense requirements for the information related to UAV state-of-the-art developments. These advanced UAV technologies may range from hand-launched, micro-UAVs to small business or jet-sized high-altitude long-range endurance platforms.

2. TREND ANALYSIS

UAVs continue to be the most dynamic and competitive growth sector of the world aerospace industry. Commercial market studies estimate that over the next 10 years, UAV development and acquisition spending will almost double from worldwide expenditures of $4.4 billion annually to $8.7 billion. The United States accounts for approximately 70 percent of the worldwide UAV research and development test and evaluation (RDT&E) spending but only 60 percent of the procurement spending. Europe and Eurasia represents the second largest source of RDT&E and acquisition spending, followed closely by the East Asia and Pacific region. ***Analyst Comment: It is likely the East Asia and Pacific region will overtake European and Eurasian UAV expenditures in the next decade. (Confidence Level: Moderate)***

2.1. UAV Regions of Origin

Defense industry reporting indicates that UAV RDT&E programs vary by region, technological competencies, and resources. Whether the collection efforts are motivated to enhance country-specific production capabilities, promote a country's competitiveness for the growing UAV world market, augment a specific country's military competencies, or develop potential countermeasures, UAV technology remains an intense focus of foreign collection efforts. Defense industry reporting reveals entities from the following regions attempted to acquire export-controlled, UAV-related technology in FY08 (See Figure 5):

- South and Central Asian entities represented the most prolific collectors, requesting complete UAV systems, composite materials, auto pilot systems, and sensor payload technology.
- Near East collectors attempted joint ventures and offered maintenance and training services in exchange for United States' classified systems. Suspicious technology requests focused on control software and radio frequency microwave components.
- East Asian and Pacific entities utilized all available means of collection to target UAV technology including military joint agreements, illicit collection attempts, joint venture proposals, and approved foreign military sales. These regional entities requested production details as well as platform and individual components like auto tracking antennas.
- European and Eurasian collectors used a variety of state and non-state actors to acquire UAV command and control programs and airframe carbon composite manufacturing details.

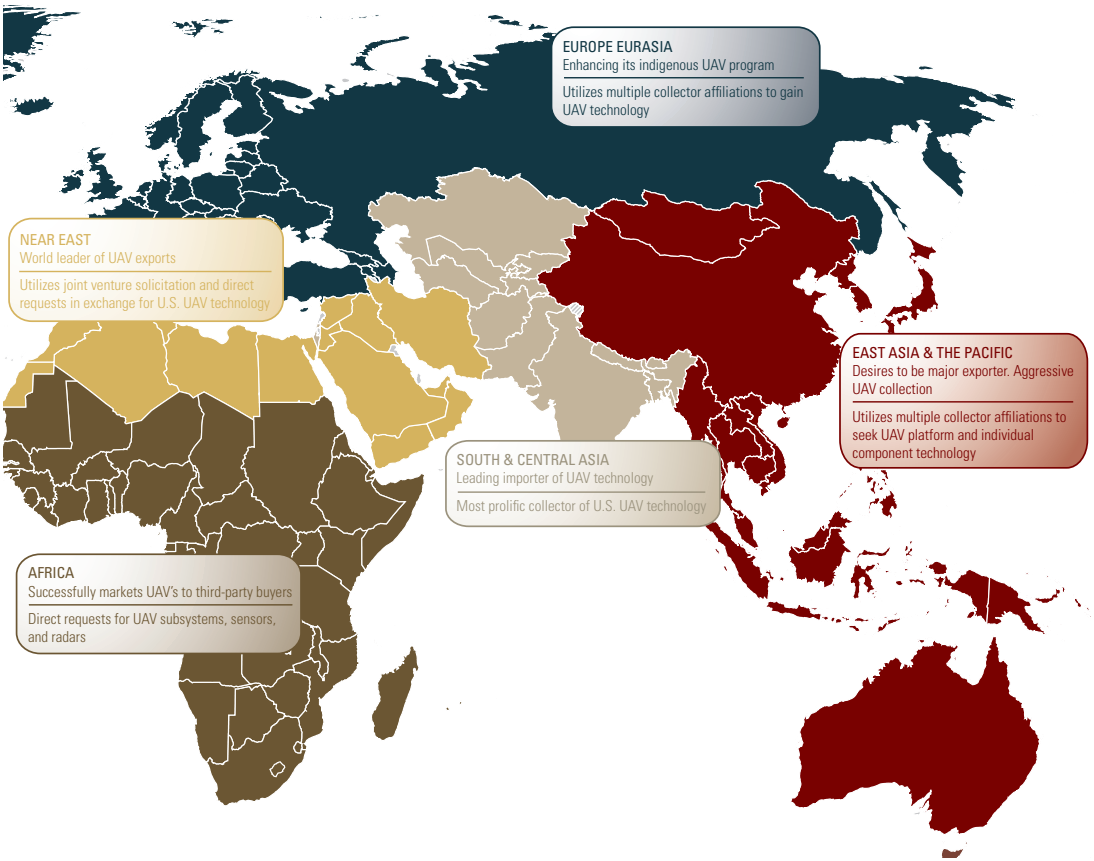
Defense industry reporting involving UAV technologies revealed a diverse effort not unique to any single world region. Most collection efforts emanated from regions with more advanced industrial capabilities or active UAV development programs. Typically, these collection efforts focused on specific UAV technologies essential to a particular region's RDT&E program.

Analyst Comment: Although regional entities occasionally sought complete systems, it is likely the desire for fully functional UAV capabilities most commonly originated from regions attempting to address existing internal or border conflicts that taxed their limited command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities. (Confidence Level: High)

FOREIGN UAV COLLECTION:

A Perspective Based on Defense Industry Reporting

FIGURE 5



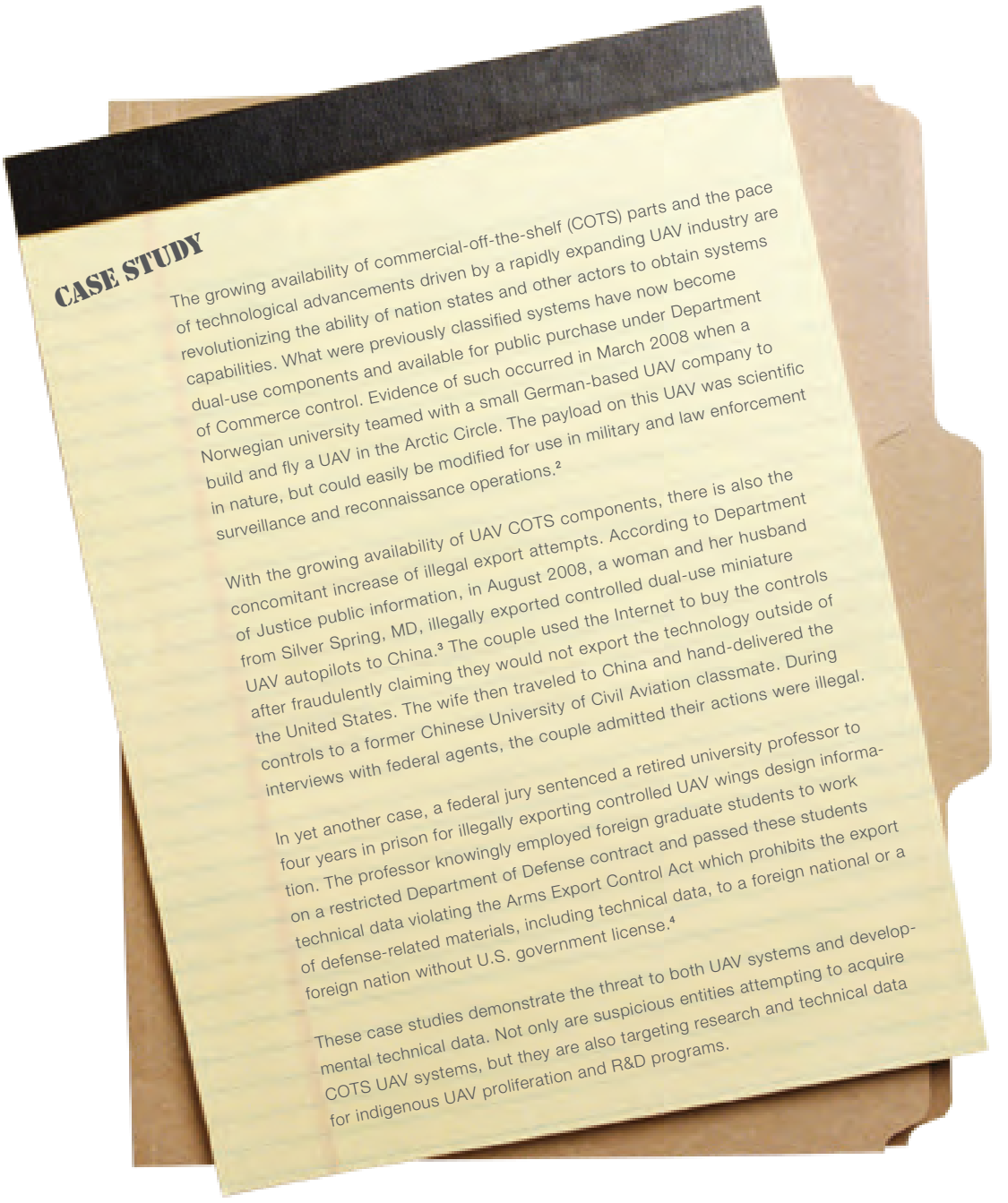
2.2. Targeted Technology

DSS suspicious contact reports showed that UAV technology collection attempts covered all aspects of UAV systems. The collectors ranged from high-tech companies in industrially-advanced countries to emerging third-world countries. Targeted technologies spanned the entire UAV spectrum and included:

- Software control programs
- Data link control systems
- Electro-optic sensors
- Infrared sensors
- Synthetic aperture radars
- Signals intelligence
- Electronic warfare systems
- Chemical-biological-radiological-nuclear sensors
- Launch and recovery systems
- C4ISR systems
- Propulsion designs
- Inertial navigation systems
- Advanced composite materials designs

3. ANALYTICAL FORECAST

In the last few years, there has been an evolution in battle space doctrine to use superior intelligence to defeat the enemy instead of relying exclusively on the application of overwhelming force. This new doctrine elevates the importance of UAV capabilities and drives the imperative to acquire UAV technologies. The proliferation of UAV RDT&E programs and associated fielding of systems has resulted in an ever-increasing demand for UAV technology and expertise. To maintain economic competitiveness, UAV companies, as well as suspicious collectors, can be expected to use every available means to acquire breakthrough technologies. Exploitation of joint ventures and/or teaming collaborations to acquire information will become increasingly common, as will attempts to solicit information from defense industry directly involved with UAV or associated dual-use technologies. As a major developer of UAV technologies, it is highly likely that defense industry's UAV technologies will remain premier targets of both an overt and covert foreign collection focus. (Confidence Level: High)



CASE STUDY

The growing availability of commercial-off-the-shelf (COTS) parts and the pace of technological advancements driven by a rapidly expanding UAV industry are revolutionizing the ability of nation states and other actors to obtain systems capabilities. What were previously classified systems have now become dual-use components and available for public purchase under Department of Commerce control. Evidence of such occurred in March 2008 when a Norwegian university teamed with a small German-based UAV company to build and fly a UAV in the Arctic Circle. The payload on this UAV was scientific in nature, but could easily be modified for use in military and law enforcement surveillance and reconnaissance operations.[2]

With the growing availability of UAV COTS components, there is also the concomitant increase of illegal export attempts. According to Department of Justice public information, in August 2008, a woman and her husband from Silver Spring, MD, illegally exported controlled dual-use miniature UAV autopilots to China.[3] The couple used the Internet to buy the controls after fraudulently claiming they would not export the technology outside of the United States. The wife then traveled to China and hand-delivered the controls to a former Chinese University of Civil Aviation classmate. During interviews with federal agents, the couple admitted their actions were illegal.

In yet another case, a federal jury sentenced a retired university professor to four years in prison for illegally exporting controlled UAV wings design information. The professor knowingly employed foreign graduate students to work on a restricted Department of Defense contract and passed these students technical data violating the Arms Export Control Act which prohibits the export of defense-related materials, including technical data, to a foreign national or a foreign nation without U.S. government license.[4]

These case studies demonstrate the threat to both UAV systems and developmental technical data. Not only are suspicious entities attempting to acquire COTS UAV systems, but they are also targeting research and technical data for indigenous UAV proliferation and R&D programs.


EAST ASIA
AND THE PACIFIC

EAST ASIA AND THE PACIFIC

1. OVERVIEW

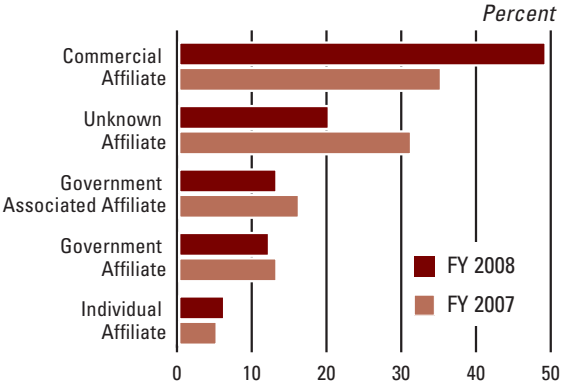
For the fifth consecutive year, the East Asia and the Pacific region retained its status as the home to the most prolific collectors of U.S. technology. Defense industry fiscal year 2008 (FY08) reporting revealed only minor variations from previous years in the types of technologies targeted and similarly the manner suspicious entities utilized to acquire them. Collectors of all persuasions continued to express keen interest in information systems technologies, specifically, those with dual-use applications involving command, control, communication, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities.

Furthermore, there was little to no change in the collection method entities commonly employed. The direct request method of operation (MO) was, by far, the most prevalent technique of choice with collectors often brazenly requesting restricted technology. Interest in aeronautics continued to swell and was especially focused on technologies associated with unmanned aerial vehicles (UAVs).

The use of commercial entities to collect controlled information and technologies far outpaced any other collector category, further expanding its traditional dominance as the regional collection affiliation of choice. The continued decrease of reports from government or government affiliated entities collecting information and concomitant increase of reports emanating from commercial collectors reinforces the assessment that East Asian and Pacific collectors likely avoid traditional state-sponsored affiliates in an attempt to mask illicit intelligence activities.

AFFILIATIONS

FIGURE 6



2. COLLECTOR AFFILIATIONS

As discussed in the overview, the commercial category of collectors dominated FY08 reporting, more than doubling any other collector affiliation, a recurring theme noted over the last three years. The continued rise of the commercial collector affiliation and the corresponding downward trajectory in the number of government or government affiliated suspicious contact reports (SCRs), reiterated a growing reliance on collection methods that mask state-sponsored interest. Furthermore, SCRs indicated regional entities continued to exploit non-traditional collectors, like graduate and post-graduate students applying for positions in United States defense industry, as a guise to acquire sensitive technologies.

Analyst Comment: While the growing global marketplace and ease of Internet connectivity may be partially responsible for the increase in commercial

collections, analysis of the SCRs and the corresponding decrease in the numbers of government or government affiliated collection attempts suggests it is likely that foreign intelligence agencies are successfully exploiting the commercial sector as their typically less alarming collection surrogates. (Confidence Level: Moderate)

The second most prolific regional affiliation in FY08 was the unknown affiliate; responsible for 20 percent of the East Asia and Pacific collection attempts. The lack of information in some direct requests or email solicitations makes it extremely difficult to determine if a government or commercial affiliation likely exists. In many cases, the only information the entity provided in a predominantly Internet-based request was an IP address that may or may not be related to the sender's region of origin.

Analyst Comment: The popularity of the "unknown" affiliation is likely derived from mass emailing ventures, a cost-effective measure to maximize the collector's return on requests for restricted or controlled technology. (Confidence Level: Moderate)

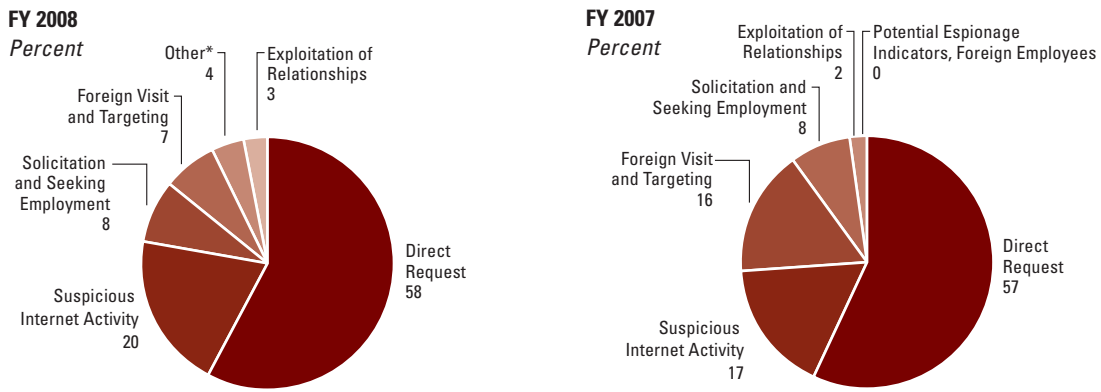
3. METHODS OF OPERATION

The direct request MO retained its top position as the favored MO for FY08, with just over half of all such requests relying on email and web-card submissions to request information and purchase technology. Also, the use of foreign visits and targeting as a collection method fell from the third most common MO in FY07 to fourth most prevalent in FY08.

Not to be overlooked, suspicious Internet activity continued to maintain its ranking as the second most preferred method, frequently involving confirmed intrusions of unclassified cleared defense contractor (CDC) computer systems. When compared against all regions, East Asia and the Pacific dominated as the most prolific in suspicious Internet activity. Collectors relied heavily on network obfuscation techniques to mask their locations and respective identities.

METHODS OF OPERATION

FIGURE 7



* Includes foreign employees and potential espionage indicators

Readily available information relating to various export-controlled technologies, programs, and personnel continued to assist in targeting those would-be victims. ***Analyst Comment: Requests for information and price quotes via email is the preferred MO to target United States technologies. This collection technique underscores the "low-risk, high-gain" efficiency associated with the direct request MO. Sending multiple requests for the same information to different individuals on a CDC network maximizes the available opportunities for the collectors to gain the information they seek. Additionally, the abundance of personnel and technical information contained within CDC websites, as well as the growing use of social networking sites, gives a likely targeting advantage to East Asia and the Pacific cyber actors exploiting the Internet. (Confidence Level: Moderate)***

4. TARGETED TECHNOLOGIES

During FY08, collectors in the East Asia and Pacific region showed significant interest in information systems technologies, often requesting data and hardware associated with battlefield management and

TARGETED TECHNOLOGIES

TABLE 1

Developing Science and Technologies List (DSTL) Codes	FY 2008 Percent
Information Systems	24
Aeronautics	11
Non-DSTL Technology	10
Marine Systems	10
Positioning, Navigation, and Time	10
Laser and Optics	7
Sensors	7
Electronics	6
Armaments and Energetic Materials	4
Materials and Processing	3
Space Systems	2
Ground Systems	2
Manufacturing and Fabrication	2
Chemical	> 0
Energy Systems	> 0
Nuclear	> 0
Weapons Effects	> 0
Directed and Kinetic Energy	> 0
Signature Control	> 0
Biological	0
Biomedical	0

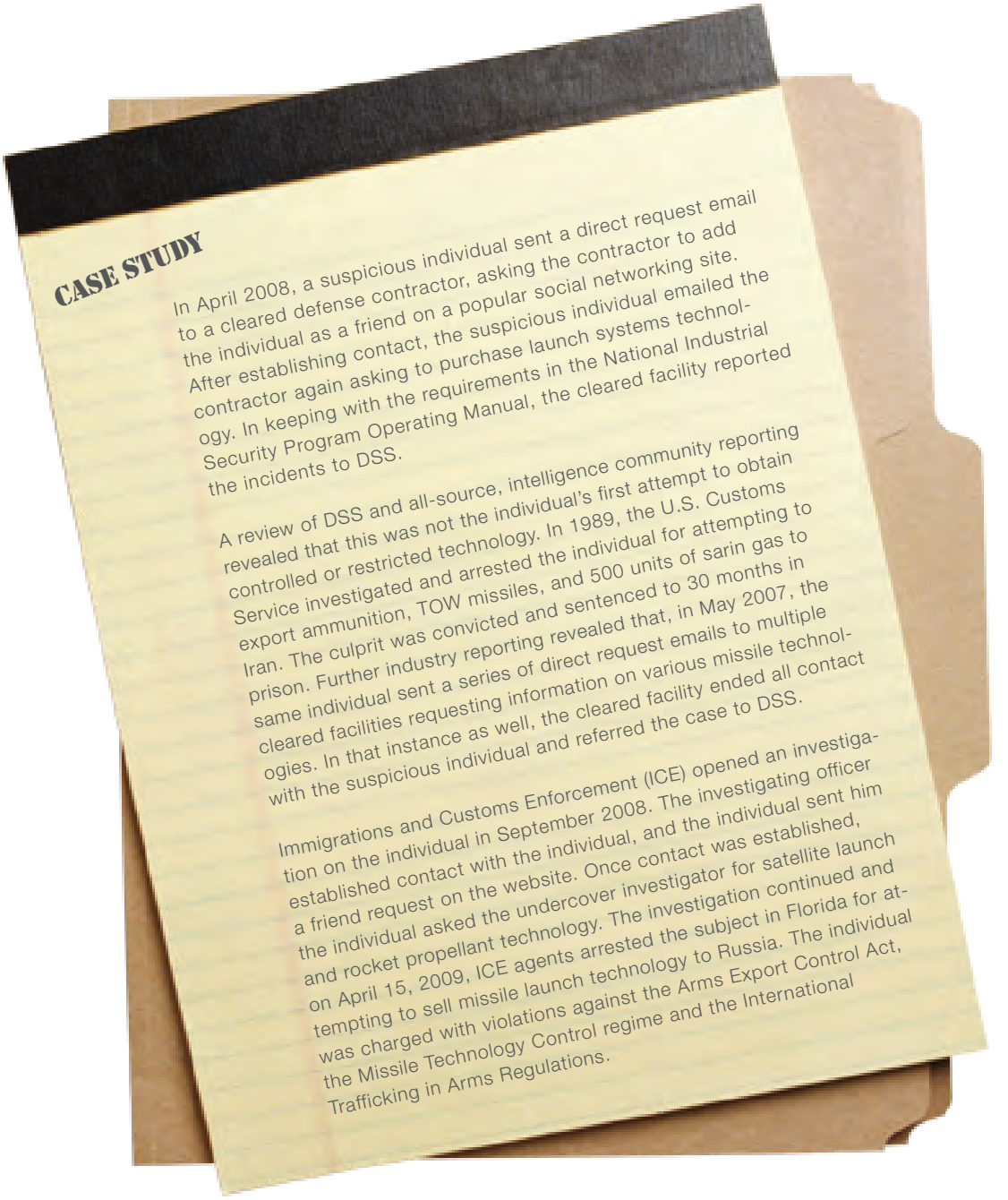
Developing Science and Technologies List (DSTL) Codes	FY 2007 Percent
Information Systems	28
Aeronautics	11
Sensors	10
Laser and Optics	9
Armaments and Energetic Materials	9
Marine Systems	6
Electronics	6
Manufacturing and Fabrication	4
Positioning, Navigation, and Time	4
Non-DSTL Technology	3
Space Systems	2
Weapons Effects	2
Ground Systems	2
Biological	1
Energy Systems	1
Chemical	1
Signature Control	< 1
Materials and Processing	< 1
Directed and Kinetic Energy	< 1
Biomedical	> 0
Nuclear	> 0

simulation systems. The nature of specific inquires largely replicated FY07 reporting, indicating C4ISR technologies were, and still are, in high demand. The aeronautics category represented the second strongest concentration of interest, most notably in inquiries related to UAV technologies. Closely following aeronautics technology, collectors requested marine systems and positioning, navigation, and time technologies information, with a keen interest in autonomous underwater vehicles and global positioning system simulators. Additionally, the armaments and energetic materials technology category continued to decline in the hierarchy of requested technologies, accounting for only four percent, down from the fifth most targeted technology in FY07.

Analyst Comment: Analysis of FY08 industry reporting reinforces previous assessments that interest in information systems-related technologies is most likely attributable to collectors focusing on research and development shortcomings with the goal of modernizing aging military C4ISR assets. (Confidence Level: High)

5. ANALYTICAL FORECAST

Consistencies in FY07 and FY08 reporting indicate entities in the East Asia and Pacific region are highly likely to continue focusing on the acquisition of dual-use technologies to advance internal capabilities, especially as it applies to C4ISR. Also, the ploy of using commercial or academic sector requests to circumvent import/export restrictions will likely continue as an attractive option to mask state-sponsored collection activities. Exploitation of joint agreements and legitimate purchases, executed for legal applications, will continue to enable illicit acquisition of dual-use technologies intended for restricted applications. Additionally, key regional collectors will likely continue to place their collection emphasis on the aeronautics industry, most probably in an attempt to acquire access to advanced UAV technologies. (Confidence Level: High)



CASE STUDY

In April 2008, a suspicious individual sent a direct request email to a cleared defense contractor, asking the contractor to add the individual as a friend on a popular social networking site. After establishing contact, the suspicious individual emailed the contractor again asking to purchase launch systems technology. In keeping with the requirements in the National Industrial Security Program Operating Manual, the cleared facility reported the incidents to DSS.

A review of DSS and all-source, intelligence community reporting revealed that this was not the individual's first attempt to obtain controlled or restricted technology. In 1989, the U.S. Customs Service investigated and arrested the individual for attempting to export ammunition, TOW missiles, and 500 units of sarin gas to Iran. The culprit was convicted and sentenced to 30 months in prison. Further industry reporting revealed that, in May 2007, the same individual sent a series of direct request emails to multiple cleared facilities requesting information on various missile technologies. In that instance as well, the cleared facility ended all contact with the suspicious individual and referred the case to DSS.

Immigrations and Customs Enforcement (ICE) opened an investigation on the individual in September 2008. The investigating officer established contact with the individual, and the individual sent him a friend request on the website. Once contact was established, the individual asked the undercover investigator for satellite launch and rocket propellant technology. The investigation continued and on April 15, 2009, ICE agents arrested the subject in Florida for attempting to sell missile launch technology to Russia. The individual was charged with violations against the Arms Export Control Act, the Missile Technology Control regime and the International Trafficking in Arms Regulations.


NEAR EAST

NEAR EAST

1. OVERVIEW

In fiscal year 2008 (FY08), entities from the Near East region once again generated the second highest degree of collection attempts to acquire U.S. technology, consistently maintaining this position for the last four years behind East Asia and the Pacific collectors. Commercial collectors within the Near East region continued to dominate collection attempts, accounting for almost half of all targeting. Distantly following commercial entities, collectors identifiable as government associated collectors accounted for more than a quarter of the targeting effort. These collectors primarily continued to seek technologies involving information systems; however, regional entities also focused on the optics, lasers, and aeronautics categories of technology. Near East collectors most commonly utilized direct requests as a means to obtain information, followed by solicitation, seeking employment and suspicious Internet activity techniques. The collectors in this region represented a vast spectrum of entities, ranging from student and business entrepreneurs to full-fledged government operators.

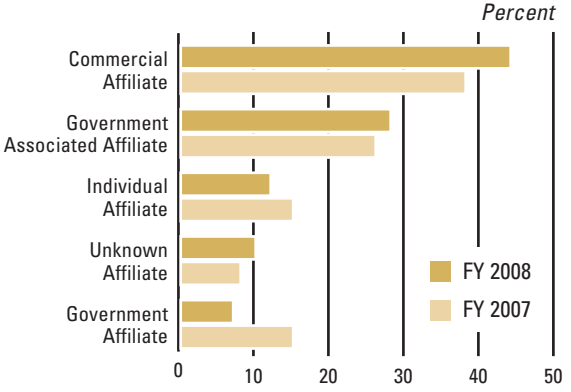
2. COLLECTOR AFFILIATIONS

Following a trend DSS noted in FY07 reporting, entities categorized as "commercial" continued to increase their collection efforts and accounted for 44 percent of all collection reports with a Near East nexus. The most significant regional change in FY08 reporting was the precipitous drop in collection efforts by entities strictly associated with government affiliates, constituting only seven percent of all collection efforts in FY08.

Analyst Comment: The continuing rise of Near East commercial entity activity continued to indicate a growing collusion between commercial entities and government associated entities, such as universities, public agencies, and research and development centers, to acquire leading-edge technology from defense industry. Consequently, the corresponding drop in strictly government entities is likely attributable to the regional governments' close control of all commercial and government associated entities' activities, reducing the need for direct government involvement in collection efforts. (Confidence Level: Moderate)

AFFILIATIONS

FIGURE 8



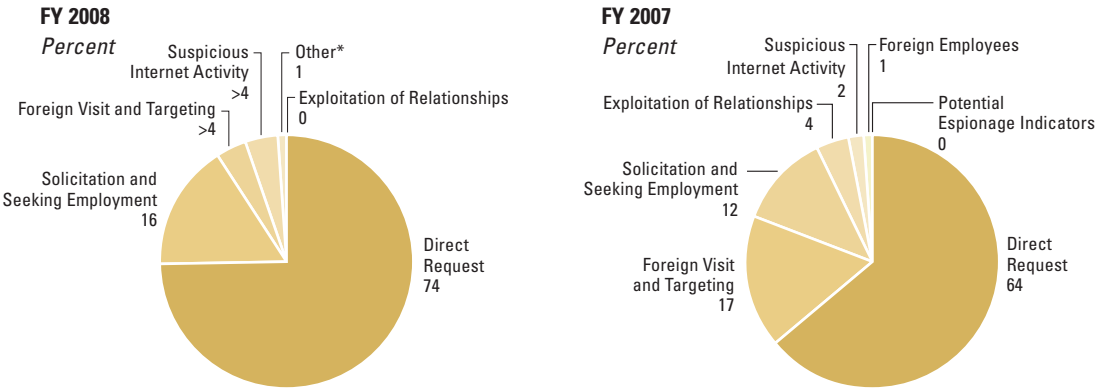
3. METHODS OF OPERATION

Near East entities continued to favor direct requests for information as the most common collection technique of choice, because of its low-risk, high-gain properties. Direct requests accounted for 74 percent of regional collection reports in FY08. Collectors also continued to use solicitation and seeking employment in their efforts to exploit cleared defense contractors (CDCs) for desired information. FY08 also saw a slight increase in the number of suspicious Internet activity incidents traceable to Near East entities. Although suspicious Internet activity incidents only accounted for less than five percent of all collection reports, this phenomenon mirrors rising cyber collection activities from other prolific regional collectors like East Asia and the Pacific and Europe and Eurasian collectors.

Analyst Comment: It is highly likely Near East collectors will continue to use direct request as their preferred method of operation (MO), but they will also use all available avenues of approach (like suspicious Internet activity) in their efforts to circumvent embargoes and target United States technology. This type of direct targeting increases the number of targets of opportunity and is likely to increase the success rate for acquiring sensitive, classified, and export-controlled United States technology. (Confidence Level: High)

METHODS OF OPERATION

FIGURE 9



* Includes foreign employees and potential espionage indicators

4. TARGETED TECHNOLOGIES

Near East entities continued to steadily target information systems technologies as related to command, control, communication, computers, intelligences, surveillance, and reconnaissance (C4ISR) programs, especially modeling and simulation systems. In a shift from previous years' reporting, attempts for lasers and optics technology increased to second place displacing reports for aeronautics technology. The specific technologies associated with lasers and optics were predominately optical software programs and unmanned aerial vehicle (UAV) targeting payloads. ***Analyst Comment: As defense industry continues to make advances in the laser and optical payloads for the aeronautics field, it is highly likely that entities will continue to pursue aggressive collection attempts on this area in order to develop indigenous UAVs with weapons delivery and targeting capabilities. (Confidence Level: High)***

Since 2003, the number of UAVs fielded in the Afghanistan and Iraq wars increased over five-fold, with a corresponding increase

TARGETED TECHNOLOGIES

TABLE 2

Developing Science and Technologies List (DSTL) Codes	FY 2008 Percent
Information Systems	28
Laser and Optics	> 23
Aeronautics	15
Sensors	7
Electronics	> 5
Positioning, Navigation, and Time	> 4
Marine Systems	3
Energy Systems	2
Armaments and Energetic Materials	2
Directed and Kinetic Energy	2
Chemical	1
Biological	1
Ground Systems	1
Manufacturing and Fabrication	1
Signature Control	1
Nuclear	1
Materials and Processing	1
Biomedical	0
Space Systems	0
Weapons Effects	0
Non-DSTL Technology	0

Developing Science and Technologies List (DSTL) Codes	FY 2007 Percent
Information Systems	23
Aeronautics	13
Sensors	8
Armaments and Energetic Materials	8
Electronics	6
Laser and Optics	6
Positioning, Navigation, and Time	5
Energy Systems	4
Manufacturing and Fabrication	4
Materials and Processing	4
Non-DSTL Technology	4
Biological	4
Marine Systems	2
Nuclear	2
Chemical	2
Signature Control	2
Space Systems	1
Ground Systems	1
Biomedical	1
Directed and Kinetic Energy	0
Weapons Effects	0

in suspicious entity interest. As UAV technology evolves with ever-increasing efficiency and effectiveness, the desire to obtain UAV emerging technologies, bundled-weapons platforms, and targeting platforms will also likely increase. Not to be overlooked, the wars in Iraq and Afghanistan also generated an increased focus on the acquisition of cutting edge technologies related to C4ISR programs, especially as they related to battlefield management capabilities.

5. ANALYTICAL FORECAST

Entities originating from the Near East region will likely continue to pursue United States technology and information in order to develop their own force multipliers as well as to improve existing technology. It is highly likely they will continue to use the direct request MO in their attempts to acquire sensitive United States technology. Furthermore, channeling commercial affiliated requests through third party nations is also likely to grow in an effort to avoid sanctions and trade restrictions. As this region becomes more volatile, it is highly likely entities will continue to focus their collection on dual-use technologies such as information systems, laser and optics, and aeronautics technology, especially in the areas of C4ISR systems and UAV payloads. (Confidence Level: High)

CASE STUDY

A CDC reported receiving a request for an unusual number of advanced maritime navigation devices from an individual using a northern European name and claiming to be a maritime project manager in southern Europe. While filling out a foreign sales approval form, the CDC sales representative noticed the caller ID on her phone listed the requester's phone number country code as a Middle Eastern country to which exports of these devices are prohibited. The sales representative immediately terminated the transaction and notified her Facility Security Officer.

The quick action on the part of the sales manager circumvented what was likely an attempt to divert controlled technologies to a prohibited end-user. This case illustrates the desire to acquire United States technology through a direct request sales call diverted through a third-party nation.


EUROPE
AND EURASIA

EUROPE AND EURASIA

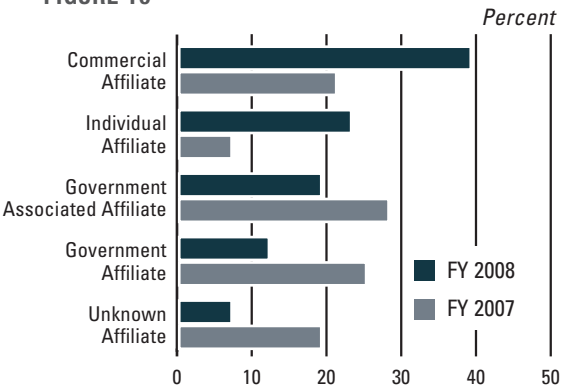
1. OVERVIEW

As has been the case since DSS began disseminating reports on foreign collection activities within defense industry, entities originating from the Europe and Eurasia region once again ranked among the top regional collectors of defense technology and information. Since fiscal year 2004 (FY04), collection attempts with a European/Eurasian nexus have remained relatively constant. However, in the last four years, collection activity recorded from this region continued to decline slightly, now representing only a 14 percent share of overall reporting in FY08. The reasons for this decline remain largely conjectural, but DSS analysis indicates European/Eurasian collection methods may not rely as much on the blatant, largely overt targeting utilized by East Asia and Pacific collectors.

Consistent with the overall trend of commercial companies and actors dominating collection attempts, FY08 defense industry reporting indicated European/Eurasian commercial entities were responsible for the majority of the targeting efforts originating from this region. Furthermore, commercial and government regional collectors continued to exploit direct requests for information as the predominant method of operation (MO) to procure United States defense technology. More than a quarter of these direct requests were especially for aeronautic technology, specifically unmanned aerial vehicle (UAV) components.

AFFILIATIONS

FIGURE 10



2. COLLECTOR AFFILIATIONS

In FY07, defense industry reporting indicated government-associated collectors were responsible for the majority of the targeting efforts. However in FY08, commercial targeting increased significantly from 21 percent to 39 percent. Additionally, over 70 percent of these commercial companies utilized email direct requests for nformation as a vehicle to contact defense industry personnel. ***Analyst Comment: This surge in commercial collection attempts is consistent with overall trends observed in other regions. It is highly likely this increase is attributable to entities deliberately attempting to shift their collection signature from governmental indicators to seemingly innocuous commercial associations. (Confidence Level: High)***

3. METHODS OF OPERATION

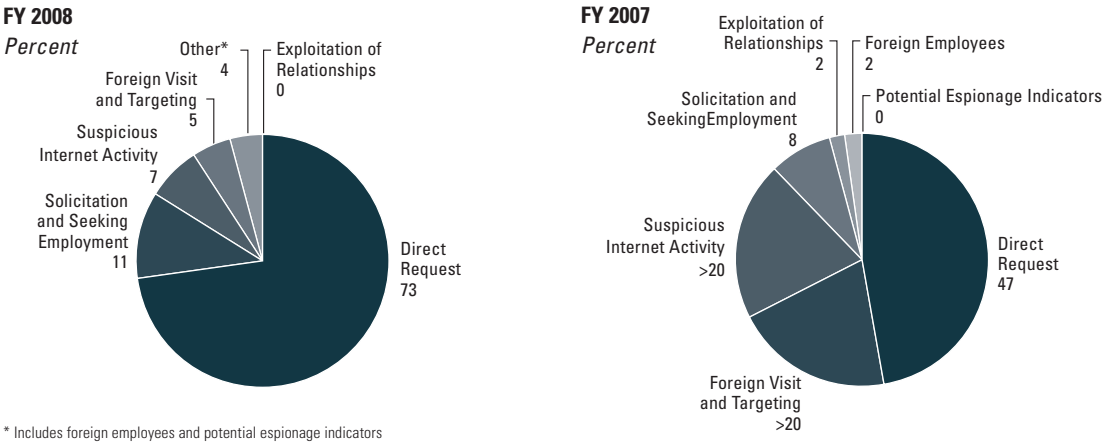
As in past years, the most frequently utilized European/Eurasian collection MO in FY08 remained direct request for information, now representing 73 percent of overall collection attempts, a dramatic increase from previous years. The combined categories of direct request and the second MO most frequently observed, solicitation and seeking employment, together accounted for over 80 percent of all reported incidents involving suspicious entities. These two methods to obtain United States technology dwarfed all other collection methods, and predominately targeted aeronautics and laser technology.

Analyst Comment: There is little indication that European/Eurasian actors are likely to change the manner of their principal overt collection efforts targeting industry. It is highly likely collectors from this region will continue to augment covert collections with relatively low-risk, high-gain requests for information, price quotes, or purchase requests via the Internet in a broadly-based effort to obtain access to sensitive information and technologies. (Confidence Level: High)

Not to be overlooked in FY08, the third most prolific MO, suspicious Internet activity, continued to play a role in European/Eurasian technology collection similar to targeting from the leading East Asia and Pacific cyber collectors. European/Eurasian cyber hosts frequently utilized intrusions and potential pre-attack targeting as cyber techniques. These cyber MOs were consistent with previous years' reporting concerning the use of socially engineered malicious emails and probe activity. (Note: Socially engineered emails, or "spear phishing" emails, are specially crafted emails designed to trick the recipient into opening a malicious attachment, possibly giving the intruder host or network access. Probe activity is likely indicative of cyber reconnaissance conducted against a victim network.)[5] ***Analyst Comment: Although the frequency of reported overt collection attempts declined from the Europe and***

METHODS OF OPERATION

FIGURE 11



* Includes foreign employees and potential espionage indicators

Eurasia region in FY08, it is likely suspicious actors working in or through this region sought other means of collection to offset traditional techniques. Cyber attacks on defense industry likely provide another avenue of approach to target critical information and technology. (Confidence Level: High)

4. TARGETED TECHNOLOGIES

Collectors from the Europe and Eurasia region continued to target essentially the same technologies they have since FY04, with only minor variations in collection priority. The most significant change in this reporting period was in the targeting of information systems technology. In previous years, information systems was the most targeted category with collectors primarily focused on encryption and modeling software; however in FY08, aeronautics technology moved into first place as the most commonly targeted technology with a focus on UAV components. European/ Eurasian entities sought all aspect of UAV technology ranging from complete systems, payloads, optics and sensors, to global positioning systems (GPS) in an effort to enhance return-to-home functions.

TARGETED TECHNOLOGIES

TABLE 3

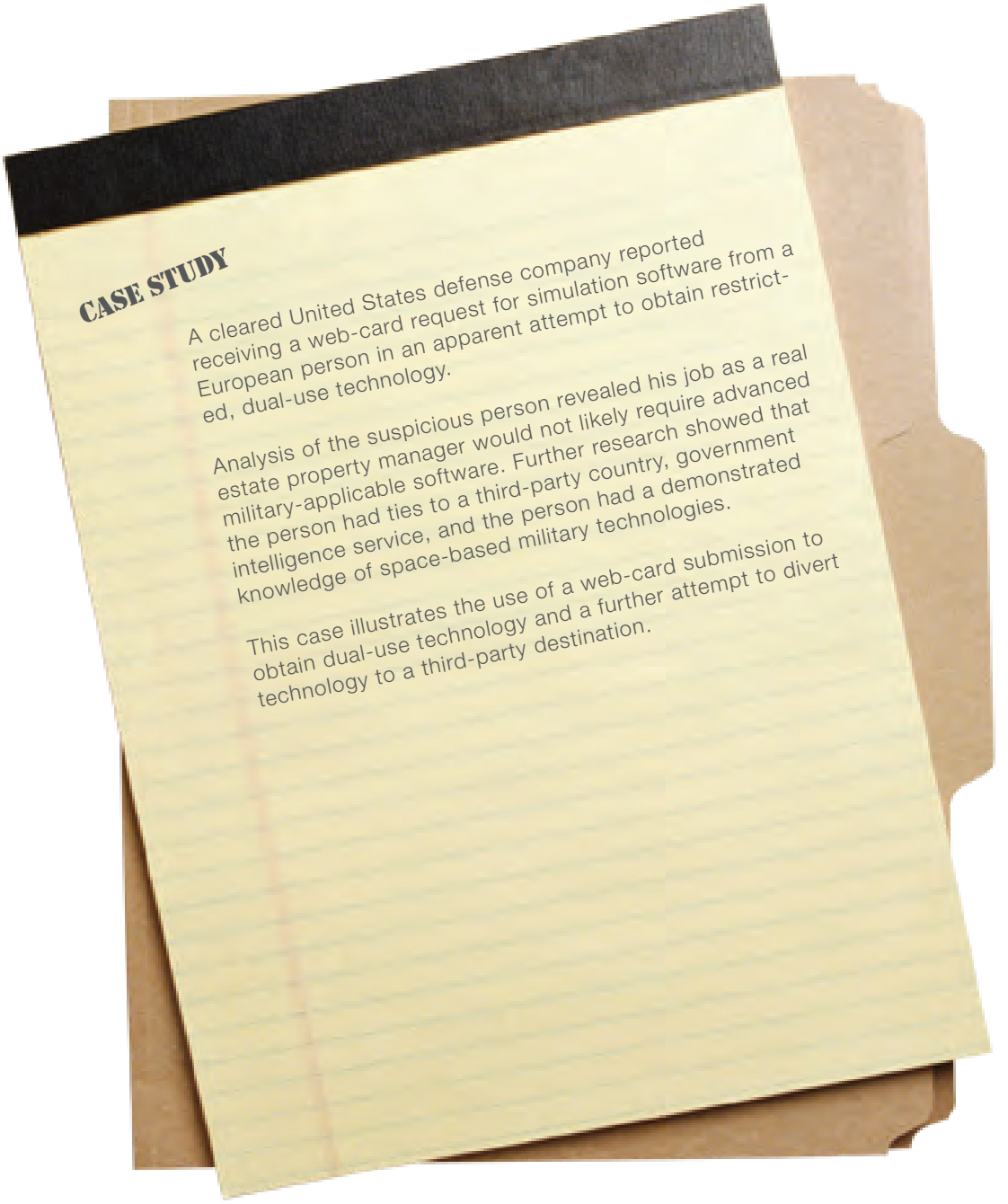
Developing Science and Technologies List (DSTL) Codes	FY 2008 Percent
Aeronautics	30
Information Systems	12
Laser and Optics	12
Marine Systems	> 9
Electronics	7
Sensors	7
Materials and Processing	> 5
Ground Systems	> 5
Positioning, Navigation, and Time	3
Weapons Effects	3
Manufacturing and Fabrication	1
Nuclear	1
Energy Systems	1
Space Systems	1
Non-DSTL Technology	1
Armaments and Energetic Materials	0
Biological	0
Biomedical	0
Chemical	0
Directed and Kinetic Energy	0
Signature Control	0

Developing Science and Technologies List (DSTL) Codes	FY 2007 Percent
Information Systems	35
Aeronautics	21
Armaments and Energetic Materials	8
Biological	6
Space Systems	6
Sensors	6
Electronics	> 4
Marine Systems	3
Laser and Optics	3
Manufacturing and Fabrication	3
Positioning, Navigation, and Time	2
Chemical	1
Ground Systems	1
Biomedical	0
Directed and Kinetic Energy	0
Energy Systems	0
Materials and Processing	0
Nuclear	0
Signature Control	0
Weapons Effects	0
Non-DSTL Technology	0

Analyst comment: It is likely entities originating from Europe and Eurasia increased aeronautics technology targeting with the intent to boost UAV production and focus on developing UAV technology. This collection priority is not likely to abate in the near future, given Europe and Eurasia's desire to enhance and continue development of their indigenous UAV programs. (Confidence Level: Moderate)

5. ANALYTICAL FORECAST

Despite a challenging economic environment, European/Eurasian entities will likely continue to pursue military modernization technologies and indigenous research and development competencies. The continued pursuit of dual-use technologies focused on UAV technological advancement will likely drive overall collection attempts in the next year. However, combined targeting of information systems and positioning, navigation, and time technology will also likely continue as a subset of aeronautics technology collection. The desire for technology components like GPS-aided inertial navigation system software, vehicle control programs, sensors, and radars may greatly enhance Europe and Eurasia's already burgeoning UAV program. It is highly likely these collectors will continue to focus on not only these payload technologies, but also on efforts to create smaller, rucksack-portable platforms. (Confidence Level: High)



CASE STUDY

A cleared United States defense company reported receiving a web-card request for simulation software from a European person in an apparent attempt to obtain restricted, dual-use technology.

Analysis of the suspicious person revealed his job as a real estate property manager would not likely require advanced military-applicable software. Further research showed that the person had ties to a third-party country, government intelligence service, and the person had a demonstrated knowledge of space-based military technologies.

This case illustrates the use of a web-card submission to obtain dual-use technology and a further attempt to divert technology to a third-party destination.


SOUTH AND
CENTRAL ASIA

SOUTH AND CENTRAL ASIA

1. OVERVIEW

Entities from or working through the South and Central Asia region generated the fourth largest number of collection attempts in fiscal year 2008 (FY08). Commercial affiliated collectors retained their status as most active pursuers of sensitive or restricted technology, while government and government affiliated collection methods were not as prolific. These collectors relied heavily on direct requests for information or technology as the preferred method of operation (MO), accounting for a staggering 79 percent of all suspicious incidents. These collection attempts effectively leveraged the Internet and email as relatively low-risk, high-gain methods of choice.

The primary technologies these entities sought included requests for aeronautics technology [unmanned aerial vehicles (UAVs)], information systems (encryption software), and sensors technology (radars), while previously dominant requests for laser and optics technologies took a back seat to UAV components and platforms.

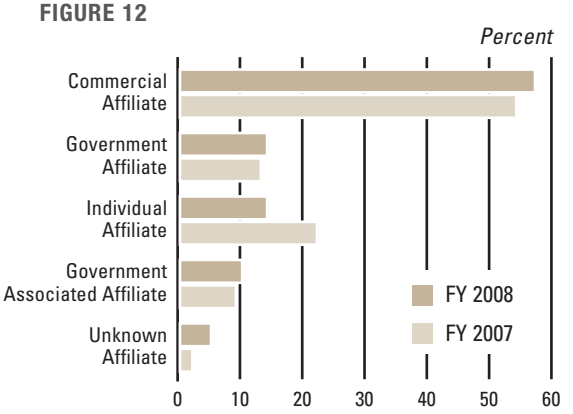
2. COLLECTOR AFFILIATIONS

As in FY07, commercial entities remained the most active collectors originating from South and Central Asia, comprising more than 50 percent of all reported incidents. Although commercial collection attempts dominated suspicious contact reporting, individual collectors continued their steady targeting of defense industry, tying with the slightly rising number of government collectors as the second most prolific collection category.

Analyst Comment: Defense industry reporting in FY08 confirms previous DSS assessments highlighting commercial entities as primary South and Central Asian collectors. The ever-expanding global marketplace and increased dependence on the Internet likely aids the dominance of commercial affiliates offering a low-risk, high-gain alternative to traditional collection methods.

AFFILIATIONS

FIGURE 12



Because of the opportunities the Internet affords commercial collectors, this tactic is not likely to abate in the near future. (Confidence Level: High)

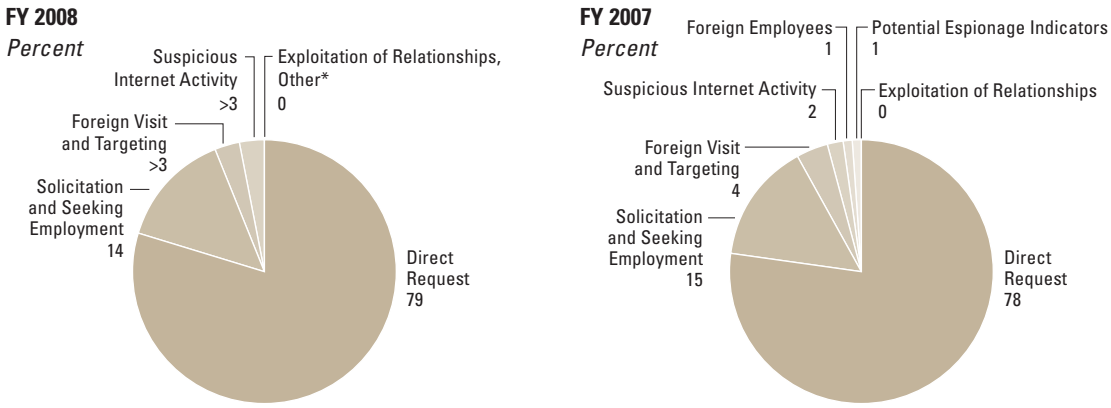
3. METHODS OF OPERATION

South and Central Asian entities continued to use direct requests for information as their primary means to target defense industry accounting for over 75 percent of collection attempts in FY08. Furthermore, the use of solicitation and seeking employment as a technique to acquire information or access was second only to the foreign visits and targeting method or tradecraft for suspicious incidents. These percentages remained relatively consistent with corresponding reporting from previous years.

Analyst Comment: In keeping with previous DSS assessments, entities from South and Central Asia prefer to utilize direct requests for information and the commercial sector to acquire United States technologies. It is highly likely this method is attributable to the cost effective nature of email and use of the Internet to maximize attempts and broaden business bases and clientele. (Confidence Level: High)

METHODS OF OPERATION

FIGURE 13



* Includes foreign employees and potential espionage indicators

4. TARGETED TECHNOLOGIES

In FY08, South and Central Asian entities focused primarily on aeronautics technology with emphasis on UAV related technologies. This targeted technology saw the largest increase in FY08 and coincides with the worldwide targeting of aeronautics and UAV systems. Not to be overlooked, information systems technology, emphasizing communications and encryption technology, also registered a small increase in collection attempts while requests for lasers and optics technology decreased.

Analyst comment: The decrease in laser and optics is likely related to the significant increase in aeronautics technology collection attempts. As the region's most prolific collector of UAV technologies, South and Central Asian entities have likely shifted focus to UAV platforms and payloads in an effort to develop indigenous UAV research and development programs and modernize military reconnaissance and surveillance equipment. (Confidence Level: Moderate)

TARGETED TECHNOLOGIES

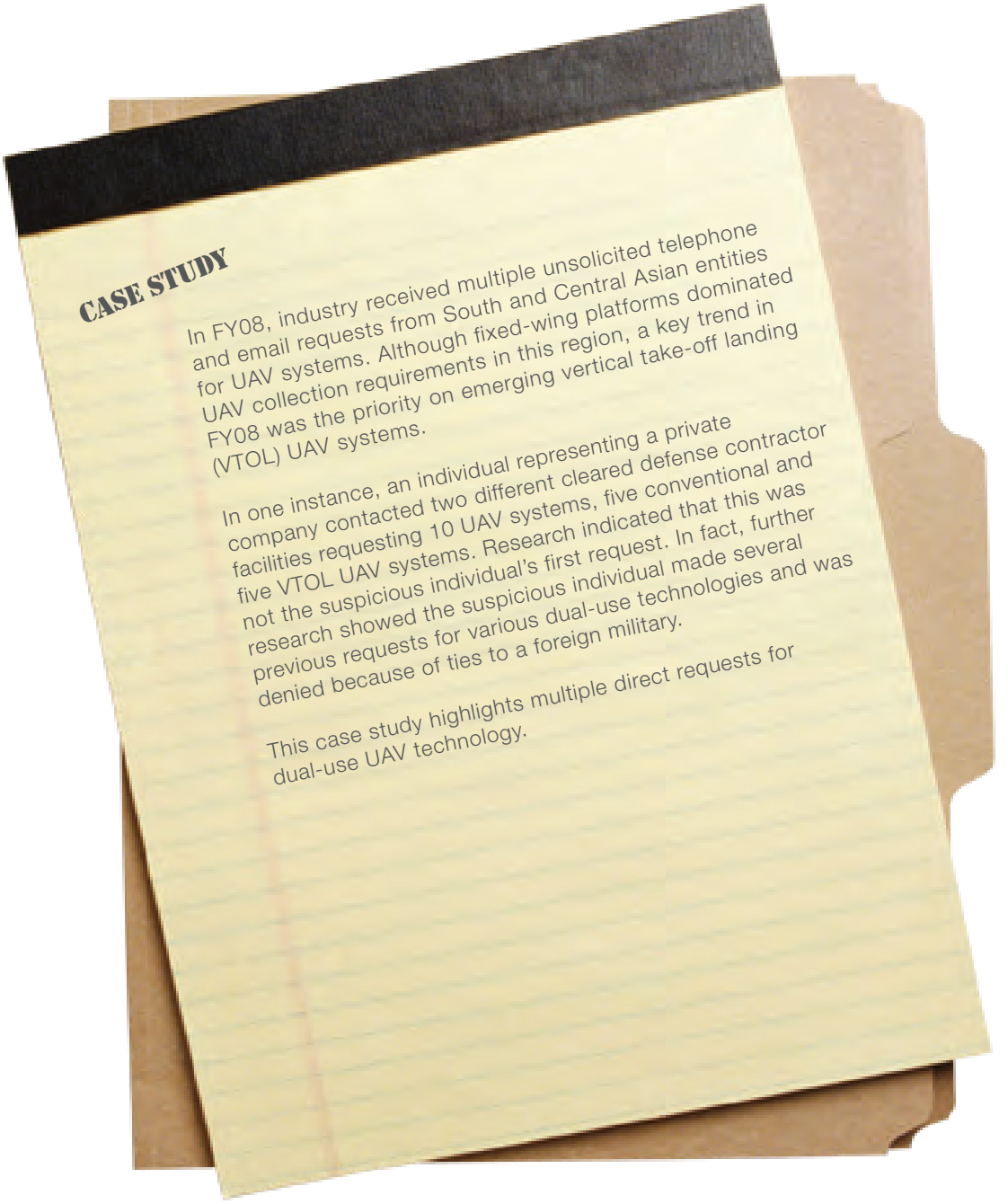
TABLE 4

Developing Science and Technologies List (DSTL) Codes	FY 2008 Percent
Aeronautics	38
Information Systems	24
Sensors	16
Space Systems	5
Marine Systems	5
Positioning, Navigation, and Time	> 3
Armaments and Energetic Materials	> 3
Electronics	> 3
Laser and Optics	2
Biological	0
Biomedical	0
Chemical	0
Directed and Kinetic Energy	0
Energy Systems	0
Ground Systems	0
Manufacturing and Fabrication	0
Materials and Processing	0
Nuclear	0
Signature Control	0
Weapons Effects	0
Non-DSTL Technology	0

Developing Science and Technologies List (DSTL) Codes	FY 2007 Percent
Information Systems	21
Sensors	14
Laser and Optics	14
Aeronautics	14
Space Systems	10
Electronics	7
Armaments and Energetic Materials	5
Manufacturing and Fabrication	4
Signature Control	2
Nuclear	2
Positioning, Navigation, and Time	2
Biological	2
Biomedical	2
Marine Systems	2
Ground Systems	1
Materials and Processing	1
Directed and Kinetic Energy	0
Chemical	0
Energy Systems	0
Weapons Effects	0
Non-DSTL Technology	0

5. ANALYTICAL FORECAST

As foreign reliance on contractual procurement firms to acquire United States technology continues, commercial entities are likely to maintain their position as the primary collector of dual-use technology in the South and Central Asia region. Furthermore, as countries within the South and Central Asia region desire to modernize their military equipment and deter perceived threats from various adversaries, this aggressive posture will likely drive future collection and targeting attempts. Interest in UAV technology and sophisticated airborne applications will likely continue in an effort to develop and improve current military forces in the event of any future regional hostilities. (Confidence Level: Moderate)



CASE STUDY

In FY08, industry received multiple unsolicited telephone and email requests from South and Central Asian entities for UAV systems. Although fixed-wing platforms dominated UAV collection requirements in this region, a key trend in FY08 was the priority on emerging vertical take-off landing (VTOL) UAV systems.

In one instance, an individual representing a private company contacted two different cleared defense contractor facilities requesting 10 UAV systems, five conventional and five VTOL UAV systems. Research indicated that this was not the suspicious individual's first request. In fact, further research showed the suspicious individual made several previous requests for various dual-use technologies and was denied because of ties to a foreign military.

This case study highlights multiple direct requests for dual-use UAV technology.

CONCLUSION

The targeting of U.S. technologies resident in defense industry remains intense and broadly-based. However, DSS analysis of fiscal year 2008 (FY08) defense industry reporting showed no significant changes from FY07 in terms of the traditional regional actors making requests, the methods of operation (MOs) they used, their affiliations, or the specific technologies being targeted.

The East Asia and Pacific region retained its status as the dominant region of origin for most collection efforts against United States technologies. Near East collectors continued their pursuit of dual-use technologies, maintaining their position as the second most prolific regional collector. Europe and Eurasia regional collectors, as well as those in the South and Central Asia region, continued as significant players; however, requests from collectors with a Europe and Eurasia nexus remained somewhat of an anomaly, steadily decreasing in volume relative to trends noted in previous years. As predicted in the previous "Targeting U.S. Technologies" report, these persistent regional collectors increased their targeting of aeronautics technology, specifically, UAV-related components, allowing that category to slowly gain momentum behind requests for the most frequently targeted discipline, information systems technology.

The direct request MO continued to be the dominant method of choice for suspicious collectors and continued to provide the greatest return for minimal investment and risk. While not all direct requests for information represent organized collection attempts, exploitation of this medium facilitated the ease with which foreign entities utilized all available approaches to gain technology or information. In FY08, regional collectors further exploited the Internet, not only making direct requests for information by email, but also through electronic attacks targeting defense industry information networks. Suspicious Internet activity with IP addresses originating in the East Asia and the Pacific region represented 79 percent of the regional cyber collection effort, a significant increase over last year's 52 percent. These apparent cyber operations mainly targeted cleared defense contractor networks used for research and development documentation, especially those related to information systems technology.

The trend to use non-government affiliated commercial surrogates as collectors to diffuse suspicions continued in FY08. Defense industry reporting indicated that state-actors from the East Asia and Pacific and Near East regions utilized both authentic commercial entities as well as illicit front companies in attempts to acquire controlled technologies. Meanwhile, South and Central Asian collectors remained more inclined to use less-traditional collectors, such as students, to gain access to restricted United States technology. This multi-dimensional threat environment will continue to require innovative and proactive countermeasures on the part of security personnel and cleared contractors acting in a concerted team effort to protect United States technology and information.

FORECAST

The rapid globalization of world economies, including defense-related industrial sectors, will drive an unprecedented degree of interface between United States industry and foreign entities eager for information and technologies resident in defense industry. Imperatives for emerging third-world countries to possess viable military and technical competencies will result in a spiraling demand for information and technology promising a competitive advantage. Cleared defense contractors (CDCs) in the United States will almost certainly remain a primary focus of foreign collection efforts, as foreign entities seek immediate competencies with minimal investment in their own indigenous programs. Additionally, The Unites States' traditional geopolitical and military rivals, as well as emerging strategic adversaries, place sensitive information in the United States defense industry at continued risk.

Defense industry reporting indicates suspicious entities will continue to target the vast spectrum of defense contractor information and technology. Information systems technology, particularly command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems with modeling and simulation programs, will likely remain priority technology targets for all regions. Aeronautics-related technologies, particularly advanced unmanned aerial vehicle (UAV) systems, are also expected to remain a major focus for all the foreign technology collectors. Missile and missile defense technologies, including sensor systems, will continue to be collection priorities for Europe, Eurasia, and Near East entities. In addition, lasers and optics; marine systems (advanced naval systems); and positioning, navigation, and time technologies (global positioning systems) will continue to be a focus for East Asia and Pacific collectors.

In the last few years, DSS analysis of industry reporting identified a rising trend of suspicious attempts for aeronautics-related technologies, specifically UAV components and systems. As a result of the global marketplace, the expansive nature of the Internet, and ease of acquiring commercial-off-the-shelf components, the desire for cutting-edge UAV information and technology is not likely to abate in the near future. As major developers of UAV technologies, defense industry should be cognizant of attempts to gain information about UAV technologies, as aeronautics technologies will likely continue as premier targets of foreign collection.

Government and commercial collection entities worldwide are highly likely to continue the use of cyber collection activities against United States government and its CDCs. Cyber intrusion offers a relatively low-risk, high-gain technique giving illicit collectors the opportunity to acquire sensitive and proprietary information stored on United States computer networks. Cyber targeting may also be utilized as a collection planning tool to identify targets of opportunity not readily apparent to traditional collectors. This cyber reconnaissance allows foreign elements to design targeting plans employing the full range of collection techniques on focused targets.

Because of the cutting-edge technical advancements they represent, the United States' dual-use technologies are expected to generate sustained interest, irrespective of whether the collector has any actual interest in the specific commercial or military

applications. Foreign commercial entities and joint enterprises will continue to complicate defense industry's ability to distinguish between legitimate global business practices and illicit attempts to acquire United States technologies. As always, this multi-dimensional threat environment will continue to require a concerted team effort between cleared contractors and security professionals to develop innovative and pro-active countermeasures to secure the integrity of information and technology in the defense industrial base. (Confidence Level: High)

This page intentionally left blank.

APPENDIX / REFERENCES

[1] MCIA; MCIA-1361-001-00; OCT 2000; Unmanned Aerial Vehicle Recognition Guide; (U// FOUO); p.5; (U//FOUO); Ref 13 MAY 2009

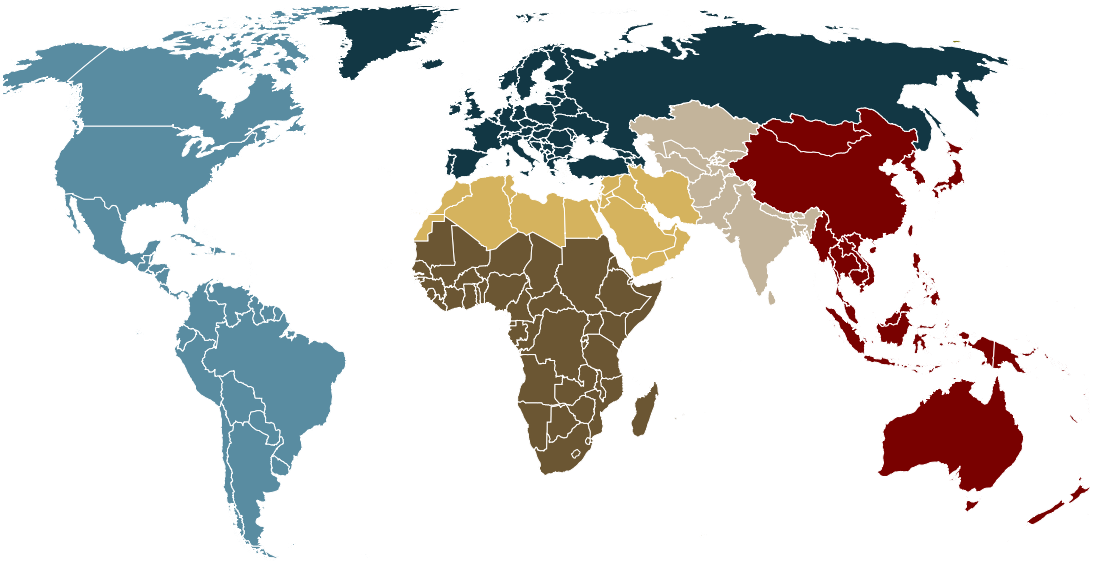
[2] Airframer.com. (2008, July). UAV Flies Successfully in Arctic Circle. http://www.airframer.com/journal_story.html?story=9244

[3] United States Attorney's Office; 2009; The Court Report Press Release; retrieved from the Department of Justice: http://usdoj.gov/usao/dc//community_prosecution/court_reports/feb09/id/1d_final_february_court_report.pdf

[4] Department of Justice Press Release. (2008, September 3). Retired University of Tennessee Professor Convicted of Arms Export Violations. http://www.usdoj.gov/opa/pr/2008/september/08-nsd-774.html. Case # 09-775

[5] Internet; Microsoft; Spear Phishing: Highly Targeted Scams; 18 SEP 2006

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	Finland	Saudi Arabia		Cuba
Eritrea	Mongolia	France	Syria		Dominica
Ethiopia	Nauru	Georgia	Tunisia		Dominican Republic
Gabon	New Zealand	Germany	United Arab Emirates		Ecuador
Gambia, The	Palau	Greece	Yemen		El Salvador
Ghana	Papua New Guinea	Greenland			Grenada
Guinea	Philippines	Holy See			Guatemala
Guinea-Bissau	Samoa	Hungary			Guyana
Kenya	Singapore	Iceland			Haiti
Lesotho	Solomon Islands	Ireland			Honduras
Liberia	Taiwan	Italy			Jamaica
Madagascar	Thailand	Kosovo			Mexico
Malawi	Timor-Leste	Latvia			Netherlands Antilles
Mali	Tonga	Liechtenstein			Nicaragua
Mauritania	Tuvalu	Lithuania			Panama
Mauritius	Vanuatu	Luxembourg			Paraguay
Mozambique	Vietnam	Macedonia			Peru
Namibia		Malta			St. Kitts and Nevis
Niger		Moldova			St. Lucia
Nigeria		Monaco			St. Vincent and the Grenadines
Rwanda		Montenegro			Suriname
Sao Tome and Principe		Netherlands			Trinidad and Tobago
Senegal		Norway			United States
Seychelles		Poland			Uruguay
Sierra Leone		Portugal			Venezuela
Somalia		Romania			
South Africa		Russia			
Sudan		San Marino			
Swaziland		Serbia			
Tanzania		Slovakia			
Togo		Slovenia			
Uganda		Spain			
Zambia		Sweden			
Zimbabwe		Switzerland			
		Turkey			
		Ukraine			
		United Kingdom			

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

This page intentionally left blank.


DEFENCE SECURITY SERVICE