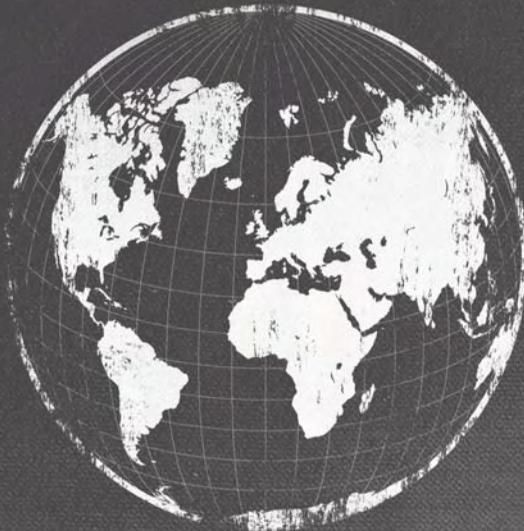


TARGETING U.S. TECHNOLOGIES:

A TREND ANALYSIS OF REPORTING
FROM DEFENSE INDUSTRY

2011

YEAR





Produced by the Defense Security Service
Counterintelligence Directorate
www.DSS.mil

EXTERNAL COORDINATION

ACIC, CIA, DIA, DOE, NCIS, NGA, ONCIX

CONTRIBUTORS

Robert Ayer, Tom Badoud, Jeff Burlette, Frank Carapezza, Hillary Clark, Kathryn Cubbon, Bryan Galloway, Mike Houlihan, Camille Johnson, Rich Mickle, Chad Pierce, Traci Rivera, Jessica Rocha, Bob Sirks, Luke Sjerven, John Stevenson, Laresa Walter, Joel West, Brett Young

TARGETING U.S. TECHNOLOGIES:

A TREND ANALYSIS OF REPORTING
FROM DEFENSE INDUSTRY

2011
YEAR

TABLE OF CONTENTS

5	PREFACE
6	BACKGROUND
9	EXECUTIVE SUMMARY
15	SPECIAL FOCUS AREA: AUTONOMOUS UNDERWATER VEHICLES
23	REGIONS
23	EAST ASIA AND THE PACIFIC
35	NEAR EAST
47	EUROPE AND EURASIA
57	SOUTH AND CENTRAL ASIA
68	OTHER REGIONS
69	CONCLUSION
71	ANALYTICAL FORECAST
73	ABBREVIATIONS / ACRONYMS
74	REFERENCE MAP
75	REFERENCES



TABLES & FIGURES

TABLES

EAST ASIA AND THE PACIFIC

30 TABLE 1: TARGETED TECHNOLOGIES

NEAR EAST

42 TABLE 2: TARGETED TECHNOLOGIES

EUROPE AND EURASIA

53 TABLE 3: TARGETED TECHNOLOGIES

SOUTH AND CENTRAL ASIA

64 TABLE 4: TARGETED TECHNOLOGIES

FIGURES

EXECUTIVE SUMMARY

9 FIGURE 1: REGION TRENDS

10 FIGURE 2: COLLECTOR AFFILIATIONS

11 FIGURE 3: METHODS OF OPERATION

12 FIGURE 4: TARGETED TECHNOLOGIES

SPECIAL FOCUS AREA: AUTONOMOUS UNDERWATER VEHICLES

17 FIGURE 5: TOP REGIONS TARGETING AUTONOMOUS UNDERWATER VEHICLES

EAST ASIA AND THE PACIFIC

25 FIGURE 6: COLLECTOR AFFILIATIONS

27 FIGURE 7: METHODS OF OPERATION

NEAR EAST

37 FIGURE 8: COLLECTOR AFFILIATIONS

39 FIGURE 9: METHODS OF OPERATION

EUROPE AND EURASIA

49 FIGURE 10: COLLECTOR AFFILIATIONS

50 FIGURE 11: METHODS OF OPERATION

SOUTH AND CENTRAL ASIA

59 FIGURE 12: COLLECTOR AFFILIATIONS

62 FIGURE 13: METHODS OF OPERATION

IN THE INTERESTS OF READABILITY AND 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 SECTION.

THIS PAGE INTENTIONALLY LEFT BLANK

PREFACE

“Eternal vigilance is the price of liberty.” This quotation, attributed to John Philpot Curran in Dublin, Ireland, in 1790, is equally applicable to the United States in the present era. Every day, foreign entities attempt to break through our collective defenses to illegally acquire U.S. technological secrets. Our national security rests on our collective success at thwarting these persistent attacks.

The stakes are high in the battle against foreign collection and espionage targeting U.S. technology, trade secrets, and proprietary information. Not only is our national security at risk but also our technological edge, which is closely tied to the health of our economy and the economic success of the cleared contractor community. Most importantly, every time our adversaries gain access to restricted information it jeopardizes the lives of our warfighters, since those adversaries can use the information to develop more lethal weapons or countermeasures to our systems.

Preventing such loss is a team effort. The Defense Security Service (DSS) supports national security by overseeing the protection of the nation’s technological base and both U.S. and foreign classified information in the hands of cleared industry. The DSS Counterintelligence Directorate seeks to identify and stop those who would unlawfully penetrate our defenses. In this mission, DSS relies on the support of cleared contractor employees and the U.S. intelligence and law enforcement communities.

The *National Industrial Security Program Operating Manual* requires cleared contractors to provide information concerning actual, probable, or possible espionage, sabotage, or terrorism. After cleared contractors report any suspicious contacts or efforts to obtain illegal or unauthorized access to restricted information or subversion activities, DSS reviews these reports and refers further cases of actionable information to partners in the law enforcement and intelligence communities for potential exploitation or neutralization.

DSS also uses these suspicious contact reports (SCRs) to develop analytical assessments to articulate the threat to U.S. information and

technology resident in cleared industry. This publication, *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry*, presents the annual statistical analysis of those SCRs. The information contained in this publication helps employees, companies, and intelligence and law enforcement professionals better understand the continuing yet changing nature of the threats we face. Increased awareness of the targeted technologies and the methods of operation that foreign entities use in their attempts to acquire U.S. technologies will only make us better at identifying and thwarting their efforts.

Like any publication, this one is only as good as the information that goes into it. The SCRs DSS analyzes originate with cleared contractor employees. Timely and accurate reporting of illicit collection attempts are the foundation upon which this process rests. Thus, the cleared contractor community is both a supplier to and a customer of DSS. This long-standing and interdependent relationship functions best when both partners understand all stakeholders’ needs, build strong relationships on the basis of trust, and interact with each other in a cooperative fashion.

The process that begins with reporting and continues with ongoing and collective analysis reaches its ultimate stage in successful investigations or operations. In fiscal year 2010, federal investigative or intelligence agencies opened more than 200 operations or investigations based on information that industry provided to DSS. These foreign collectors were identified, isolated, diverted, or otherwise thwarted.

But it can’t happen without you. It depends on all of us doing our part, every day. “Eternal vigilance is the price of liberty.”



Stanley L. Sims
Director
Defense Security Service

BACKGROUND

Department of Defense (DoD) Instruction 5200.39, dated July 16, 2008, requires the Defense Security Service (DSS) to publish a classified report detailing suspicious contacts occurring within the cleared contractor community. DSS focuses on indications of threats to compromise or exploit cleared personnel, or to obtain illegal or unauthorized access to sensitive or classified information or technologies resident in the U.S. cleared industrial base. DSS also releases this unclassified version of the report.

The instruction requires DSS to provide these reports to the DoD Counterintelligence (CI) community, national entities, and the cleared contractor community. DSS seeks to assist in raising general threat awareness, identifying specific technologies at risk, and applying appropriate countermeasures. DSS receives and analyzes suspicious contact reports (SCRs) from cleared contractors in accordance with reporting requirements defined in Chapter 1, Section 3 of the *National Industrial Security Program Operating Manual*, 5220.22-M, dated February 28, 2006. The analysis of these SCRs forms the basis for this year's report.

The information in this report covers the most prolific foreign collectors targeting the cleared contractor community during fiscal year 2010 (FY10) as compared to the previous fiscal year. The report covers

statistical and trend analysis on foreign collector affiliations, the methods foreign entities used to target the cleared contractor community, and the specific technology sectors targeted. Each section also contains a forecast of potential future activities against the cleared contractor community, based on analytical assessments.

DSS publishes *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry* as part of its 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. DSS intends the report to be a ready reference tool for security professionals in their efforts to detect, deter, mitigate, or neutralize the effects of foreign targeting.

This year, the report also highlights foreign attempts at acquiring autonomous underwater vehicle (AUV) technology from U.S. cleared industry. DSS selected this specific technology subset because reports and analysis indicate it is a growing collection area. The section provides a definition of AUV technology and analysis on reporting from cleared industry, including collector methodology.

1. SCOPE/METHODOLOGY

DSS provides statistical and trend analysis on the foreign entity threat posed to the cleared contractor community over the past fiscal year as compared to the previous year. DSS bases this report primarily on SCRs collected from the cleared contractor community, but also relies on some all-source Intelligence Community (IC) reporting.

DSS now analyzes foreign interest in U.S. defense technology in terms of the 20 categories in the Militarily Critical Technologies List (MCTL), instead of the Developing Science and Technology List used previously. The MCTL is a compendium of those science and technology capabilities existing or under development worldwide that may significantly enhance or degrade U.S. military capabilities now or in the future. It provides categories and subcategories for DSS to use in identifying and defining targeted technologies.

In addition, this publication makes occasional reference to the Department of Commerce's Entity List. This listing provides public notice that certain exports, re-exports, and transfers (in-country) to entities included on the Entity List require a license from the Bureau of Industry and Security. An End-User Review committee

(ERC) reviews and makes changes to the list annually. The ERC includes representatives from the Departments of Commerce, Defense, Energy, and State, and, when appropriate, Treasury.

DSS analysts scrutinize each SCR, examining the critical U.S. technology, the targeting entity, the method of operation, the relationships to previous reporting from the cleared contractor community, and all-source IC information.

2. EXPLANATION OF ESTIMATIVE LANGUAGE AND ANALYTIC CONFIDENCE

DSS uses the IC estimative language standard. The language used—phrases such as “we judge,” “we assess,” or “we estimate,” and terms such as “likely” or “indicate”—represents DSS's effort to convey a particular analytical assessment or judgment.

Because DSS bases these assessments on incomplete and at times fragmentary information, they do not constitute facts nor provide proof; they do not 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, the agency may 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 approximate level of probability of a development, event, or trend. Assigning precise numerical ratings to such judgments would imply more rigor than the agency intends. The chart below provides a depiction of the relationship of terms to each other.



The report uses “probably” and “likely” to indicate that there is a greater than even chance of an event happening. It uses phrases such as “we cannot dismiss,” “we cannot rule out,” and “we cannot discount” in cases when events are unlikely or even remote, but their consequences would be such that they warrant mentioning. Even when the authors use the terms “remote” and “unlikely,” they do not intend to imply that an event will not happen.

DSS uses words such as “may” and “suggest” to reflect situations in which DSS is unable to assess the likelihood of an event at all, generally because relevant information is sketchy, fragmented, or nonexistent.

In addition to using words within a judgment to convey degrees of likelihood, DSS also assigns analytic confidence levels based on the scope and quality of information supporting DSS judgments:

HIGH CONFIDENCE

- Well-corroborated information from proven sources, minimal assumptions, and/or strong logical inferences.
- Generally indicates that DSS based judgments on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment.

MODERATE CONFIDENCE

- Partially corroborated information from good sources, several assumptions, and/or a mix of strong and weak inferences.
- Generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

LOW CONFIDENCE

- Uncorroborated information from good or marginal sources, many assumptions, and/or mostly weak inferences.
- Generally means that the information’s credibility or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that we have significant concerns or problems with the sources.

EXECUTIVE SUMMARY

Each region covered in this volume is significantly diverse. Thus, even as the Defense Security Service (DSS) categorizes its observations based on the geographical area the contact initiated from, each region includes countries that are large or small, advanced or developing in economy, rising or static in regional and world impact, and active or inactive in collecting tendencies. Each region contains aspiring regional powers, if not world-level players, in various categories of achievement. And some of the most active collectors within particular regions consider themselves to be sworn enemies of each other. Each of these factors can serve as a spur to collection efforts aimed at U.S. technology, and can complicate efforts to understand the motivations behind those efforts.

The number of suspicious contact reports (SCRs) resulting from foreign attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base more than doubled from fiscal year 2009 (FY09) to FY10. The large scope and diversity of collection efforts targeting U.S. technologies meant that foreign entities simultaneously directed considerable efforts at many technologies using variations of methods and collectors.

REGIONAL TRENDS

FIGURE 1



However, there were some patterns and consistencies within the data. Analysis by DSS of these SCRs shows both continuities with and changes from previous years' reporting. Overall, the majority of collection attempts in FY10 originated from the East Asia and the Pacific region; *commercial* entities were the most active collector affiliation category for the second year in a row; targeting of *information systems (IS)* technology more than doubled from FY09; and collectors continued to most commonly use *requests for information (RFIs)* to elicit information from cleared contractors.

Even as the total SCRs from industry more than doubled from FY09 to FY10, the East Asian and Pacific region accounted for an even larger percentage of the total in FY10, increasing from 36 percent to 43 percent. East Asia and the Pacific accounted for as much of the total as the next three regions combined. Despite the dramatic increase in the number of reported cases attributed to the second most active region, the Near East, its share of the total actually declined slightly, due to the even greater increase in incidents attributable to East Asia and the Pacific.

As with the East Asia and the Pacific and Near East regions, Europe and Eurasia's reported collection attempts more than doubled from last year, causing it to displace South and Central Asia as the third most active collector region. Together, East Asia and the Pacific, the Near East, and Europe and Eurasia accounted for over three-quarters of the world-wide total reported collection attempts against the U.S. cleared industrial base.

Nonetheless, South and Central Asia remained an active collecting region. It registered a 50 percent increase in reported attempts over the last year, although its share of the total reports decreased.

While *commercial* entities maintained their place as the most active collectors, at 35 percent of the total, that marked a decrease in share from almost half of the total in FY09, and those identified as *government* collectors fell to 11 percent. The other three categories—*unknown*, *government affiliated*, and *individual*—all correspondingly increased their shares. The *commercial* collector affiliation retained its primacy in all regions, but only in South and Central Asia did it do so unchallenged.

COLLECTOR AFFILIATIONS

FIGURE 2

COMMERCIAL

Entities whose span of business includes the defense sector



GOVERNMENT AFFILIATED

Research institutes, laboratories, universities, or contractors funded by, representing, or otherwise operating in cooperation with a foreign government agency, whose shared purposes may include acquiring access to U.S. sensitive, classified, or export-controlled information



INDIVIDUAL

Persons who, for financial gain or ostensibly for academic or research purposes, seek to acquire access to U.S. sensitive, classified, or export-controlled information or technology, or the means of transferring it out of the country



GOVERNMENT

Ministries of Defense and branches of the military, as well as foreign military attachés, foreign liaison officers, and the like



UNKNOWN

Instances in which no attribution of a contact to a specific end user could be directly made



As in previous years, the *RFI* remained the most common method of operation (MO), accounting for almost half of all reported attempts, more than doubling the next closest MO, *suspicious network activity (SNA)*. Despite the dramatic lead, the percentage of SCRs reporting *RFIs* decreased significantly since FY09. In East Asia and the Pacific and Europe and Eurasia, *SNA* continued to increase significantly both in numbers of reports and in percentage of the total.

METHODS OF OPERATION

FIGURE 3

REQUESTS FOR INFORMATION

Via phone, email, or webcard approaches, these are attempts to collect protected information under the guise of price quote or purchase requests, marketing surveys, or other direct and indirect efforts



SUSPICIOUS NETWORK ACTIVITY

Via cyber intrusion, viruses, malware, backdoor attacks, acquisition of user names and passwords, and similar targeting, these are attempts to carry out intrusions into cleared contractor networks and exfiltrate protected information



SOLICITATION OR MARKETING

Via sales, representation, or agency offers, or response to tenders for technical or business services, these are attempts by foreign entities to establish a connection with a cleared contractor vulnerable to the extraction of protected information



ACADEMIC SOLICITATION

Via requests for or arrangement of peer or scientific board reviews of academic papers or presentations, or requests to study or consult with faculty members, or applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees



EXPLOITATION OF RELATIONSHIPS

Via establishing connections such as joint ventures, official agreements, foreign military sales, business arrangements, or cultural commonality, these are attempts to play upon existing legitimate or ostensibly innocuous relationships



CONFERENCES, CONVENTIONS, AND TRADE SHOWS

This refers to suspicious activity at such events—especially those involving dual-use or sensitive technologies that involve protected information—such as taking of photographs, making sketches, or asking of detailed technical questions



OFFICIAL FOREIGN VISITS AND TARGETING

Via visits to cleared contractor facilities that are either pre-arranged by foreign contingents or unannounced, these are attempts to gain access to and collect protected information that goes beyond that permitted and intended for sharing to gain unauthorized access



SEEKING EMPLOYMENT

Via resumé submissions, applications, and references, these are attempts to introduce persons who, wittingly or unwittingly, will thereby gain access to protected information which could prove useful to agencies of a foreign government



TARGETING U.S. TRAVELERS OVERSEAS

Via airport searches, hotel room incursions, computer/device accessing, telephone monitoring, personal interchange, and the like, these are attempts to gain access to protected information through the presence of cleared contractor employees traveling abroad as a result of invitations and/or payment to attend seminars, provide training, deliver speeches, and the like



CRIMINAL ACTIVITIES

Via theft, these are attempts to acquire protected information with no pretense or plausibility of legitimate acquisition



ATTEMPTED ACQUISITION OF TECHNOLOGY

Via direct purchase of firms or the agency of front companies or third countries, these are attempts to acquire protected information in the form of controlled technologies, whether the equipment itself or diagrams, schematics, plans, spec sheets, or the like

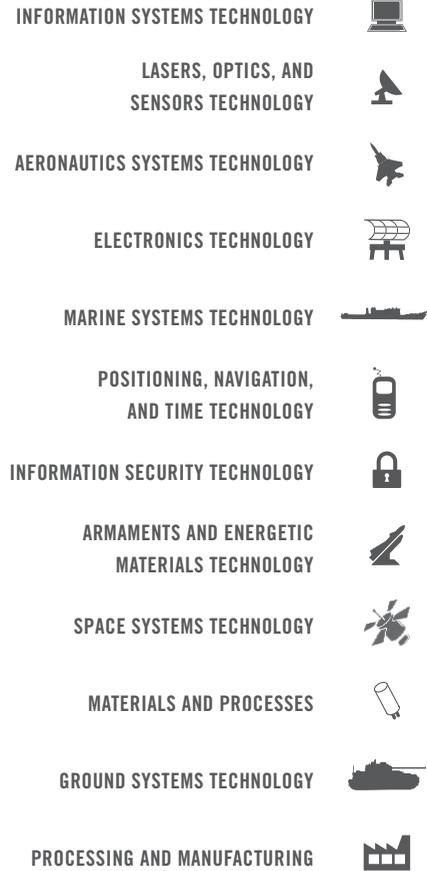


IS remained the most sought after technology category. *Lasers, optics, and sensors*, which had surged in the statistics as a collection target in FY09, settled in at second place in FY10, with *aeronautics systems* and *electronics technologies* rounding out the usual top four categories. The regions spread their collection efforts over a wider range of technologies in FY10, as represented by SCRs.

This volume includes a special focus area on autonomous underwater vehicles (AUVs) due to the FY10 reporting, which noted a rising interest among each of the regions.

TOP TARGETED TECHNOLOGY

FIGURE 4



KEY FINDINGS

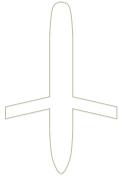
- East Asia and the Pacific remains by far the most active collecting region, making the most attempts at collecting U.S. information and technology by an increasingly wide range of methods. This region has a bold and aggressive agenda and conducts multifaceted, pervasive, and innovative collection efforts.
- All regions use the collection entities and methodologies they consider most likely to yield the desired results. While all regions rely on *commercial* agents, the U.S. cleared industrial base finds itself confronted with *government*, *government-affiliated*, *individual*, and unidentified collectors, each of which provide collecting regions with advantages in particular contexts.
- Collection MOs continue to span the range between the direct, immediate, and seemingly legitimate, such as *RFIs*; to the more indirect, more long-term, and more opaque, such as *academic solicitation*, *seeking employment*, and *solicitation or marketing*; to the often obscure *SNA* that seeks to penetrate U.S. industry networks.
- Often, regions do not discriminate between desired technological information and available information; but rising technologies—as measured either by level of development reached by the technology or by level of interest demonstrated by regional or world rivals—continue to attract special attention, with AUVs of particular interest in FY10.

THIS PAGE INTENTIONALLY LEFT BLANK

(U) SPECIAL FOCUS AREA:
AUTONOMOUS
UNDERWATER
VEHICLE
TECHNOLOGIES



SPECIAL FOCUS AREA: TARGETING AUTONOMOUS UNDERWATER VEHICLE TECHNOLOGIES



1. OVERVIEW

Autonomous underwater vehicles (AUVs) are a class of underwater vessels capable of submerged, self-propelled locomotion using various enabling technologies to navigate and perform diverse tasks.

AUVs have a variety of military and commercial uses. The U.S. Navy identifies nine areas for its AUV programs: intelligence, surveillance and reconnaissance (ISR); mine counter measures (MCM); anti-submarine warfare (ASW); inspection and identification; oceanography; communication/navigation network node; payload delivery; information operation; and time-critical strike.¹

Commercial applications include underwater surveys, fisheries research, search and recovery, wreck and navigational hazard mapping, and water profile sampling.

Many AUVs can be configured for a variety of underwater missions, and some commercial and military missions are similar in nature. AUVs provide navies with a cost-effective way to modernize their ability to affect underwater battlespace and protect key ports and installations.

The Defense Security Service (DSS) intends this special focus area assessment to alert cleared industry to the increasing foreign threat to AUV technology and assist in countering that threat.

2. TREND ANALYSIS

As of late 2009, there were approximately 630 AUVs worldwide. Experts anticipate the AUV market will grow exponentially by 2020, with roughly 1,400 AUVs being built over the next decade to meet worldwide demands. They project global expenditures on AUVs to total 2.3 billion U.S. dollars from 2010 to 2019.²

Military applications of AUVs have lagged behind commercial ones; however, military research and funding is increasing at a rapid pace throughout the world as more countries realize the potential value of AUVs and invest in research and development (R&D). By 2020, maritime experts expect militaries to provide roughly half of all AUV funding.³ Obtaining sensitive U.S. information regarding AUVs will provide other countries with needed information to advance their indigenous AUV programs and their production of countermeasures to U.S. military systems.

Foreign interest in U.S. AUV technologies has risen over the past several years, as indicated by increased collection attempts. Industry reporting from fiscal year 2010 (FY10) reflects this trend: foreign entities that actively targeted cleared contractors working on AUV issues showed a particularly strong interest in transforming and upgrading their naval forces.

Foreign collectors employed a variety of collection techniques to gain access to sensitive, classified, or export-controlled information. Common methods of operation

(MOs) included *requests for information (RFIs)*, *suspicious network activity (SNA)*, *solicitation or marketing*, and *seeking employment* with cleared contractors.

3. COLLECTOR ORIGINS

During FY10, of those targeting AUV platforms and associated technologies, entities from East Asia and the Pacific led the way with 72 percent of the total, followed by others from the Western Hemisphere, Near East, Europe and Eurasia, and South and Central Asia, none with more than 13 percent of the total.

TOP REGIONS TARGETING AUTONOMOUS UNDERWATER VEHICLES

FIGURE 5



EAST ASIA AND THE PACIFIC

The geography of the East Asian and Pacific region contributes to interest in expanding and improving naval capabilities. AUVs can provide both offensive and defensive capabilities in both littoral waters and further offshore.

Some East Asian and Pacific countries have contentious relationships with each other. When one country demonstrates an aggressive interest in developing a new naval technology such as AUVs, this can spur a parallel interest in other regional neighbors, targeting the same technologies, and extending even to the use of similar MOs.

None of the regions have achieved the U.S. level of overall industrial development nor the capability for military applications of technology. Access to more advanced AUV technology would allow the regions to both accelerate the implementation of improved underwater systems and save time and money by obtaining and reverse-engineering U.S. AUV technologies.

East Asia and the Pacific was the most prolific region in reported collection attempts directed at U.S. AUV technologies in FY10, accounting for over 70 percent of all AUV-related suspicious contact reports (SCRs) worldwide.

Analyst Comment: The U.S. Navy's ability to establish and maintain underwater battlespace dominance is of special importance in this region. Successful development of AUVs for East Asian and Pacific military purposes would likely pose a threat to that dominance by

increasing foreign understanding U.S. AUV technologies, potentially enabling them to develop effective countermeasures. (Confidence Level: Moderate)

Based on past practice, the East Asian and Pacific region also represents a significant risk of unauthorized transfer of AUV technology, not only within the region but also to other regions. Such transfer might be motivated by either commercial profit or geostrategic goals, and could be performed deliberately or inadvertently, the latter the result of less-than-robust export control systems.

THE NEAR EAST

Near East AUV programs lag behind those of the United States and East Asia and the Pacific. Collection efforts originating in the region remain at a relatively low level. However, those efforts do continue, as evidenced by industry reporting, and are likely to represent an increasing priority over the next decade. AUVs have particular value for regional powers, as asymmetric naval strategies can threaten sea lines of communication at their most vulnerable points.

4. AFFILIATIONS AND METHODS OF OPERATION

East Asian and Pacific collectors primarily depended on commercial entities to obtain sensitive U.S. technology in FY10. Suspicious entities used *RFIs* in more than half of the AUV-related SCRs, with emails, faxes, or phone calls to seek price quotes and technical information being most prevalent. *SNA* accounted for a quarter of the incidents targeting cleared facilities working on AUV technology in FY10.

AUVs are a dual-use technology and brokers often claimed that the technologies sought were for commercial use. *Commercial* entities falsified documents and misrepresented end users to collect controlled U.S. technologies.

Analyst Comment: If AUV suppliers were to ship such technology, such purchasers would likely provide it to government or military end users, either for employment on an existing AUV platform or for longer-term reverse-engineering. (Confidence Level: Moderate)

Similarly, collecting entities such as *government-affiliated* universities often used *academic solicitation*, describing the sensitive AUV information targeted as having solely scientific and educational purposes with little to no apparent military

application. Personnel affiliated with academic institutions sought to sponsor exchanges of personnel or information, submit research papers for peer review, or send students to participate in classified or sensitive research projects.

Analyst Comment: Suspicious entities successful in establishing such relationships would almost certainly seek to exploit them to gain access to sensitive or classified U.S. AUV information and technology. (Confidence Level: High)

Other *government-affiliated* entities from East Asia and the Pacific that engaged in AUV technology collection efforts in FY10 included state-sponsored R&D agencies.

UNDERWATER GLIDERS

Gliders are a type of AUV designed specifically for oceanic missions that require long endurance: weeks, or even months. By comparison, other AUVs tend to conduct limited-duration missions lasting hours, or at most days.

Underwater gliders make use of a variety of auxiliary driving mechanisms, such as ocean thermal energy, to quietly “glide” in the water with minimal energy consumption. While not as fast as standard AUVs, gliders using buoyancy-based propulsion have a significantly greater range and mission duration than AUVs propelled by electric motors. This makes them ideal for ISR. Diving abilities depend on the specific glider, but most range between 200 and 1,500 meters; deeper-diving gliders are under development.

Underwater gliders typically carry sensors such as sonar, hydrophones, and thermal sensors used for mapping or monitoring the ocean environment and wildlife. The U.S. Navy uses gliders for battlespace reconnaissance and mapping. Flotillas of gliders can establish a sensing network in an operational area of interest to provide commanders with the data to support their mission planning.

Industry reporting indicates that foreign targeting of underwater glider technology significantly increased in FY10 when compared to FY09.

Near Eastern collections, in contrast, were more likely to depend on *individuals* targeting AUVs, using *RFIs*. Nonetheless, Near East entities also used *academic solicitation* in their attempts to collect information. Non-traditional collectors such as individual university students sought research positions or placement at various U.S. universities or facilities where they might gain access to U.S. AUV programs. Such supposedly unaffiliated students also attended international trade shows, solicited vendors, and attempted to integrate themselves into the scientific community.

5. TARGETED TECHNOLOGIES

DSS analysis of FY10 industry reporting demonstrated the wide range of AUV technology collection attempts. Reporting indicated interest in not only conventional AUVs, but gliders as well, and not only AUVs themselves but all aspects of AUV enabling technologies, such as various types of underwater sensors.

Countries wishing to develop a robust military AUV capacity need to improve both overall AUV capabilities and enabling technologies. Such capabilities and technologies include navigation, communications, design and construction, sensors, propulsion, and power.

Similarly, collectors ranged from sophisticated producers in industrially advanced countries seeking specialized sub-systems to emerging third-world countries seeking entire AUV systems for military modernization programs.

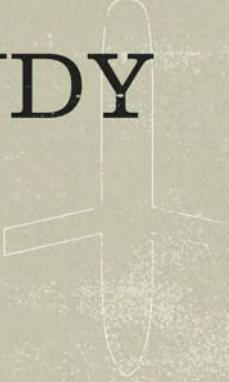
6. ANALYTICAL FORECAST

Reporting from industry confirms that U.S. AUVs and related technologies are of significant interest to the rest of the world. *Commercial*, *individual*, and *government-affiliated* entities are likely to continue using a variety of MOs, especially *RFI* and *SNA*, to collect U.S. AUV technology and information. **(Confidence Level: Moderate)**

Any technologies or information acquired will likely help foreign governments develop their indigenous AUVs, assist foreign navies in countering U.S. AUVs, and increase the threat to U.S. undersea battlespace dominance. **(Confidence Level: Moderate)**

Based on trends in the AUV industry, DSS assesses that it is very likely that demand for AUVs will increase dramatically over the next several years, especially as more military and commercial capabilities develop. DSS assesses that, as the technology advances, foreign collectors will almost certainly increase their efforts to satisfy that demand by targeting U.S. cleared contractors working on AUVs or related systems. **(Confidence Level: High)**

CASE STUDY



In 2010, a U.S. cleared contractor received an email from an East Asian and Pacific company requesting to purchase one of the cleared contractor's military AUVs and other related components, including batteries and a communications antenna. The requestor did not specify either the intended use or the end users.

This collection attempt should be considered in the context of a pattern of similar reported incidents that demonstrated the substantial East Asian and Pacific interest in acquiring AUV technology. Over the course of seven months in FY10, ostensibly commercial entities and academic institutions from the region made five separate requests to purchase export-controlled AUV technology.

Analyst Comment: Records of such collection attempts capture the number and diversity of East Asian and Pacific commercial entities submitting *RFIs* for AUVs or enabling technologies. Any such AUV technology obtained by these companies, although dual-use, would probably find its way to military applications, providing much-needed assistance to indigenous AUV programs. Such acquisitions would likely assist collecting countries in understanding current levels of U.S. AUV technology, thus aiding in their development of countermeasures. (Confidence Level: Moderate)

THIS PAGE INTENTIONALLY LEFT BLANK

EAST ASIA AND THE PACIFIC



EAST ASIA AND THE PACIFIC



1. OVERVIEW

Even as total suspicious contact reports (SCRs) from industry multiplied by a factor of almost two and a half from fiscal year 2009 (FY09) to FY10, the East Asian and Pacific region accounted for an even larger percentage of the total in the more recent year, increasing from 36 percent to 43 percent. East Asia and the Pacific provided as many of the reported suspicious contacts as the next three regions combined.

Statistically, the most likely East Asian and Pacific collection attempt consisted of a *commercial* entity using a direct *request for information (RFI)* to acquire sensitive information about U.S. *information systems (IS) technology*. But the picture was dynamic: *unknown* collectors reduced the previous year's gap behind *commercial* entities as the leading collector agents, *suspicious network activity (SNA)* similarly closed the gap with *RFIs* as the leading method of operation (MO), while *IS* re-opened a larger gap with *lasers, optics, and sensors (LO&S)* as the top targeted technology. The large scope of collection efforts traceable to East Asia and the Pacific meant that

considerable efforts were simultaneously directed at many other technologies and that the collection thrust was conducted at a high tempo by many other methods and entities, as well.

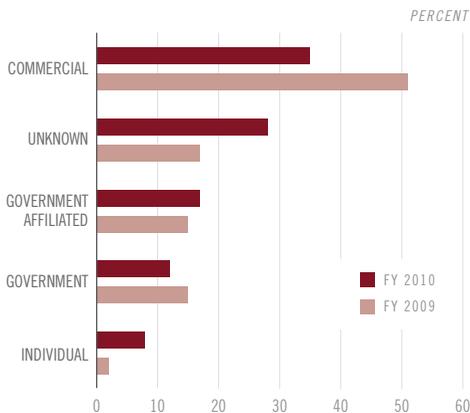
2. COLLECTOR AFFILIATIONS

Collectors linked to East Asia and the Pacific were most commonly affiliated with *commercial* entities. Collection attempts by *commercial* entities in the region have consistently increased since 2008. In FY10 such cases accounted for a higher proportion, 35 percent, than *government* and *government-affiliated* collectors combined, at 12 and 17 percent respectively. However, the percentage of East Asian and Pacific SCRs ascribed to the *commercial* category actually declined from the 51 percent of FY09; the *unknown* category registered the corresponding increase, from 17 to 28 percent. Therefore, even as the overall number of SCRs increased, the most notable change in affiliation suggested that collectors were becoming increasingly adept at camouflaging their identities.

The jump in the number of attempts with *unknown* affiliations comes in part from the region's high level of *suspicious network activity (SNA)* in the form of cyber intrusion attempts directed at cleared contractor networks. Specific attribution for such attempts is often difficult to ascertain; for example, while many such requests might appear to originate from a university, a nonacademic entity may be cloaking its collection attempt behind an academic email address. Nonetheless, the Defense Security Service (DSS) successfully resolved a large number of unknown cases to Internet protocol (IP) addresses in East Asia and the Pacific.

COLLECTOR AFFILIATIONS

FIGURE 6



An academic nexus showed up in other categories as well. East Asian and Pacific academic institutions such as universities made up a large part of the *government-affiliated* category, while foreign students applying to cleared contractors associated with U.S. universities made up a large part of the *individual* category.

When viewed individually, many of the SCRs resolving to *commercial* entities seemed innocuous. However, DSS observed several separate *commercial* entities requesting similar or identical technologies in a relatively short time frame. The grouping of the requests suggested that the entities focused their collection activity in a manner that resembled the procurement systems that many foreign countries use to acquire military technology.

Procurement systems vary considerably within East Asia and the Pacific. In some countries, *commercial* entities may be overtly approved, overseen, and even officially certified by government procurement agencies. Such countries are likely to use acquisition mechanisms that are very similar to the relatively open tender-based tasking of procurement agents characteristic of the United States and other Western countries. *Commercial* entities working on behalf of such East Asian and Pacific countries often readily admitted that government agencies would be the end users of any technology supplied.

Elsewhere within East Asia and the Pacific, governmental practices are generally more opaque, both as to the relationship between agencies and entities and as to processes. In fact, some of these countries went to great lengths to conceal any connection between *commercial* and *government* entities, and became increasingly sophisticated in their camouflage methods. Commercial companies often employed complicated business structures and separate company names—techniques characteristic of front companies.

DSS analysis identified a number of such U.S.- or third country-based entities that linked back to *government* collectors in East Asia and the Pacific, either overtly or through other business connections. These entities used various means of transshipment and specified alternate end uses for the requested technologies.

Analyst Comment: Some East Asian and Pacific collectors showed relative sophistication in their knowledge of best practices for making seemingly innocent requests for cleared contractor systems and of the relevant shipping logistics and export regulations. DSS assesses that it is highly likely that collectors from East Asia and the Pacific, pursuant to substantial interest in the acquisition of particular systems or technologies, conducted campaigns to acquire those technologies resident in U.S. cleared industry, and, upon their acquisition, to evade export controls. (Confidence Level: High)

The military applications for autonomous underwater vehicles (AUVs) are relatively new, but many navies intend to incorporate this technology into their inventories, and it is an area increasingly targeted world-wide for collection attempts. Because AUVs constitute a new direction for many countries, requests targeting AUVs and related technologies often require *commercial* entities to request technologies well outside the scope of their established, stated business interests. AUVs are a dual-use technology, with many legitimate civilian applications. In most *commercial* requests, the requestor did not identify the end user or intended use.

3. METHODS OF OPERATION

In FY09, direct requests represented nearly three-quarters of the cases; in FY10 the corresponding *RFIs* declined to less than half. Reports of *SNA* more than doubled.

Analyst Comment: It is likely that there is a correspondence between the decline in the percentage of *RFIs* and the increase in the *SNA* percentage. These results likely demonstrate collectors' shift toward less direct methods, conducting their probes while remaining further removed from the cleared contractors. (Confidence Level: Moderate)

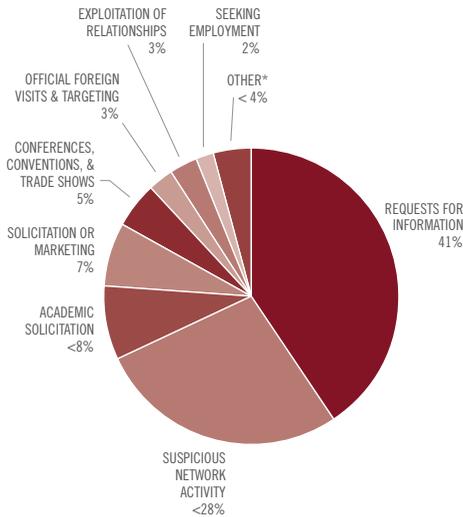
However, even as *RFIs*' percentage of all collection attempts declined in FY10, their number of *SCRs* increased considerably; and, in contrast to the overall region, in some East Asian and Pacific countries the proportional use of *RFIs* increased as well.

Both *commercial* and *academic* entities used *RFIs*, including direct purchase requests, in their attempts to gain access to classified or sensitive U.S. technologies. The majority of the attempts were made via relatively blunt emails that stated the technology of interest and the desired quantity. Other requests asked broad, seemingly innocuous questions, but such queries are capable of eliciting replies that would confirm or deny collecting countries' suspicions concerning research on and the capability, strength, and status of sensitive technologies.

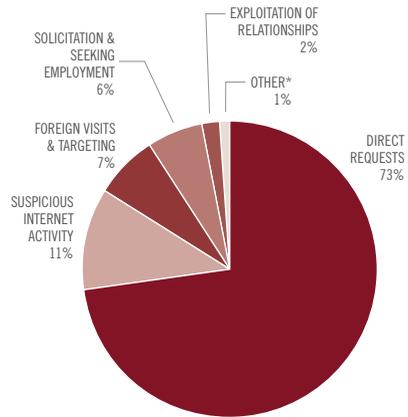
METHODS OF OPERATION

FIGURE 7

FY 2010
PERCENT



FY 2009
PERCENT



*Includes MOs not otherwise listed. Singularly, these methods represent less than one percent of the total.

Analyst Comment: The use of *RFIs* makes it very likely that the collector can obtain required information without using the time-consuming and expensive resources employed by a traditional intelligence officer. Thus *RFIs* offer an approach characterized by low cost yet a potential for high reward. DSS assesses that East Asian and Pacific collectors will almost certainly continue a substantial use of this MO. (Confidence Level: High)

In some incidents, however, the suspicious entity demonstrated a more nuanced approach, such as changing from commercial-grade to military-grade specifications and systems in the course of negotiations with the cleared contractor.

Analyst Comment: Attempting to upgrade specifications or system demands midway through the purchasing process likely constituted an attempt to circumvent the export control process via misdirection or to use the cleared contractor's desire to complete a sale already in process to gain access to otherwise restricted technologies. (Confidence Level: Moderate)

In a noticeable shift in reporting, there was a huge increase—by a factor of eight—from last year to this in attempts to gain access to U.S. technology or information using *SNA*. The majority of the incidents were unsuccessful brute-force attempts to access cleared contractor networks. Such computer-based intrusion attempts tended to be non-specific in nature, often attempting to extract large amounts of data from cleared contractor networks without targeting any specific technology.

In contrast, DSS analysis categorized roughly 30 percent of these *SNA* cases as either root- or user-level intrusions. In these instances, foreign entities may have gained access to unclassified cleared contractor networks, potentially compromising sensitive but unclassified information resident on those networks. The most prevalent vector for root- and user-level intrusions was spear phishing emails. This method provides malicious attachments or links to outside websites in an attempt to obtain employees' personal information or credentials or otherwise gain access to the networks.

While many of the attempts were unsophisticated, FY10 saw a number of relatively advanced spear phishing attempts. In order to convince employees to download malicious applications, probers crafted emails that appeared as if they had been sent from within the company, using contact information and uniform resource locators (URLs) designed to match or resemble those affiliated with the cleared facility.

Analyst Comment: Beyond lending an assumed credibility to the email, the use of cleared contractor naming conventions in the URLs also likely facilitated the storage

and organization of collected information, implying collaboration between multiple requesting entities.

(Confidence Level: Moderate)

Some East Asian and Pacific entities structure their collection campaigns and craft their attempts to take advantage of the fact that computers, and especially computer networks, know no geographical boundaries. DSS correlated network intrusion incidents to known foreign computer network operations intrusion sets. However, the technical indicators of intrusions may be constantly changing. Penetrators used email spoofing, obfuscation techniques, and more advanced tradecraft to assume a false identification, hide their activity on a compromised network, and disguise the destination of the exfiltrated data.

Analyst Comment: Attributing *SNA* to a particular country is usually harder than for any other MO. While instigators may use a particular country's infrastructure, technical barriers sometimes prevent positive identification of the originating country. Although DSS was often able to attribute *SNA* attempts to particular countries within East Asia and the Pacific, a significant number of *SNA* attempts remain in the unknown category. However, even in such cases, DSS efforts may still yield attack indicators and information on MOs that help the United States improve its defenses. (Confidence Level: Moderate)

East Asian and Pacific collectors took steps to get closer to U.S. cleared contractors and their facilities, whether engaged in research, design, laboratory work, or manufacturing.

Collectors for countries already engaged in ongoing patterns of interaction and cooperation with the United States, including existing technology agreements, used the *solicitation and marketing services* and the *targeting of U.S. travelers overseas* MOs to capitalize on this advantage. In one case, cleared contractor employees traveled to East Asia and the Pacific to deliver electronic components pursuant to a contract. When the end user reported the components were inoperable, the U.S. company representatives discovered physical evidence that the components had been opened, in contravention to existing technology agreements. This intrusion and others like it may indicate attempted reverse-engineering.

Analyst Comment: Each of these MOs accounted for fewer than 10 percent of the East Asian and Pacific SCRs. DSS assesses that it is likely that these MOs were not more commonly used because of the increased success of *RFIs* via email and the heightened sensitivity to East Asian and Pacific contacts that made such targeting less successful. (Confidence Level: Moderate)

While technology agreements can be mutually beneficial, DSS assesses that the enhanced exposure combined with aggressive collection attempts means that the threat of exploitation remains high, and some foreign successes will be very likely. (Confidence Level: High)

Approximately eight percent of reported collection attempts from East Asia and the Pacific sought information via the longer-term MO of *academic solicitation*. This is eight times the number of such

approaches in FY09. Students and academic professionals from research institutes and universities sought to engender ties between themselves and cleared contractors. Highly qualified graduate students, including many already in possession of doctoral degrees, were particularly active. Cleared contractors reported a notable number of requests sent to cleared laboratories whose work was incompatible with the requesting individual's field of research.

A shorter-term method was attempted in the form of *solicitation and marketing services*, in which a *commercial* entity typically offered to build a relationship with a cleared contractor, either by providing products to the contractor or by marketing the contractor's products in the entity's country of origin.

Analyst Comment: It is likely that many East Asian and Pacific businesses successful in building such relationships use them as a conduit to exploit cleared contractors and acquire sensitive technologies. (Confidence Level: Moderate)

4. TARGETED TECHNOLOGIES

As defined on the Militarily Critical Technologies List (MCTL), the technologies most targeted by East Asian and Pacific collectors remained generally consistent from last year. The most notable change was a seeming relative ebbing of last year's intense interest in *LO&S*, with proportional increases noted instead in *IS*—still the single leading category—and *marine systems technology*.

TARGETED TECHNOLOGIES

TABLE 1

MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL) CATEGORIES	FY 2010 PERCENT	DEVELOPING SCIENCE AND TECHNOLOGY LIST (DSTL) CATEGORIES	FY 2009 PERCENT
INFORMATION SYSTEMS TECHNOLOGY	25	INFORMATION SYSTEMS TECHNOLOGY	21
LASERS, OPTICS, AND SENSORS TECHNOLOGY	13	SENSORS TECHNOLOGY	17
AERONAUTICS SYSTEMS TECHNOLOGY	8	UNKNOWN	13
ELECTRONICS TECHNOLOGY	7	ELECTRONICS TECHNOLOGY	11
MARINE SYSTEMS TECHNOLOGY	7	AERONAUTICS TECHNOLOGY	8
POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	5	POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	5
INFORMATION SECURITY TECHNOLOGY	5	ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	5
ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	5	MARINE SYSTEMS TECHNOLOGY	4
SPACE SYSTEMS TECHNOLOGY	3	GROUND SYSTEMS TECHNOLOGY	3
GROUND SYSTEMS TECHNOLOGY	2	LASER AND OPTICS TECHNOLOGY	3
MATERIALS AND PROCESSES TECHNOLOGY	1	SPACE SYSTEMS TECHNOLOGY	3
PROCESSING AND MANUFACTURING TECHNOLOGY	1	MATERIALS AND PROCESSING TECHNOLOGY	2
CHEMICAL TECHNOLOGY	1	WEAPONS EFFECTS TECHNOLOGY	2
NUCLEAR SYSTEMS TECHNOLOGY	1	BIOLOGICAL TECHNOLOGY	1
SIGNATURE CONTROL TECHNOLOGY	1	CHEMICAL TECHNOLOGY	1
BIOLOGICAL TECHNOLOGY	> 0	MANUFACTURING AND FABRICATION TECHNOLOGY	0
DIRECTED ENERGY SYSTEMS TECHNOLOGY	> 0	ENERGY SYSTEMS TECHNOLOGY	0
ENERGY SYSTEMS TECHNOLOGY	> 0	NUCLEAR TECHNOLOGY	0
WEAPONS EFFECTS TECHNOLOGY	> 0	SIGNATURE CONTROL TECHNOLOGY	0
BIOMEDICAL TECHNOLOGY	> 0	BIOMEDICAL TECHNOLOGY	0
NO MILITARY CRITICAL TECHNOLOGY REQUESTED	11	DIRECTED AND KINETIC ENERGY TECHNOLOGY	0
OTHER*	3		

* Note: Includes cases not otherwise listed

This was an overall result, however; some collectors within the region maintained last year's high level of interest in *LO&S*. *Aeronautics systems* technologies remained in third place overall; East Asian and Pacific entities with a significant interest in unmanned aerial systems (UAS) and their related components also tended to be interested in the *positioning, navigation, and time*-related technologies that support such systems.

FY10 reporting indicated that East Asian and Pacific collectors targeted *IS* more than any other technology section. Where analysis was able to specify, the most coveted technology was command, control, computers, communications, intelligence, surveillance, and reconnaissance (C4ISR) platforms. However, the majority of SCRs concerning *IS* were non-specific in nature, as they were primarily the result of cyber reporting. Although it was difficult for DSS to determine the specific targeted technology or system in these cases, DSS attributed a number of them to *IS*, based on the work conducted by the cleared facility in question.

Analyst Comment: The lack of a specific and known targeted technology in many East Asian and Pacific cases involving *IS* hindered further analysis regarding the goals of such collection attempts. DSS assesses there is at least an even chance that the overall increase in targeting and the technologies sought after demonstrate an interest in upgrading C4ISR capabilities. (Confidence Level: Low)

Despite the overall proportional decrease, in FY10 *LO&S* remained a major factor in regional collection efforts, as measured by industry reports. Notably, both *commercial* and *academic* entities requested a range of subsystems which have substantial applications in military laser technology and AUV sensor systems.

One of the most substantial areas of growth in the data during FY10 was *marine systems*, with reported collection attempts more than tripling overall and more than doubling within East Asia and the Pacific. This category's sharp increase was driven by reported requests for AUVs. While the growth in this category reflected the numerous *commercial* and *academic* entities requesting AUV systems, it failed to fully reflect the frequent requests for AUV enabling technologies in other sections of the MCTL.

AUVs have yet to achieve their full military potential. Militaries around the world are deploying AUV systems for a variety of intelligence collection and warfare applications. In FY10, East Asian and Pacific-affiliated collectors targeted underwater gliders specifically.

Analyst Comment: East Asian and Pacific militaries are interested in both increasing their ability to control and defend littoral areas and extending their reach beyond those waters. It is very likely that they seek to acquire AUVs for integration into indigenous systems. (Confidence Level: High)

5. ANALYTICAL FORECAST

Within East Asia and the Pacific, countries span a wide range in the closeness of their current relationships with the United States: some friendly, some relatively hostile. But the region also represents a wide range of strategic agendas vis-à-vis the United States for the future: some countries are and will likely seek to remain allies, whereas others increasingly are rivals. Therefore, countries will likely continue to vary in their degree of concern over the potential impact on relations with the United States of their attempts to obtain illegal or unauthorized access to classified information or technologies resident in the U.S. cleared industrial base. **(Confidence Level: Moderate)**

But, the United States aside, several East Asian and Pacific countries are also involved in very active rivalries with other countries within the region. Therefore, it is very likely that none of them will cease their collection attempts, and East Asia and the Pacific will almost certainly remain the most prolific area for reported collections in FY11. **(Confidence Level: High)**

In pursuit of such efforts, the East Asian and Pacific region is likely to employ collectors of all affiliations. *Commercial*, *academic* and *government-affiliated* actors are likely to continue using overt, seemingly innocuous MOs to mask their true identity and affiliation. But as cleared contractors increasingly recognize that such contacts, regardless of benign initial appearance, are likely designed to exploit cleared industry's

technological base, SCRs on suspicious *commercial* and *academic* contacts, in particular, are likely to continue to increase. **(Confidence Level: Moderate)**

The continued high number of *RFIs* reported and the reliance on other relatively overt methods, such as *targeting of U.S. travelers* overseas, even by relatively sophisticated collectors, illustrates that such methods probably have been an effective way of illicitly acquiring and exploiting U.S. technology, and will likely be used by East Asian and Pacific collectors as long as they are effective. However, as industry continues to become more aware of the threat that such contacts pose, the use of other MOs will likely continue to increase. **(Confidence Level: Moderate)**

Along this line, the increased reporting of *SNA* represents a significant change in DSS data. Intelligence Community reporting documents long-standing reliance by East Asian and Pacific collectors on computer-based MOs. However, DSS assesses that, while the increase in SCRs likely signifies more intrusion attempts, it also likely reflects an increased awareness and reporting among cleared contractors about the use of the cyber domain. Such SCRs will probably continue increasing as members of the cleared industrial base learn to recognize these attempts. **(Confidence Level: Moderate)**

For some U.S. technologies, alternative sources of similar or equal quality exist in third countries, some of which have more manageable export barriers, and these

countries are also subject to collection attempts. But the United States remains a primary target. East Asian and Pacific collectors likely persist in targeting U.S. suppliers because they not only seek to acquire U.S. technology for integration into indigenous systems, but also to understand the capabilities possessed by the U.S. military. It is likely that further military development and exploitation of these technologies will compromise U.S. operational capabilities in East Asia and the Pacific in the future.

(Confidence Level: Moderate)

If East Asian and Pacific entities acquire U.S. information or technologies, they are likely to continue to attempt to reverse-engineer acquired technologies. In some cases this will likely be to advance indigenous research and development (R&D) capabilities so as to meet national mandates, including the development of countermeasures, while in others it will likely result from a desire to re-export the technology for profit.

(Confidence Level: Moderate)

CASE STUDY

During FY10, a company from East Asia and the Pacific requested UAS prototyping services from several cleared contractors to assist in completing a UAS project for its nation's military.

To fulfill similar goals, numerous companies and academics from East Asia and the Pacific requested both full UAS systems as well as enabling technologies. They submitted *RFIs* and made *academic solicitations* for *aeronautic systems* (AS) technology, focused on UAS. Some entities appeared to prefer *SNA*, specifically cyber intrusion attempts, to target AS technologies. They attempted to infiltrate the networks of cleared contractors performing AS R&D.

Analyst Comment: DSS assesses that such targeting of separate aspects of complementary systems almost certainly involves a coordinated effort in quest of these technologies. The interest in the particular components corroborated previous reports concerning the country's focus on developing and quickly deploying extensive, indigenous, space-based C4ISR systems. This would allow the gradual reduction of reliance on foreign sources of space-ready technology. (Confidence Level: High)

This example illustrates the overlap and connections between different categories of technologies from the MCTL. UAS technology falls under the larger category of AS. But operational control of UAS usually involves C4ISR capabilities that rely in part on *space systems*. Depending on the particular stage of development a country may be in with its pursuit of a next-generation capability, its collection goals may ebb and flow over a particular one- or two-year period with regard to particular technologies. But its overall interest in these interrelated technologies is unlikely to disappear.

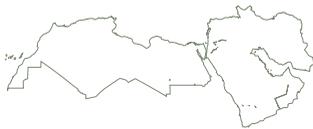
For example, in FY10, SCRs based on collection attempts targeting UAS technology linked to the East Asian and Pacific country in question decreased in frequency over the course of the year. Similarly, reports of its acquisition attempts against *space systems* decreased slightly from FY09. However, reporting showed that particular components used in satellites and high-altitude avionics were a particular focus in FY10, with requesting entities targeting a handful of cleared contractors.

Analyst Comment: DSS assesses that it is likely that at a certain point during the year this country's entities managed to acquire or develop the services or products to meet their current UAS requirements, leading to the drop-off in attempts. However, as the UAS programs in question continue to develop, it is likely that collectors will resume requesting more advanced UAS technology, including supplementary enabling technologies to expand the functionality and effectiveness of existing systems. (Confidence Level: Moderate)

NEAR EAST



NEAR EAST



1. OVERVIEW

In fiscal year 2010 (FY10) the number of reported cases traced to the Near East region more than doubled over the previous year. Yet as a percentage of all suspicious contact reports (SCRs), the Near East's share actually declined slightly, due to the even greater increase in reporting attributed to East Asia and the Pacific. Nonetheless, the Near East remained the second most active region in foreign attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base.

As a region, the Near East is subject to a great deal of turmoil. Continuing problematic aspects include the Arab-Israeli conflict, a war in Iraq and the effects of another next door in Afghanistan, violent extremism, religious disputes over holy sites, unresolved border disputes, and populist uprisings in numerous Near Eastern countries in early 2011. The region contains aspiring states, regional powers, and world players in various categories of achievement. Some of the most active collectors in the region engage in active enmities with other countries in the region or nearby.

As both a cause and a result of this turmoil, the area has many illiberal if not authoritarian governments. Many of these states consider it imperative to maintain the utmost military capabilities they can acquire. While the various states within the region have different relationships with the United States, all seek to gain as much advantage from whatever access to U.S. sensitive or classified information and technology they can gain.

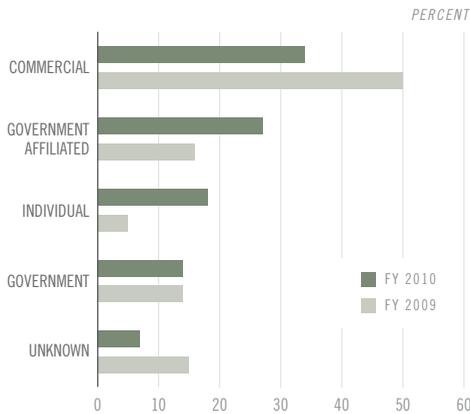
In FY10 the top Near East collector affiliation remained the *commercial* category, but the percentage declined significantly from FY09, while three other categories increased. The most common method of operation (MO), the *request for information (RFI)*, decreased in percentage of attempts from last year, but still accounted for half of this year's total. *Information systems (IS)* remained the most sought after technology; however, the Near East spread its collection efforts over a wider range of technologies than previous years.

2. COLLECTOR AFFILIATIONS

There was interesting movement in the collector affiliation categories from last year. In FY10, only one source, *government* collectors, remained unchanged as a percentage, at 14 percent of collections. Last year's largest category, *commercial*, declined from 50 to 34 percent, while last year's smallest category, *individual*, more than tripled, from 5 to 18 percent of the total. For the remaining two categories, *government affiliated* increased considerably, while *unknown* decreased considerably.

COLLECTOR AFFILIATIONS

FIGURE 8



The decrease in the *unknown* category's share suggests that both industry and the Defense Security Service (DSS) were more successful at discerning the identities of the collectors encountered. Of those identities, SCRs attributed to *individuals* and *government-affiliated* collectors increased more rapidly than those attributed to *government*, and significantly more so than *commercial* collectors.

Analyst Comment: The nature of many Near Eastern governments may explain why this region is an exception to the general trend toward increased reliance on commercial collectors. More authoritarian regimes tend to be less willing to delegate governmental functions to nongovernmental entities operating within their borders. (Confidence Level: Low)

The marked percentage decline in SCRs attributed to *commercial* entities was not a result of fewer *commercial* affiliations; in fact, there was a 50 percent quantitative increase in *commercial* reports.

Because of the varied nature of the governments in the Near East, industry reporting indicated that some used more *government-affiliated* collectors than others. Such *government-affiliated* entities might consist of premier science and technology universities and research institutions or large government-affiliated companies.

Analyst Comment: Considering the past degree of reliance on this category of collectors, the degree of investment by countries in their government-affiliated infrastructure, and recent trends in industry reporting, DSS assesses that collection by *government-affiliated* entities will probably continue at an increased level in FY11. (Confidence Level: Moderate)

During FY10, DSS observed the most significant increase in reported collection attempts by *individual* collectors: the category's percentage of the total tripled from FY09. This category represented

a relatively high percentage of the reported cases from states where the ruling government has a poor relationship with the United States.

Analyst Comment: This pattern almost certainly indicates government interest in obscuring collection attempts. DSS assesses it is very likely this trend will continue, with individuals concealing their affiliation in an effort to deceive U.S. companies. (Confidence Level: High)

In some cases the *commercial* affiliation, like the resort to *individual* collectors, can be attributed to an attempt by governments with poor relationships with the United States to minimize their signature in collection efforts. By using a collector entity distanced from the government, the request is likely to draw less attention.

Some governments within the region had no hope of gaining U.S. technologies for their militaries on a cooperative basis. In such cases, companies requested dual-use technology, claiming commercial applications as justification. A frequent augmentation to this tactic was to seek out third countries with relaxed export control laws and trade agreements to divert U.S. technology.

Analyst Comment: It is possible that some of the requests originating from *commercial* entities in the Near East contained falsified end-user information. If acquired, dual-use items may be diverted to military and/or government elements to support modernization efforts, or to third parties. (Confidence Level: Low)

3. METHODS OF OPERATION

It is necessary to follow the data regarding the MOs used by Near Eastern collectors through the categorization and labeling changes DSS made since last year's report.

Last year's direct requests decreased as a percentage from 69 percent to this year's 50 percent for *requests for information (RFIs)*.

The 15 percent for FY09's solicitation and seeking employment category yielded a combined 27 percent for FY10's *solicitation and marketing, seeking employment, and academic solicitation*. *Academic solicitation* was especially significant, as that single category in FY10 experienced two times the number of cases as the entire combined category last year.

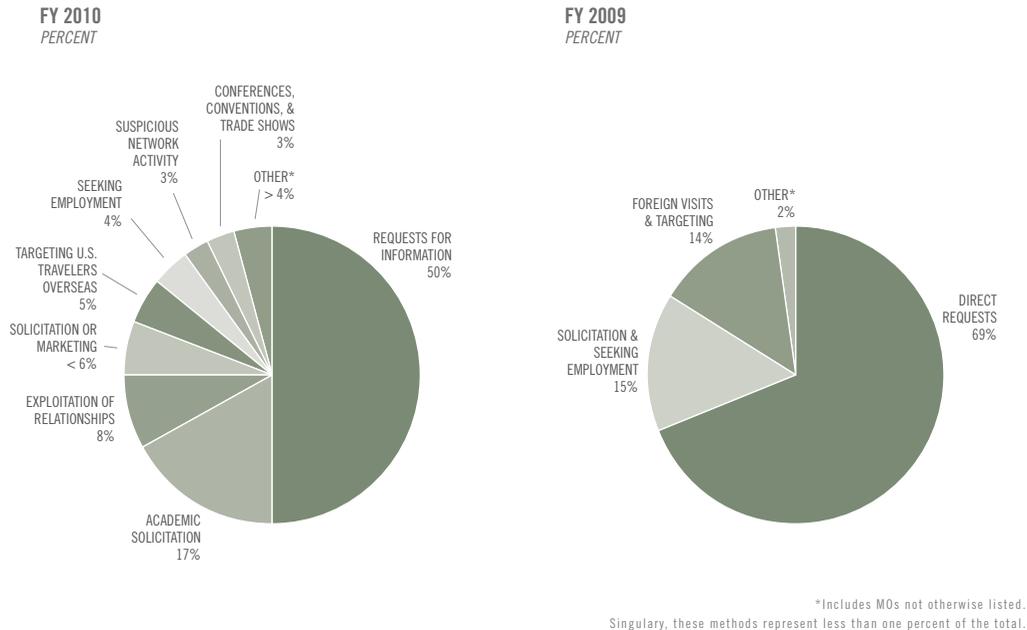
Last year's 14 percent for foreign visits and targeting declined slightly to 9 percent for the three new categories (*foreign travel and targeting; official foreign visits and targeting; and conferences, conventions, and trade shows*) combined.

This region yielded no SCRs on suspicious internet activity or exploitation of relationships in FY09, but in FY10 *suspicious network activity (SNA)* and *exploitation of relationships* accounted for 3 and 8 percent of total SCRs.

The overall significance of this data is that half of the region's reported collection attempts were made using *RFIs*. In addition, direct approaches made during short-term exposures (e.g., targeting cleared contractor employees during some kind of travel) still represent a significant part of the effort. However, reporting also increased

METHODS OF OPERATION

FIGURE 9



in MOs that require more patience, such as *academic solicitation* and *seeking employment*. In such cases, entities are prepared to invest significant time and effort to develop a long-term relationship so as to achieve placement and access that may yield opportunities to obtain illegal or unauthorized access to sensitive or classified information and technology.

As noted, industry reporting showed that overt *requests for information (RFIs)* remained the predominant MO in FY10. The use of email, telephonic, or in-person solicitation remains consistent as the principal collection techniques.

Analyst Comment: It is likely that Near Eastern entities attempting to procure sensitive U.S. technology and information use *RFI* as the primary method because such solicitations are less intrusive and can appear innocuous or legitimate in nature. (Confidence Level: Moderate)

As noted, the use of *academic solicitations* continued to rise. Industry reports showed that student requests varied, but were typically for post-graduate positions, research assistantships, thesis assistance, and review of scientific publications, or requests for dual-use technology for use in research.

Analyst Comment: In keeping with the Near East's typically close relationship between *government* and *commercial* entities, many universities and corporations conduct research and development (R&D) for government and military projects. It is likely that most, if not all, of the technology and information they generate, including via *academic solicitation*, can support government and military R&D projects in some way. (Confidence Level: Moderate)

Especially notable during FY10, several Near Eastern nationals—some located in their own countries, some in the United States—sought employment with cleared contractors to become directly involved in the most commonly sought after U.S. defense technologies.

As measured by SCRs, Near Eastern entities used *SNA* in only three percent of collection attempts in FY10, either because their infrastructure and capabilities in this area were rudimentary or because other MOs seemed to promise higher returns.

Analyst Comment: DSS continues to receive SCRs on attempted collections of telecommunication technology and information technology software, indicating an active Near Eastern desire to acquire the technology necessary to increase the capability to conduct *SNA*. The U.S. cleared industrial base will probably experience increased *SNA* as the relevant communications networks improve. (Confidence Level: Moderate)

For those countries within the Near East maintaining closer relationships with the United States, including those with technical assistance agreements (TAAs) between a company of that foreign country and U.S. cleared contractors, the targeting of U.S. personnel by foreign defense company personnel increased significantly. According to FY10 SCRs, the visitors casually but persistently asked for sensitive information outside the scope of the TAA throughout the U.S. visits.

Targeting U.S. travelers overseas emerged as a common MO for the Near East in FY10. Tactics included randomly selecting employees for invasive questioning at airport security checkpoints, during which time the employees' company-issued laptops and electronic devices were confiscated and reportedly exploited. In addition, some cleared employees experienced unauthorized hotel room entries and suspicious check-in procedures.

Analyst Comment: It is unlikely that airport security personnel had reason to select the cleared employees for additional screening. Instead, the airport and hotel security officers in question were probably associated with the national and/or military counterintelligence services responsible for counterintelligence, airport, and/or defense industry security. (Confidence Level: Moderate)

4. TARGETED TECHNOLOGIES

While SCRs concerning collection attempts aimed at the most commonly targeted technologies all approximately doubled, the relative relationships between those technology categories remained fairly consistent.

IS; aeronautics systems; and lasers, optics, and sensors (LO&S) technologies remained the Near East's most sought after, yet their respective percentages of the total all declined. Industry reporting indicates that the Near East spread its collection efforts more broadly in FY10.

IS remained the perennial favorite technology, but the interconnections with *aeronautics systems, LO&S, and space systems* technology were significant, with some resultant shifting of precedence between those categories. Several countries within the region are aspiring space powers, seeking to operate their own rockets and launch their own satellites. There is often a relationship between a country's civilian space program and its ballistic missile program. Technologies used in space launch vehicles (SLVs) and civilian space programs can be modified to support ballistic missile programs. Historically, countries have developed SLV and ballistic missile programs concurrently because of the similarities in the technology. Given the geopolitical situation within the Near East, this often gives rise to a concomitant interest in and attempts to develop missile defense and countermeasure systems. Such indigenous space and rocket

programs continue to advance, with several communications and remote sensing satellites currently in development.

Nonetheless, these rising programs are generally still reliant on technology legally and illegally procured from international entities, foreign governments, and commercial producers. In addition to the many students requesting to study space-related programs, Near Eastern collectors targeted technology that could support a space program, such as remote sensing and geospatial information systems.

As an example, in FY10 Near Eastern collectors continued to seek fiber optic gyroscopes (FOGs), likely for use in ballistic missile programs. Targets included not only FOGs themselves but related technology, including restricted U.S. high-resolution commercial imagery, high-resolution imagery satellites, and downlink stations. Some attempts to illicitly acquire protected technology used third-party intermediaries in the United States and other countries.

A related phenomenon affecting *IS* collection efforts was the focus on modeling and simulation software. Several cleared contractors received requests for export-controlled missile modeling and simulation software programs commonly used in the design and analysis of missile aerodynamics and performance. Industry also reported numerous requests for modeling and simulation software capable of predicting realistic three-dimensional radar signatures.

TARGETED TECHNOLOGIES

TABLE 2

MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL) CATEGORIES	FY 2010 PERCENT	DEVELOPING SCIENCE AND TECHNOLOGY LIST (DSTL) CATEGORIES	FY 2009 PERCENT
INFORMATION SYSTEMS TECHNOLOGY	16	INFORMATION SYSTEMS TECHNOLOGY	20
AERONAUTICS SYSTEMS TECHNOLOGY	13	AERONAUTICS TECHNOLOGY	19
LASERS, OPTICS, AND SENSORS TECHNOLOGY	11	SENSORS TECHNOLOGY	12
ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	5	LASER AND OPTICS TECHNOLOGY	8
ELECTRONICS TECHNOLOGY	5	ELECTRONICS TECHNOLOGY	8
SPACE SYSTEMS TECHNOLOGY	5	POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	7
MARINE SYSTEMS TECHNOLOGY	4	MARINE SYSTEMS TECHNOLOGY	5
MATERIALS AND PROCESSES TECHNOLOGY	4	UNKNOWN	5
POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	4	GROUND SYSTEMS TECHNOLOGY	4
PROCESSING AND MANUFACTURING TECHNOLOGY	3	ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	3
INFORMATION SECURITY TECHNOLOGY	3	MATERIALS AND PROCESSING TECHNOLOGY	3
ENERGY SYSTEMS TECHNOLOGY	2	ENERGY SYSTEMS TECHNOLOGY	2
SIGNATURE CONTROL TECHNOLOGY	2	CHEMICAL TECHNOLOGY	2
BIOLOGICAL TECHNOLOGY	2	SPACE SYSTEMS TECHNOLOGY	2
GROUND SYSTEMS TECHNOLOGY	1	BIOLOGICAL TECHNOLOGY	1
CHEMICAL TECHNOLOGY	1	MANUFACTURING AND FABRICATION TECHNOLOGY	1
NUCLEAR SYSTEMS TECHNOLOGY	1	WEAPONS EFFECTS TECHNOLOGY	1
WEAPONS EFFECTS TECHNOLOGY	1	DIRECTED AND KINETIC ENERGY TECHNOLOGY	0
BIOMEDICAL TECHNOLOGY	< 1	SIGNATURE CONTROL TECHNOLOGY	0
DIRECTED ENERGY SYSTEMS TECHNOLOGY	< 1	NUCLEAR TECHNOLOGY	0
NO MILITARY CRITICAL TECHNOLOGY REQUESTED	8	BIOMEDICAL TECHNOLOGY	0
OTHER*	8		

* Note: Includes cases not otherwise listed

Analyst Comment: DSS assesses that such requests for various missile modeling and simulation software programs likely mean that some states within the region are developing their missile programs and improving their missile defense capabilities through the acquisition of sensor and radar technologies. (Confidence Level: Moderate)

Within the *LO&S* category, Near Eastern collectors requested software programs with applications in space-based imaging systems and missile guidance systems. Some *commercial* companies from the region requested technology associated with unmanned aerial systems (UAS) or proposed joint ventures to develop a UAS. In yet another case the use of a possible front company with links to the Near East revealed regional interest in acquiring a UAS sensor data link which provides in-flight communications to and from UAS. Other disparate phenomena, such as Near Eastern students seeking to study mechanical and aerospace engineering, could also be related to interest in U.S. UAS design activities going on at cleared contractor facilities conducting R&D for the Department of Defense.

Development and deployment of missile defense and countermeasure systems requires access to specific sub-technologies. While some within the Near East have or are attempting to develop their own systems, they continue to make acquisition of U.S. technology a priority. In FY10 these included radar; sensor-to-shooter command, control, communications, computers, intelligence, surveillance, and reconnaissance technology; and cellular monitoring technology within the *IS* category.

5. ANALYTICAL FORECAST

Most countries within the Near East are far from achieving long-term self-sufficiency in technology development. When indigenous technologies or systems fail to perform effectively, acquisition of the corresponding U.S. technology is very likely to remain a collection goal and even increase in priority. For the foreseeable future, countries within the region will almost certainly remain dependent on foreign acquisition to support their various military industrial base and defense strategies. **(Confidence Level: High)**

Countries within the Near East that have established and seek to sustain a degree of global economic advantage and effective security measures will likely continue to attempt to acquire U.S. technology and information through both legitimate and illicit means. It is likely that regional collection tactics will evolve, favoring innovative methods that appear legitimate. **(Confidence Level: Moderate)**

The prevalence of *individual* and *unknown* collector affiliations in SCRs will probably persist. As Near Eastern collectors continue to provide little or no identifying information, increasingly seeking to mask their true affiliations, *RFIs* will probably become more difficult to attribute.

(Confidence Level: Moderate)

Some Near East collectors will likely continue to rely on third-party intermediaries, front companies, and procurement agents in pursuit of U.S. technologies. In many cases the end use and end users can be obscured easily, making it difficult to trace collector affiliation. **(Confidence Level: High)**

The Near East's exploitation of *academic solicitation*, including using students, professors, scientists, and researchers as collectors, will probably continue. Placing academics at U.S. research institutions under the guise of legitimate research offers access to developing U.S. technologies and cutting-edge research. The likely result will be better educated scientists and engineers able to provide the necessary intellectual infrastructure to indigenously create defense technologies to fulfill future military requirements. **(Confidence Level: Moderate)**

Where U.S. cleared contractors have defense contracts with Near Eastern companies, it is likely that the participation of foreign government personnel in visiting delegations will increase. The exploitation efforts (e.g., persistent questioning outside the scope of the agreement and unwittingly bringing in cameras/laptops/thumb drives) may continue to be interpreted as innocuous and legitimate, but DSS assesses that it is likely that these efforts will remain a preferred tactic to circumvent U.S. export control laws. **(Confidence Level: Moderate)**

The top targeted technologies will likely remain consistent as aspiring powers in the Near East continue force modernization efforts. It is likely that *aeronautics* and *space systems* technologies will continue to be a major focus as indigenous UAS, space, and ballistic missile programs continue to develop. **(Confidence Level: Moderate)**

An exception to this probable consistency is that, based on trends in the autonomous underwater vehicle (AUV) industry, DSS assesses that it is likely that worldwide demand for AUVs will increase dramatically over the coming years, especially as more military and commercial capabilities are developed. As the technology advances, some may successfully acquire AUVs through legitimate means, but DSS assesses that it is likely that foreign collectors will increase their targeting of U.S. cleared contractors working on AUVs or related systems over the next several years. Any technologies or information acquired will probably help foreign governments develop their indigenous AUVs, assist foreign navies in countering U.S. AUVs, and potentially threaten U.S. undersea battlespace dominance. **(Confidence Level: Moderate)**

Reporting from industry confirms that some of the collectors most active in targeting U.S. AUVs and related technologies are from the Near East. DSS assesses that *government-affiliated*, *commercial*, and *individual* entities from the region are likely in the immediate future to attempt to collect AUV technology and information. They are likely to use a variety of MOs, largely reliant on *RFI* followed by *SNA*. **(Confidence Level: Moderate)**

Given the unstable security situation in the Near East and the adjacent South and Central Asia region, countries within the Near East will very likely remain interested in UAS technology due to its value for intelligence collection and indications and warning. This means the more advanced U.S. UAS technology will almost certainly remain a collection priority for the near term. **(Confidence Level: High)**

CASE STUDY



In FY10, a cleared contractor received an email request from a representative of an East Asian and Pacific-based company for 30 units of a space-related technology and copies of the associated information. While conducting negotiations with the cleared contractor, the company's representative identified an end user within the Near East. The cleared contractor immediately halted negotiations due to applicable export restrictions.

The company is an electronics component distribution company, a subsidiary of a larger holding company. The owners of the electronics company are Near Eastern nationals. One of them has been involved in supplying defense-related electronics to their country's military, and has admitted to successfully acquiring U.S. technology in the past. Over the last few years the owners have contacted U.S. businesses and cleared contractor facilities in attempts to acquire numerous items, most of which are of concern to the U.S. military due to their potential to directly and adversely affect its forces operating in the field.

Analyst Comment: Although several of the technologies have legitimate civilian uses, the characteristics of the technologies make them highly sought after for military applications. According to the cleared contractor, the quantities of the particular technology ordered were exceptionally small; typical requests are in the thousands. The small size of the order is commensurate with the development of a prototype; or, when combined with the accompanying information, it may represent an attempt to reverse-engineer the technology. Based on the company's affiliation within the Near East, it is almost certain that it ordered the items for the government in question. (Confidence Level: High)

THIS PAGE INTENTIONALLY LEFT BLANK

EUROPE AND EURASIA



EUROPE AND EURASIA



1. OVERVIEW

There are many historical, cultural, and geostrategic ties and developmental and economic similarities between the United States and Europe and Eurasia. Many countries within the region see the United States as a model for innovation, modernization, and manufacturing expertise and look to it for assistance in achieving their own national defense, military, and technological goals. Sometimes the United States provides this assistance willingly; sometimes foreign collectors attempt to obtain it illicitly.

Since fiscal year 2009 (FY09), the number of suspicious contact reports (SCRs) ascribed to each of the six regions increased dramatically; Europe and Eurasia's reported collection attempts more than doubled from FY09 to FY10.

As a result, Europe and Eurasia displaced South and Central Asia as the third most reported collector. It should be noted that Europe and Eurasia—a region that contains many U.S. allies—helped to account collectively for 15 percent of the total world-wide reports of collection attempts against the U.S. industrial base.

While *commercial* entities remained the most active collectors in the region, collection attempts from *unknown* and *individual* collectors increased their share. *Requests for information (RFIs)* remained the most common method of operation (MO), but the most dramatic change was the rise in targeting via *suspicious network activity (SNA)*. Consistently battling for the top targeted technology category within this region, *information systems (IS)* technology returned to being the top targeted category.

2. COLLECTOR AFFILIATIONS

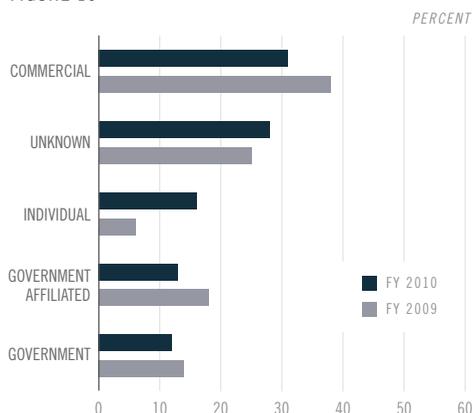
Defense Security Service (DSS) analysis of industry reporting shows that Europe and Eurasia is moving increasingly toward the pursuit of illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. Personal and/or individual economic goals may drive some of the collectors, whereas others may be acting on behalf of national or corporate entities while successfully masking their identities and/or affiliations. Based on FY10 industry reporting, European and Eurasian actors targeting U.S. technologies included anyone

from representatives of private companies to foreign liaison officers, journalists, civil servants, and scientists.

Overall, although the number of SCRs ascribed to the region in FY10 doubled from the previous year, the percentage of incidents attributed to *commercial*, *government*, and *government-affiliated* entities from Europe and Eurasia decreased. Attempts attributed to *unknown* and *individual* collectors increased.

COLLECTOR AFFILIATIONS

FIGURE 10



Most notable in comparison to the relatively modest changes in other categories was the rise in reported collection attempts by *individual* actors. Reports ascribed to *individuals* linked to Europe and Eurasia multiplied by a factor of six since last year. In FY09, *individual* actors were the least active collectors, but in FY10 SCRs ascribed to *individuals* almost tripled their relative share, from 6 percent in FY09 to 16 percent in FY10.

Analyst Comment: These statistics probably reflect an attempt by entrepreneurs to take advantage of economic modernization programs in parts of Europe and Eurasia. (Confidence Level: Moderate)

Despite the small decrease in the overall percentage of reports from FY09, FY10 reporting showed that *commercial* entities remained the most active collectors from Europe and Eurasia, with the number of reported attempts doubling. Reported attempts by collectors in the second most active category, *unknown*, increased by a similar proportion, from 25 to 28 percent.

Analyst Comment: Intelligence Community reporting indicates that commercial firms from Europe and Eurasia target U.S. military technologies and export a considerable quantity of indigenously produced technologies to countries of concern to the United States. DSS assesses that the continued strength of reporting that falls into the *commercial* category likely reflects the region's role as a technology supplier within the defense industry trade. (Confidence Level: Moderate)

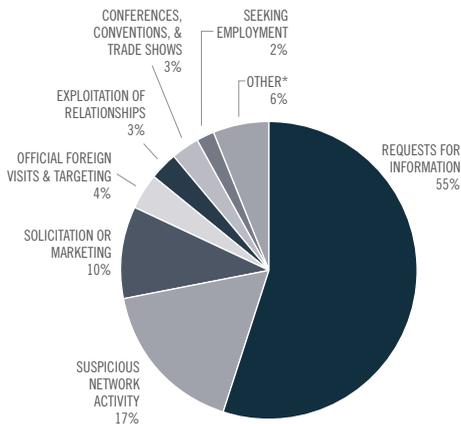
3. METHODS OF OPERATION

All of the methods of operation (MOs) in the DSS categorization scheme experienced an increase in reported attempts in FY10. However, in proportional terms, *exploitation of relationships* had no change, and *RFIs* (formerly direct requests), and the combination of the three categories that make up the former foreign visits and targeting declined. *RFIs* declined from 69

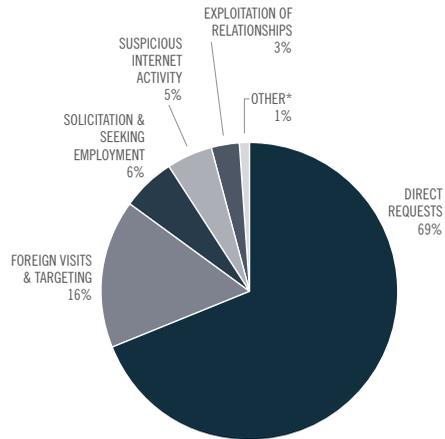
METHODS OF OPERATION

FIGURE 11

FY 2010
PERCENT



FY 2009
PERCENT



*Includes MOs not otherwise listed. Singularly, these methods represent less than one percent of the total.

to 55 percent of the total SCRs attributed to the region, the combined visitors and traveling sections from 16 to 8 percent.

The United States maintains friendly relations with almost all the countries in Europe and Eurasia and, as a matter of geostrategic policy, encourages many of them to increase defense spending and modernize their militaries. U.S. cleared contractors and industry from Europe and Eurasia share longstanding relationships, including in the form of joint ventures.

Based on industry reporting, European and Eurasian collectors often used overt *RFIs* to seek technology from U.S. cleared industry, primarily in the form of emails or web-card submissions.

Analyst Comment: Joint ventures and the relationships they nurture can convince some foreign partners that an *RFI* is not illicit but actually both innocuous and justified, perhaps even welcomed by the United States. Nonetheless, it is likely that *RFIs* allow foreign entities an opportunity to gain access to information normally denied to them. Since such *RFIs* offer a combination of low risk, low cost, and potentially high payoff, they will probably continue to be an option frequently used by European and Eurasian collectors. (Confidence Level: Moderate)

Similarly, longstanding relationships and a history of frequent interactions between the United States and Europe and Eurasia meant that the *official foreign visits and targeting; targeting of U.S. travelers overseas; and conferences, conventions, and trade shows*

MOs remained a factor in the soliciting of information and technology in FY10. Together they accounted for eight percent of the total industry reporting for Europe and Eurasia.

However, industry reporting in FY10 indicated that European and Eurasian collectors increasingly used indirect MOs in their attempts to gain access to cleared industry information or technology. *Academic solicitation, solicitation or marketing, and seeking employment* combined increased by almost a factor of five, more than doubling their share of the total. Of these, *solicitation or marketing* was the third most reported MO in FY10, at ten percent. As a single category, it accounted for almost four times as many SCRs as the broader former category of solicitation and seeking employment did in the FY09 data.

Analyst Comment: European and Eurasian collecting entities demonstrate a willingness to invest the time and effort necessary to integrate themselves or their personnel into

the cleared contractor realm via longer-term business or academic relationships and processes. If entities successfully solicit a business relationship with cleared contractors, they could probably exploit that relationship to gain access to or compromise sensitive components of advanced military systems. (Confidence Level: Moderate)

Most significantly, however, the number of SCRs listing *SNA* multiplied by a factor of eight from FY09, and this category more than tripled its share of the total. *SNA* now constitutes the second most commonly used MO for Europe and Eurasia, whereas in FY09 it was only the fourth. The majority of cyber incidents attributed to Europe and Eurasia involved multiple login attempts or the use of remote administrative tools.

Europe and Eurasia is home to an active and significant cyber criminal underground. Members of these underground communities conduct activities such as the theft and

SUPPLY CHAIN IMPLICATIONS⁴

Supply chain vulnerabilities provide adversaries access to corporate information systems, including those of cleared contractors. Globalization, especially the outsourcing of information technology (IT), provides potential adversaries greater access to, and therefore greater opportunity to compromise, hardware and software, including that which goes into our most sensitive military systems.

A foreign intelligence entity that partners with a U.S. commercial entity could exploit the relationship by supplying components destined for incorporation into a targeted technology. The modified hardware or software may maliciously compromise supply chain security, leading to stolen data, system corruption, and operational compromise.

The United States' shift toward outsourcing the development and assembly of IT components reduces the transparency and traceability of the supply chain. This increases the opportunity to insert corrupted software or altered hardware. Yet although international mergers and foreign acquisitions of suppliers may exacerbate the problem, even domestic production processes are not immune.

resale of personally identifiable information and the compromising and selling or leasing of access to computer networks.

Analyst Comment: In the course of such activities, cyber criminals are likely to gain access to information that may be of value to national intelligence services. It is likely that in multiple instances technical and program information from cleared industry was compromised through such collateral collection. Foreign intelligence entities would likely find this information useful in satisfying collection efforts directly or in targeting or vetting potential assets. While clear links between cyber criminal underground elements and national intelligence services for the transmission of such information are not always evident, such a connection probably exists. (Confidence Level: Moderate)

Another notable trend identified through FY10 cleared industry reporting is the increase in suspicious emails containing variants of the Zeus Trojan, which steals online credentials (e.g., usernames, passwords, online banking information).

4. TARGETED TECHNOLOGIES

European and Eurasian governments vary considerably in their goals regarding defense spending, with some continuing a gradual decline and others ramping up. However, many share a goal of producing a considerable portion of their own defense platforms to reduce reliance on foreign military imports, thereby decreasing foreign influence on their policy-making.

Analyst Comment: This dedication to improving indigenous defense industries likely contributed to the high number of SCRs received from industry in FY10

involving *commercial* collectors attempting to fill technological gaps or shortcomings. (Confidence Level: Moderate)

Among the categories of technology targeted by illicit collection attempts in FY10, three historically prominent categories (*aeronautics systems; electronics; and lasers, optics, and sensors*) approximately doubled in reported cases, yet declined as a percentage of total SCRs, with the former top category, *aeronautics*, declining from 22 to 16 percent.

Armaments and energetic materials and positioning, navigation, and time all remained in the range of four to five percent of total SCRs each; *marine systems* was at one percent.

Some other categories, however, showed noteworthy changes from the previous year.

Space systems and information security, which were negligible or nonexistent in FY09, accrued an appreciable number of cases and established themselves at five percent of the total each.

Both *government and commercial* entities sought U.S. technology within the *IS* and *aeronautics* sectors. The targeted systems constituted some of the United States' most cutting-edge technologies, including software, communications, data transmission, imaging, and unmanned aerial systems.

Analyst Comment: These technologies have a wide range of commercial and governmental applications. As militaries within the region engage in modernization campaigns, they will likely continue to target them to upgrade intelligence, surveillance, and reconnaissance (ISR) capabilities. (Confidence Level: High)

TARGETED TECHNOLOGIES

TABLE 3

MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL) CATEGORIES	FY 2010 PERCENT	DEVELOPING SCIENCE AND TECHNOLOGY LIST (DSTL) CATEGORIES	FY 2009 PERCENT
INFORMATION SYSTEMS TECHNOLOGY	26	AERONAUTICS TECHNOLOGY	22
AERONAUTICS SYSTEMS TECHNOLOGY	16	INFORMATION SYSTEMS TECHNOLOGY	16
LASERS, OPTICS, AND SENSORS TECHNOLOGY	12	ELECTRONICS TECHNOLOGY	10
ELECTRONICS TECHNOLOGY	7	SENSORS TECHNOLOGY	10
INFORMATION SECURITY TECHNOLOGY	5	LASER AND OPTICS TECHNOLOGY	9
SPACE SYSTEMS TECHNOLOGY	5	ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	7
ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	4	MARINE SYSTEMS TECHNOLOGY	6
POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	4	UNKNOWN	6
MATERIALS AND PROCESSES TECHNOLOGY	2	POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	5
GROUND SYSTEMS TECHNOLOGY	2	GROUND SYSTEMS TECHNOLOGY	2
SIGNATURE CONTROL TECHNOLOGY	2	NUCLEAR TECHNOLOGY	2
PROCESSING AND MANUFACTURING TECHNOLOGY	1	CHEMICAL TECHNOLOGY	2
MARINE SYSTEMS TECHNOLOGY	1	MATERIALS AND PROCESSING TECHNOLOGY	1
DIRECTED ENERGY SYSTEMS TECHNOLOGY	1	MANUFACTURING AND FABRICATION TECHNOLOGY	1
NUCLEAR SYSTEMS TECHNOLOGY	1	SPACE SYSTEMS TECHNOLOGY	1
BIOLOGICAL TECHNOLOGY	1	DIRECTED AND KINETIC ENERGY TECHNOLOGY	1
CHEMICAL TECHNOLOGY	1	WEAPONS EFFECTS TECHNOLOGY	0
ENERGY SYSTEMS TECHNOLOGY	1	ENERGY SYSTEMS TECHNOLOGY	0
BIOMEDICAL TECHNOLOGY	0	BIOLOGICAL TECHNOLOGY	0
WEAPONS EFFECTS TECHNOLOGY	0	BIOMEDICAL TECHNOLOGY	0
NO MILITARY CRITICAL TECHNOLOGY REQUESTED	6	SIGNATURE CONTROL TECHNOLOGY	0
OTHER*	2		

* Note: Includes cases not otherwise listed

5. ANALYTICAL FORECAST

Because of limited resources, even the strongest and most advanced defense industries in Europe and Eurasia do not have the capability to indigenously produce all the weapons systems and technologies they require. DSS assesses that the region will likely remain a significant threat to U.S. technology and information resident in cleared industry, with no indication of abatement in the coming years.

(Confidence Level: Moderate)

Modernization is a priority across Europe and Eurasia, and its militaries will need to develop new technologies to replace aging and obsolete weapons and systems. DSS assesses that it is likely that *commercial* collectors will continue their attempts to collect sensitive, classified, and export-controlled U.S. defense technologies to boost indigenous military and defense industries and development programs.

(Confidence Level: Moderate)

IS and *aeronautics* systems will likely remain among the top targets for European and Eurasian collectors in FY11. Priorities will likely focus on technologies applicable to strategic nuclear forces and aerospace defenses, command and control and reconnaissance systems, and long-range, high-precision weapons.

(Confidence Level: Moderate)

Increased interest in supplying sensitive technologies to foreign customers also will likely direct collection requirements emanating from Europe and Eurasia. As

the defense industry within the region continues to grow, and especially to the extent that the region is a major arms exporter, third-party transfer of U.S. technology will likely be a concern.

(Confidence Level: Moderate)

DSS assesses that domestic requirements and the region's pattern of third-party transfer will probably drive an increased effort by European and Eurasian entities to collect U.S. export-controlled technology to save money and time, while simultaneously enabling them to develop technologies to counter U.S. systems.

(Confidence Level: Moderate)

Collectors from the Europe and Eurasia region will likely continue to prefer to make requests directly to cleared industry in their efforts to fill technology requirements not satisfied by sanctioned partnerships and exchanges. Depending on the state of their relations with the United States at a particular time, countries within the region will probably shift between *SNA* and *RFIs* coming from *unknown* actors and from *government* entities.

(Confidence Level: Moderate)

CASE STUDY



In 2010, an individual representing a company from Europe and Eurasia contacted a cleared contractor and requested a price quote for export-controlled technology components with defense and space applications. DSS research revealed two previous requests by the same foreign company for information on export-controlled technologies, including an earlier identical request to the same cleared company.

The requesting company also has a connection to a technical European and Eurasian university that performs research and development on a number of technologies with military applications in conjunction with several countries of concern.

Analyst Comment: This case study illustrates the symbiotic, effective, yet often hidden relationships between *commercial*, *academic*, and *government* organizations common in Europe and Eurasia, and their usefulness in obtaining U.S. export-controlled technologies. Persistent requests on the part of commercial firms, combined in some cases with the use of foreign partners that come under less export scrutiny, probably succeeded in filling critical technology gaps in the past. Technologies obtained likely gravitated into the hands of entities able to reverse-engineer and indigenously reproduce items required to expedite national military modernization efforts. (Confidence Level: Moderate)

THIS PAGE INTENTIONALLY LEFT BLANK

SOUTH AND CENTRAL ASIA



SOUTH AND CENTRAL ASIA



1. OVERVIEW

South and Central Asia contains aspiring regional powers and near-world-level players in various categories of accomplishment. Some of the most active collectors in the region engage in active enmities with other countries in the region or nearby.

South and Central Asia remained an active collecting region, registering an increase in reported attempts of over 50 percent from last year. Yet its share of the total reports of foreign collection attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base decreased from fiscal year 2009 (FY09) to FY10, from 15 to 9 percent. As a result, it fell from being the third-ranking to the fourth-ranking region, displaced by Europe and Eurasia.

Commercial entities remained the most common collector affiliation, found on two-thirds of all suspicious contact reports (SCRs) linked to South and Central Asia. *Requests for information (RFIs)* remained the most common method of operation (MO) used by the region's collectors, identified in over three-quarters of the SCRs. And *information systems (IS)* remained the single most sought after technology.

2. COLLECTOR AFFILIATIONS

Using *commercial* entities to seek to obtain illegal or unauthorized access to sensitive or classified information or technologies resident in the U.S. cleared industrial base remained the region's overwhelming favorite, as registered by FY10 SCRs.

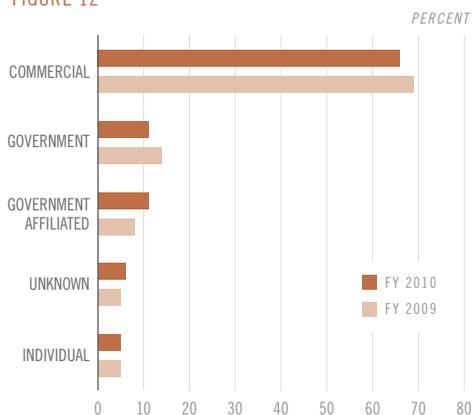
Yet as a percentage of the total, the *commercial* category declined slightly from last year, as did reported attempted collections by *government* entities, while the percentage attributed to *individuals* held steady. *Government-affiliated* and *unknown* entities increased in percentage from last year. However, in the context of the overall reported attempts, the continued strong preference for using *commercial* entities as collection agents, at two-thirds of the total, is the most salient factor.

South and Central Asian defense establishments tend to be state-run but include *commercial* concerns. In FY10, the *commercial* entities' involvement ranged from large private firms supporting the defense industry to small procurement agents and intermediaries.

Analyst Comment: While there has been some movement within South and Central Asia toward privatization, *government-affiliated* entities overwhelmingly dominate the defense procurement process. In the few FY10 cases in which private *commercial* entities without government contracts initiated suspicious contacts to cleared contractors, it is still likely that they were acting pursuant to government needs rather than completely separate profit-seeking projects. (Confidence Level: Moderate)

COLLECTOR AFFILIATIONS

FIGURE 12



South and Central Asia defense establishments typically consist of networks of entities responsible for policymaking, planning, and implementation; research facilities; and factories. In general, the public-sector entities are the major components of the state-run defense industry, while the commercial firms support them. Typically, this support role

involves securing foreign, including U.S., subcomponents and supplying them to larger, indigenous systems designed by government entities.

Analyst Comment: The Defense Security Service (DSS) assesses that it is likely that the majority of FY10 commercial contacts attributable to companies from South and Central Asia occurred while operating in this support role. (Confidence Level: Moderate)

Analysis of cleared industry reporting indicates that state-run design centers and research institutes issue procurement tenders for the needed components. In effect, state-run defense industries use the tenders to task others to be its suppliers. These tenders are often posted on official South and Central Asia government websites accessible to the public, and are complete with technical specifications. In several instances, DSS linked commercial requests to purchase technology directly from cleared contractors to publicly accessible government global tenders issued on behalf of the defense establishment of a government within South and Central Asia.

Analyst Comment: DSS assesses that the majority of the reported suspicious contacts attributable to South and Central Asia *commercial* entities were probably in response to government tender processes. It is likely that in many cases these government-issued global tenders serve as the sole mechanism for tasking these *commercial* entities. (Confidence Level: Moderate)

Commercial defense companies, procurement agents, and U.S.-based middlemen all compete to fulfill these tenders. Numerically, the majority of South and Central Asia *commercial* entities requesting U.S. technology in FY10 were procurement agents and middlemen. Typically, procurement agents from the region accept the tenders and comb the Internet in search of companies marketing products matching the tender specifications. A majority of the cleared contractors targeted by South and Central Asia procurement agents appear to maintain web pages complete with comprehensive product catalogs and contact information.

Once a procurement agent successfully identifies a company marketing the desired product, he typically contacts the company, often through email, seeking a price quote and additional product information or brochures.

Analyst Comment: DSS interprets that, because many procurement agents seek to satisfy the same tenders as their competitors, the actors are likely persistent in their attempts to obtain illegal or unauthorized access to restricted or classified information or technologies resident in the U.S. cleared industrial base. (Confidence Level: Moderate)

Some *commercial* entities maintain strong ties with the military and intelligence agencies of their countries and South and Central Asia procurement agents do so openly, but when successful at acquiring sensitive U.S. technology may also pass it on to third parties. Other South and Central Asia concerns may act as front companies

to procure military technology, hiding the true end user of the technology, then illicitly smuggling it to their home countries.

Analyst Comment: While DSS assesses that many entities acting in response to tenders are legitimate, it is likely that many others attempt and will continue to attempt to illicitly acquire protected technology. (Confidence Level: Moderate)

In comparison to the large *commercial* category, FY10 collection attempts attributed to *government* and *government-affiliated* requests for U.S. technology each made up 11 percent of all reporting with South and Central Asia origins. Most incidents appeared to involve end users seeking to support ongoing projects by directly purchasing systems or acquiring technical information instead of going through the global tender process. Almost all of these incidents involved overt requests in which individuals identified their affiliations and, in some cases, the end use of the requested technology.

Analyst Comment: Despite the seemingly overt nature of many requests, it is likely that seemingly legitimate requests from some South and Central Asian entities were intended for malicious end users; however, DSS could not confirm such diversions of technology during FY10. (Confidence Level: Moderate)

Examples of *government* agents targeting cleared industry involved military attachés at the region's various foreign embassies in Washington, D.C., expressing interest in

purchasing systems, or eliciting professional and personal information from cleared contractor employees at social events.

Government-affiliated scientists and engineers working at research centers reached out to their U.S. counterparts to request information, including pricing and specifications for sensitive systems as well as personal information. In one incident, an entity from South and Central Asia requested contact information, photographs, and lodging information for cleared contractor employees who met with foreign researchers while attending an overseas conference.

Several FY10 SCRs concerned entities listed on the Department of Commerce's Entity List, and it is likely that some *commercial* entities were acting on behalf of other organizations on the Entity List.

Analyst Comment: The primary method that *government* entities use to task procurement agents to acquire certain technologies appears fairly transparent. But because it is very likely that additional tasking avenues outside of the official tender processes exist, not all *commercial* requests can be linked to specific tenders or *government* end users. (Confidence Level: High)

3. METHODS OF OPERATION

As with collector affiliations, proportional rankings remained much the same regarding South and Central Asian MOs between FY09 and FY10. While *RFIs* declined slightly as a percentage of the total, the other categories

retained their relative positions. *RFIs* accounted for over three-quarters of total regional SCRs, far outpacing the number of reports in the next most common category, *solicitation or marketing*.

The majority of the *RFI* attempts were requests to purchase defense technology and inquiries to cleared industry employees asking for pricing information, product brochures, and system specifications for export-controlled or sensitive systems. Many of the contacts with *commercial* origins were likely in response to government-issued global tenders. Consistent with past years' reporting, the requests often constituted responses to advertisements and solicitations on cleared contractor websites.

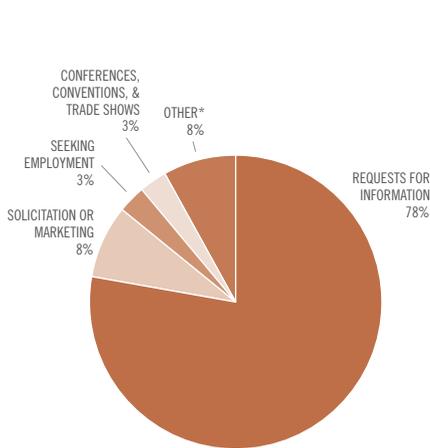
In FY10 industry reporting indicated that most *RFIs* consisted of emails to cleared contractors requesting technical details and pricing information concerning military systems. Notably, DSS observed that a number of legitimate business relationships—initiated via email contact—developed between South and Central Asia entities and cleared contractors. Previous industry reporting indicated that several direct approaches by procurement agents from the region resulted in legitimate sales of export-controlled systems to countries within South and Central Asia.

Analyst Comment: Procurement agents from the region likely view direct email *RFIs*, even when unsolicited, as a legitimate and successful means of initiating a business relationship and conducting business. The reliance on this method by legitimate

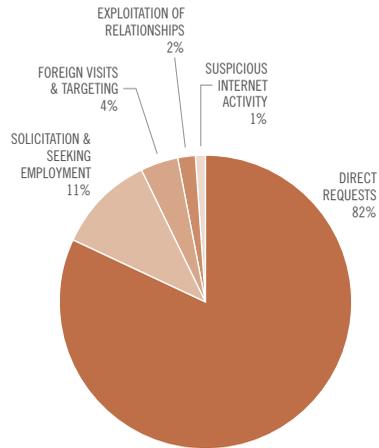
METHODS OF OPERATION

FIGURE 13

FY 2010
PERCENT



FY 2009
PERCENT



*Includes MOs not otherwise listed. Singularly, these methods represent less than one percent of the total.

entities means that not all entities requesting information intend exploitation. (Confidence Level: Moderate)

However, it is difficult to differentiate between those contacts that constitute attempts to violate export control laws through end-use misrepresentation and those that are wholly legitimate. It is likely that suspicious entities conceal nefarious requests among the numerous legitimate ones, and that some otherwise legitimate entities almost certainly have conducted illegal technology transfer. (Confidence Level: Moderate)

The second most common MO used by South and Central Asia collectors was *solicitation or marketing*, followed by *seeking employment* and *conferences, conventions, and trade shows*. Throughout FY10, businesses from the region regularly

contacted a number of cleared contractors in an effort to market their own products or services. Many of these offers involved the outsourcing of work such as software design back to the region.

In FY10, DSS saw a continuation of a trend, first identified during FY09, of the increased use of U.S.-based procurement agents and middlemen to facilitate foreign requests for U.S. technology.

Analyst Comment: Many of these U.S.-based businesses appeared to operate similarly to procurement agents in South and Central Asia. It is likely that countries within the region direct the unauthorized transfer of defense technology. (Confidence Level: Moderate)

4. TARGETED TECHNOLOGIES

The number of reported collection attempts targeting technologies from the Militarily Critical Technologies List (MCTL) increased in all the most targeted categories, with reports in some doubling and even tripling. Within the proportional rankings, there was varied movement among the targeted technologies between FY09 and FY10.

The largest decrease was in the percentage ascribed to the combined category of *lasers, optics and sensors (LO&S)*, from 27 percent last year to 18 percent in FY10. *Electronics* and *aeronautics systems* also registered relative declines.

Increases in the percentage of reported attempted collections linked to South and Central Asia occurred in the *IS; positioning, navigation, and time; and marine systems* categories.

Industry reporting indicated South and Central Asian entities directed their technology acquisition efforts during FY10 toward categories that span the MCTL spectrum, representing a wide variety of technologies with multiple applications. As military and defense systems in the region age, they will need increasingly scarce replacement parts.

Analyst Comment: DSS assesses that it is likely that South and Central Asian entities intend to use the varied technologies they seek to support force modernization requirements and/or system upgrades, both in response to the perceived threat from each other and in support of domestic counterinsurgency efforts.
(Confidence Level: Moderate)

With the above overall picture in mind concerning the many technology areas targeted in FY10, four MCTL categories received the most attention, accounting for a combined total of more than 50 percent of reporting: *IS; LO&S; aeronautics systems; and positioning, navigation, and time.*

In FY10, *IS* was the most targeted category. Types of technologies targeted included secure communication systems, signals intelligence systems, and advanced modeling software. Further scrutiny of the requests revealed that their specific technology foci included software security programs, inertial navigation systems, and communications security equipment. A large component of collection attempts by South and Central Asia entities in FY10 targeted technologies used to integrate existing systems.

Within the *LO&S* category, collecting entities targeted several specific technologies, including up-to-date night vision systems and a variety of electro-optical and thermal imaging systems.

Analyst Comment: The majority of requests for export-controlled imaging systems were for large quantities; these are likely intended to equip operational military or other state-controlled forces. Smaller numbers of such systems appeared destined for use in the monitoring of laboratory testing procedures; such systems will likely aid in the indigenous research and development of other, unknown systems or technologies.
(Confidence Level: Moderate)

TARGETED TECHNOLOGIES

TABLE 4

MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL) CATEGORIES	FY 2010 PERCENT	DEVELOPING SCIENCE AND TECHNOLOGY LIST (DSTL) CATEGORIES	FY 2009 PERCENT
INFORMATION SYSTEMS TECHNOLOGY	18	SENSORS TECHNOLOGY	19
LASERS, OPTICS, AND SENSORS TECHNOLOGY	< 18	ELECTRONICS TECHNOLOGY	17
AERONAUTICS SYSTEMS TECHNOLOGY	9	INFORMATION SYSTEMS TECHNOLOGY	14
POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	< 8	AERONAUTICS TECHNOLOGY	13
ELECTRONICS TECHNOLOGY	< 6	LASER AND OPTICS TECHNOLOGY	8
MARINE SYSTEMS TECHNOLOGY	5	POSITIONING, NAVIGATION, AND TIME TECHNOLOGY	7
INFORMATION SECURITY TECHNOLOGY	5	ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	4
ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY	4	MARINE SYSTEMS TECHNOLOGY	3
SPACE SYSTEMS TECHNOLOGY	4	BIOLOGICAL TECHNOLOGY	3
GROUND SYSTEMS TECHNOLOGY	3	GROUND SYSTEMS TECHNOLOGY	3
PROCESSING AND MANUFACTURING TECHNOLOGY	3	CHEMICAL TECHNOLOGY	2
MATERIALS AND PROCESSES TECHNOLOGY	3	ENERGY SYSTEMS TECHNOLOGY	2
CHEMICAL TECHNOLOGY	2	MATERIALS AND PROCESSING TECHNOLOGY	2
SIGNATURE CONTROL TECHNOLOGY	1	SIGNATURE CONTROL TECHNOLOGY	2
BIOMEDICAL TECHNOLOGY	1	UNKNOWN	2
NUCLEAR SYSTEMS TECHNOLOGY	1	SPACE SYSTEMS TECHNOLOGY	1
BIOLOGICAL TECHNOLOGY	0	BIOMEDICAL TECHNOLOGY	0
DIRECTED ENERGY SYSTEMS TECHNOLOGY	0	DIRECTED AND KINETIC ENERGY TECHNOLOGY	0
ENERGY SYSTEMS TECHNOLOGY	0	MANUFACTURING AND FABRICATION TECHNOLOGY	0
WEAPONS EFFECTS TECHNOLOGY	0	NUCLEAR TECHNOLOGY	0
NO MILITARY CRITICAL TECHNOLOGY REQUESTED	7	WEAPONS EFFECTS TECHNOLOGY	0
OTHER*	4		

* Note: Includes cases not otherwise listed

5. ANALYTICAL FORECAST

Collection efforts in South and Central Asia are driven by several factors. The region currently lacks the indigenous capability to produce much of the military technology it desires. While some countries may have successfully reverse-engineered relatively sophisticated systems, indigenous defense industries are still developing a limited spectrum of technologies likely intended for integration into existing defense systems. It is very likely that South and Central Asian defense industries for the foreseeable future will not be able to produce the sophisticated defense systems many countries in the region feel they need to counter perceived threats, whether from each other or insurgents, and will continue to target U.S. industry information and technology. **(Confidence Level: High)**

These factors mean that South and Central Asia collecting entities will probably continue to look outside the region for needed technologies. South and Central Asian defense industries and militaries will probably show no hesitation in looking overseas to procure defense systems when domestic *commercial*, *government*, and *government-affiliated* suppliers fail to meet expectations. South and Central Asia remains reliant on U.S., European, and other foreign-supplied military systems and technology to support modernization efforts, and it is likely that collection entities will continue to target U.S. technology into the near future. **(Confidence Level: Moderate)**

Collectors from the region will almost certainly continue to target *IS* and *LO&S* technology in support of ongoing military systems development, integration, and/or reverse-engineering efforts.

(Confidence Level: High)

Parts of the region are slowly evolving and the United States is working to ensure the evolution is in a positive direction. Thus, the United States is moving closer to some countries in the region, with export restrictions reduced, and organizations removed from the U.S. Department of Commerce's Entity List. Such steps will likely lead to increased contact between foreign defense industries within the South and Central Asia region and the U.S. defense industrial base, including joint military projects. **(Confidence Level: Moderate)**

DSS assesses that cleared contractors involved in joint projects are likely to be the focus of even more intense collection activities. While industry reporting does not indicate that foreign intelligence entities directly control the targeting of U.S. technology, DSS assesses that it is unlikely the disparate network of South and Central Asia research establishments and public- and private-sector companies, encompassing both the *commercial* and *government-affiliated* categories, will not be employed in a similar MO in the future. **(Confidence Level: Moderate)**

Intra-regional hostilities, inter-regional alliances, and the desire for commercial profit all remain factors. Therefore, DSS assesses that transference of U.S. technology from South and Central Asia to third parties remains likely, and the various resultant relationships remain subject to exploitation. **(Confidence Level: Moderate)**

In the short term, DSS assesses that the *commercial* and *government-affiliated* public-sector defense companies, procurement agents, and intermediaries that are characteristic of South and Central Asia defense establishments will likely continue to generate the largest volume of reporting as they seek to procure components needed for military modernization efforts. **(Confidence Level: Moderate)**

CASE STUDY



In March 2009, a presumed South and Central Asian national contacted a cleared contractor in an attempt to acquire export-controlled parts used in counter-battery radar systems.

In November 2009, a different U.S. cleared contractor received an unsolicited email from the same individual expressing interest in purchasing the same radar system that was requested in the March incident.

The suspicious individual was a representative of a trading company from his home country. Multiple sources indicate that his home government established the trading company as a front company to procure export-controlled technology and equipment for the national military, and that the trading company had previously sought products on behalf of several military services and defense-affiliated entities.

The trading company was the subject of several other SCRs reporting attempts to purchase export-controlled electronics products and communications equipment used in military aircraft.

In another instance, the trading company attempted to procure multiple items on behalf of its government defense procurement agency, which directed the company not to identify the end user.

Analyst Comment: DSS assesses that it is likely that much of this trading company's activity consists of acquisition attempts conducted at the behest of its government's defense and intelligence establishments. Such collection efforts aimed at sensitive U.S. technology probably will continue in FY11. (Confidence Level: Moderate)

OTHER REGIONS



In the past, the Defense Security Service has limited coverage in the unclassified version of *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry* to the four regions most active in collection attempts, as measured by industry reporting. This year, for the first time, DSS included attribution to other world regions of reported cases of illicit collection attempts to provide a more complete picture of world-wide targeting.

Together, reported cases traceable to the Western Hemisphere and Africa combined were less than ten percent of the world total for both FY09 and FY10. However, like all regions, these areas showed increases in reported attempts to obtain illegal or unauthorized access to classified information or technologies resident in the U.S. cleared industrial base. Reported collection attempts from the Western Hemisphere more than doubled from last year.

The Western Hemisphere relies more on *commercial* entities than any other affiliation, although on a percentage basis this tendency declined from last year. Whereas collectors attributed to the African region previously had been overwhelmingly *government* entities, in FY10 over half were *commercial*.

In both FY09 and FY10, both regions relied heavily on direct approaches, now labeled *requests for information (RFIs)*. In FY10, *RFIs* accounted for nearly 60 percent of reported Africa-originated cases and around 70 percent of the Western Hemisphere cases.

Based on industry reporting in FY10, both regions are most actively seeking *information systems; lasers, optics, and sensors; aeronautic systems; and electronics systems*. Regarding Africa, reported collection efforts both increased in numbers from FY09 and broadened in the categories of technologies targeted. Within the FY10 Africa data, DSS analysis identified a focus on unmanned ground and aerial systems and associated technologies. This can likely be attributed to several African nations' desires to increase the intelligence, surveillance, and reconnaissance capabilities of their ground forces to counter internal political instability and threats originating from neighboring countries.

CONCLUSIONS

The technology base of the United States is under constant attack. This pervasive and enduring threat is like the weather: ever-present yet ever changing. Any perceived lull in attacks against our technology base is like the eye of a storm: if you wait five minutes, the aggressiveness and nature of the attack will change. However, unlike the weather, our foes are calculating, cunning, and manipulative.

The foreign entities' motivations may vary from striving for the advantage on some future battlefield to simply stealing information and technology for economic gain. No matter the motivation, any loss of technology to an adversary or competitor degrades our nation's strength both militarily and economically.

In fiscal year 2010 (FY10), the Defense Security Service (DSS) witnessed a stunning increase of over 140 percent in the number of suspicious contact reports (SCRs) determined to be of intelligence value. This growth occurred globally: all regions yielded more SCRs in FY10 than in FY09. The increase likely resulted not only from aggressive foreign collection targeting cleared industry, but also the diligence of cleared industry in identifying and reporting suspicious activity. For example, improved awareness about computer network operations likely accounted for the considerable increase in the number of SCRs reporting suspicious activity on cleared contractor networks.

Technology collection spanned the entire spectrum of categories on the Militarily Critical Technologies List. Industry reporting indicated that *information systems (IS)* received the most attention from foreign entities during FY10. Entities from five of the six geographic regions targeted *IS* technology more than any other sector; entities from Africa targeted *IS* technology equally with *aeronautics* and *lasers, optics, and sensors (LO&S)*. This global tendency to target *IS* technology likely results from continued U.S. dominance in *IS* technology development, design, and integration. Also remaining consistent with previous years, *LO&S* and *aeronautics* were the next most commonly targeted technology sections.

Commercial entities remained the most common collectors in FY10 reporting: DSS attributed 35 percent of suspicious contacts to *commercial* entities, down from 49 percent in FY09. However, the affiliation of the entity often provided no clear indication of the end user. *Commercial* entities regularly target technology based on government-tendered requirements, but some *commercial* entities target technology to gain an advantage over competitor companies rather than in response to a specific requirement identified by their government.

The *unknown* entities category constitutes a growing category of interest, up from 17 percent of the total in FY09 to 26 percent of a larger total in FY10. The increase in

computer network operations targeting cleared industry and the improvement by collecting entities of their ability to conceal their identities when contacting cleared contractors likely caused this growth.

Entities targeting U.S. technologies used *requests for information* most commonly, accounting for nearly half of the reported suspicious incidents. Computer network operations, categorized as *suspicious network activity*, had the greatest increase in number of reports. This likely reflects both persistent cyber collection directed at cleared industry and improved network monitoring by cleared industry.

Academic solicitation enjoyed significant favor among entities from the East Asia and the Pacific and Near East regions. *Academic solicitation*—using students, professors, scientists, and researchers as collectors—was a new category in FY10; previously, DSS had broken *academic solicitation* between the old categories of seeking employment, direct request, and foreign travel, depending on the situation. Globally, *academic solicitation* accounted for six percent of all suspicious contacts; however, it constituted 18 percent of suspicious contacts DSS attributed to the Near East. This MO will likely continue to gain popularity in regions lacking the capacity for sophisticated computer network operations or experience difficulty in acquiring technology due to export controls or economic sanctions.

FY10 witnessed a persistent stream of collection attempts targeting U.S. technologies. Entities from all regions of the globe sought U.S. technologies to obtain an advantage against regional adversaries, replicate U.S. capabilities, develop countermeasures to U.S. systems, or simply profit commercially. Both friends and foes targeted U.S. technologies. Collectors' leading targets were *IS*, *LO&S*, and *aeronautic systems* technologies, but FY10 reporting suggests that foreign entities targeted an even broader spectrum of technologies resident in cleared industry than last year.

ANALYTICAL FORECAST

Maintaining competitiveness, whether militarily or economically, requires access to and application of the latest technologies. Developing innovative technology requires time and resources; some countries save both time and money by pilfering technology developed by others. Foreign collectors, whether they are *government*, *commercial*, or other entities, will likely attempt to steal technology to gain a military or economic advantage. The need for technology and the willingness of some to acquire it through nefarious means will probably continue and grow for the foreseeable future. **(Confidence Level: Moderate)**

U.S. cleared contractors will almost certainly continue to be the prime target of foreign intelligence entities (FIE) seeking to obtain the latest technologies. FIE will very likely target the entire spectrum of technology to improve their countries' military capabilities, develop countermeasures to U.S. and other western systems, or introduce rival systems into the commercial market. **(Confidence Level: High)**

Information systems (IS) technology remained the perennial favored target of FIE targeting cleared industry in fiscal year 2010, and *IS* technology will likely remain the most sought after technology for the foreseeable future. U.S. dominance in the development and application of *IS* makes U.S. cleared industry an attractive target for foreign entities seeking the latest

in *IS* hardware and software technology. Foreign collectors will likely continue to target U.S. technologies relating to *lasers*, *optics*, and *sensors (LO&S)* and aeronautics systems. While *IS*, *LO&S*, and *aeronautics systems* will probably remain the favored technologies, U.S. cleared industry must remain vigilant to protect all sensitive or classified information and technology against likely collection attempts. **(Confidence Level: Moderate)**

Although *requests for information* will very likely remain the most common method of operation, foreign entities will almost certainly increase their use of *suspicious network activity (SNA)* and *academic solicitation*. The dependence on *IS* for project development, information storage, and communication creates vulnerabilities for systems connected to the Internet. With the convenience of the Internet comes vulnerability to computer network exploitation by sophisticated adversaries. Due to the availability of vast amounts of data stored on systems and networks connected to the Internet, foreign entities will almost certainly continue and likely increase their attempts to exploit the Internet to illicitly and covertly obtain information from cleared industry. **(Confidence Level: High)**

Commercial entities will likely remain the most active collector affiliation. However, it is likely that the number of entities categorized

as *unknown* will increase. The anonymity of the Internet and its applications, such as email and web cards, allows collectors to hide their identities. This, combined with the difficulty of tracing sophisticated cyber attacks, points toward the likelihood of an increase in the number of attempted collections that the Defense Security Service will classify as being of *unknown* affiliation. **(Confidence Level: Moderate)**

U.S. cleared contractors will continue to develop advanced and highly sought after technologies. This makes them the primary target for foreign entities seeking to improve their country's abilities or to simply profit from pirating the technology. The pervasive threat to U.S. technology is likely to continue for the foreseeable future; collectors will probably take advantage of any avenue that provides them access to cutting-edge technology. Entities that successfully acquire the technology will likely develop a competitive edge economically and militarily. **(Confidence Level: Moderate)**

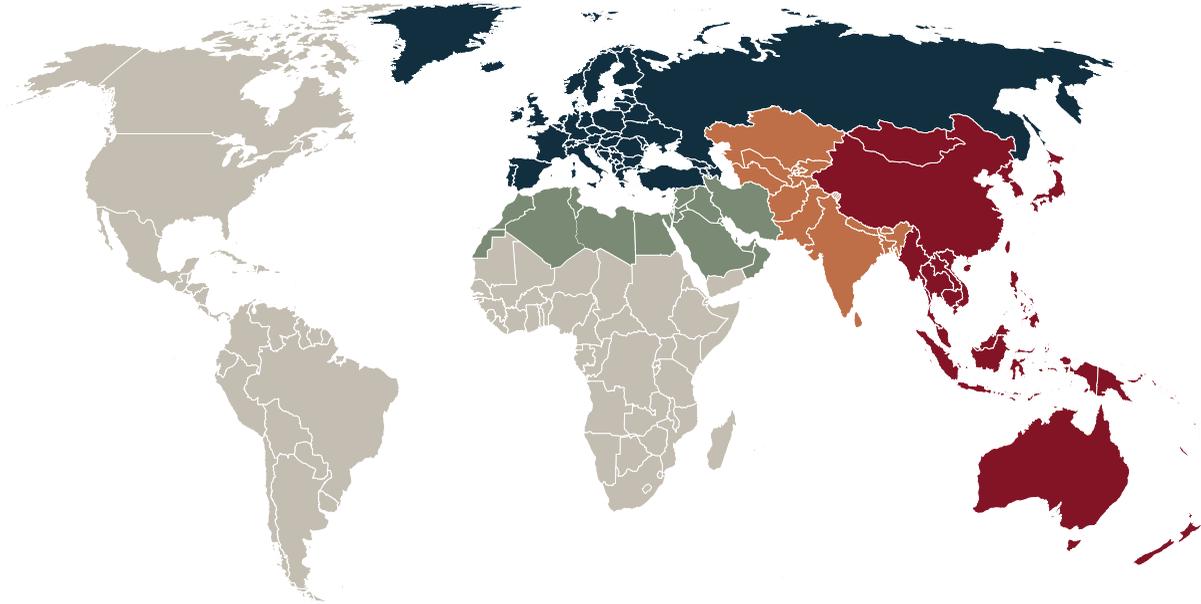
EXPLANATION OF ABBREVIATIONS AND ACRONYMS

ALL ARE U.S. UNLESS OTHERWISE INDICATED

OMITTED: FOREIGN ACRONYMS THAT APPEAR IN ONLY ONE PLACE
(COMPANY NAMES, ACADEMIC INSTITUTIONS, ETC.)

ACIC	Army Counterintelligence Center	IS	information systems
AS	aeronautics systems	ISR	intelligence, surveillance, and reconnaissance
ASW	anti-submarine warfare	IT	information technology
AUV	autonomous underwater vehicle	LO&S	lasers, optics, and sensors
C4ISR	command, control, communications & computers, intelligence, surveillance, and reconnaissance	MCM	mine countermeasures
CI	counterintelligence	MCTL	Militarily Critical Technologies List
CIA	Central Intelligence Agency	MO	method of operation
DIA	Defense Intelligence Agency	NCIS	Naval Criminal Investigative Service
DoD	Department of Defense	NGA	National Geospatial-Intelligence Agency
DOE	Department of Energy	ONCIX	Office of the National Counterintelligence Executive
DSS	Defense Security Service	R&D	research and development
DSTL	Developing Science & Technologies List	RFI	request for information
ERC	End-User Review Committee	SCR	suspicious contact report
FIE	foreign intelligence entity	SLV	space launch vehicle
FOG	fiber-optic gyrocompass	SNA	suspicious network activity
FY	fiscal year	TAA	technical assistance agreement
IC	Intelligence Community	UAS	unmanned aerial system
IP	Internet protocol	URL	uniform resource locator

REFERENCE MAP*



*Note: Map reflects reporting period for fiscal year 2010

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			

REFERENCES

¹ (U); DON; https://www.csp.navy.smil.mil/Files_UUV/UUV's/UUV_MasterPlan_11-9-2004Version.pdf; 9 Nov 2004; The Navy Unmanned Undersea Vehicle (UUV) Master Plan; Extracted and Overall Classification is UNCLASSIFIED; Ref 9 Jun 2010; Background

² (U); Monthly Publication; Offshore Shipping Online; AUV Market to Total US\$2.3 Billion over the Next Decade; 18 Dec 2009; <http://www.oilpubs.com/oso/article.asp?v1=9106>; Ref 24 Nov 2010; Shipping Industry Publication-Background

³ (U) IBID [2]

⁴ (U); Website; National Institute of Standards and Technology, Information Technology Laboratory; Supply Chain Risk Management (SCRM); 19 Nov 2009; p. 1; www.scrm.nist.gov; Ref 13 May 2011; Government Report-Background



