2015 TARGETING U.S. TECHNOLOGIES

A TREND ANALYSIS OF CLEARED INDUSTRY REPORTING

2015 TARGETING U.S. TECHNOLOGIES

A TREND ANALYSIS OF CLEARED INDUSTRY REPORTING

3 PREFACE

4 BACKGROUND

10 EXECUTIVE SUMMARY

14 SPECIAL FOCUS AREA: COUNTERFEIT MICROELECTRONICS

18 REGIONAL ANALYSIS

- EAST ASIA AND THE PACIFIC 18
- NEAR EAST 24
- SOUTH AND CENTRAL ASIA 30
- EUROPE AND EURASIA 36
- OTHER REGIONS 42

44 OUTLOOK

46 APPENDICES

- WEIGHTED RANKING 46
- DSS CATEGORIZATION DESCRIPTIONS 48
- ACRONYMS & ABBREVIATIONS 52
- REGIONAL BREAKDOWN 54

Date of Information: October 1, 2014

Product coordinated with: ACIC, NCIS, & NGA

PAGE INTENTIONALLY LEFT BLANK

PREFACE

Woodrow Wilson once said, “I not only use all the brains that I have, but all that I can borrow.” There is a persistent threat to the United States from foreign collectors that continually try to borrow “brains” and steal intellectual property belonging to the U.S. cleared industrial base. Our adversaries target the cleared industrial base to gain a technological edge and compromise our data. They target technology, personal information, computer networks, and military systems. Information and technology lost to these foreign collectors imperil the lives of our warfighters and the nation’s economic wellbeing.

The Defense Security Service (DSS) is chartered to oversee the protection of U.S. and foreign technologies and classified information resident in the cleared industrial base under the authority of the National Industrial Security Program and its assigned counterintelligence (CI) mission. A critical component of securing the cleared industrial base is the partnership between cleared industry and DSS in protecting information and technology.

Cleared contractors recognize potential collection attempts and report these attempts to DSS. DSS receives these reports, analyzes them to identify foreign collectors targeting U.S. cleared industry, and works to disrupt foreign collection operations directly and in concert with other government agencies. In fiscal year 2014 (FY14), DSS received over 34,000 reports from industry, an 8 percent increase from the previous fiscal year. From these reports, 989 subjects of investigation or operations were identified, which is a 38 percent increase over FY13.

DSS also uses industry reporting to develop analytical assessments to articulate the threat to U.S. information and technology. This annual publication, *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting* reflects the compilation and analysis of the reports received during FY14. DSS produces analytic products, including this report, to improve cleared industry’s and U.S. government agencies’ awareness of who targets cleared industry, what they target, and the methodologies they employ in attempts to gain access to restricted information and technology.

DSS has a responsibility to our partners in cleared industry to provide them with a clear picture of the threat posed by foreign collectors targeting their facilities and personnel. Any time our foes access classified data there is an increased threat to the warfighter, since those adversaries can use that technology to develop countermeasures to our systems or create weapons of greater lethality. DSS intends this publication to provide cleared employees, companies, law enforcement, and intelligence professionals a better understanding of the threat we all face. The more we understand the threat, the better chance we have of thwarting our enemies.

Increased awareness of the technology targeted and the methods our adversaries use enables us to better identify and prevent future illicit attempts. Foreign collectors’ attempts to infiltrate the cleared industrial base can be thwarted by a team effort between DSS, cleared contractors, and law enforcement and intelligence agencies. A constant awareness of the threat, vigilance on behalf of industry, and diligent support from DSS ensures our country remains strong, healthy, and secure.

Stanley L. Sims
Director
Defense Security Service

BACKGROUND

THE ROLE OF THE DEFENSE SECURITY SERVICE

DSS supports national security and the warfighter, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of industry. The DSS CI Directorate identifies threats to U.S. technology and programs resident in cleared industry and articulates the threat for industry and U.S. government leaders.

THE ROLE OF INDUSTRY

In carrying out its mission, DSS relies on the support of cleared contractor employees and the U.S. intelligence and law enforcement communities. Chapter 1, Section 3 of the *National Industrial Security Program Operating Manual (NISPOM),* 5220.22-M, dated February 28, 2006, requires cleared contractors to remain vigilant (in person and online) and report any suspicious contacts to DSS. The process that begins with initial reporting of all such contacts and continues with ongoing and collective analysis reaches its ultimate stage in successful investigations or operations.

In accordance with the reporting requirements laid out in the *NISPOM*, DSS receives and analyzes reports of suspicious contact from cleared contractors. DSS categorizes these reports as suspicious, unsubstantiated, or of no value. For each reported collection attempt, DSS data aggregation and analysis methodologies seek to gather as much information as possible: who instigated the attempt, where it came from, what its aim was, and what methods of collection it used. Comprehensive analysis of information from across all companies and elements of cleared industry forms the basis for this report, and determines the actions DSS takes and the advice it gives to cleared contractors to combat the threat.

Cleared contractor reporting provides information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversion activities to the Federal Bureau of Investigation and DSS. When indicated, DSS refers cases of CI concern to its partners in the law enforcement and intelligence communities for potential exploitation or neutralization. DSS follows up by informing industry of remedial actions that can decrease the threat in the future. This builds awareness and understanding of the individual and collective threats and actions and informs our defenses.

THE REPORT

Department of Defense (DoD) Instruction 5200.39, *Critical Program Information Protection within the DoD*, dated May 29, 2015, requires DSS to publish an annual classified and unclassified report, each detailing suspicious contacts occurring within the cleared contractor community. The focus of this report is on efforts to compromise or exploit cleared personnel, or to obtain unauthorized access to sensitive or classified information and technologies resident in the U.S. cleared industrial base.

Each year DSS publishes *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting* (*Trends*). In this report, the 17th annual *Trends*, DSS provides a snapshot of its findings on foreign collection attempts. It provides a statistical and trend analysis that covers the most prolific foreign collectors targeting the cleared contractor community during FY14, compares that information to the previous year's report, and places that comparison into a larger context.

DoD Instruction 5200.39 requires DSS to provide its reports to the DoD CI community, national entities, the defense contractor community, and DoD component heads. This report constitutes part of DSS' ongoing effort to assist in better protecting the cleared industrial base by raising general threat awareness, encouraging the reporting of incidents as they occur, identifying specific technologies at risk, and applying appropriate countermeasures. 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. DSS previously released a classified version of this report.

DEFENSE SECURITY SERVICE REPORTING DEFINITIONS

DSS sorts each report received from cleared industry pursuant to Section 1-302b of the NISPOM into one of three distinct categories: suspicious contact report (SCR), unsubstantiated contact report (UCR), or assessed no value (ANV). Subsequent information and reevaluation may cause changes in these categorizations, e.g., an SCR may change to a UCR.

SCR – A report DSS receives from cleared industry that contains indicators that it is almost certain, or likely, or there is an even chance that some individual, regardless of nationality, attempted to obtain unauthorized access to sensitive or classified information and technology or to compromise a cleared employee. Reports designated as SCRs represent incidents most likely to have involved actual attempts to do so.

UCR – A report of an incident in which it is unlikely that any individual, regardless of nationality, attempted to obtain unauthorized access to sensitive or classified information and technology or compromised a cleared employee. However, DSS retains such reports, as the aggregate of several UCRs or information obtained subsequently may result in the identification of foreign intelligence activity.

ANV – A report that only remotely represents a CI concern, such as an email or credit card scam. DSS does not retain reporting assessed as ANV.

SCOPE/METHODOLOGY

DSS considers all reports collected from the cleared contractor community. It then applies analytical processes to them, including the DSS foreign intelligence threat assessment methodology. After sorting all reports into the three categories— suspicious contact report (SCR), unsubstantiated contact report (UCR), and assessed no value—we base this publication on SCRs and select UCRs. The analyses also incorporate references to all-source Intelligence Community (IC) reporting.

The *Trends* is organized first by region, then by targeted technology, methods of operation (MO), and collector affiliation (see Appendix for descriptions). It incorporates statistical and trend analyses on each of these areas.

DSS analysts review the SCRs and UCRs of CI concern to determine the threat level the incident poses to actually compromise cleared industry personnel or obtain access to technology or information resident in

cleared industry. The analysts assess each incident based on the actor, action, and targeted technology and apply a threat rating of Low, Medium, High, or Critical to each of the three categories. The combined ranking of the three categories determines the threat score for each report. Therefore, each report that analysts consider of CI concern will have an overall threat ranking of Low, Medium, High, or Critical.

In this year's report, DSS for the first time ranked the regions by the aggregate threat score of all reports associated to that region instead of ranking them based solely on the raw number of reports (see Appendix for more information). Previously, DSS ranked the regions by the share or percentage of the total number of reports for the year.

The weighted ranking represents the region's share of the aggregate threat score of all reports for FY14. For example, entities from the East Asia and the Pacific region accounted for 38 percent of all reports in FY14; however, the threat score for reports associated with this region represented 41 percent of the total weighted score for the reports in FY14. Thus, the ranking represents the assessed threat to U.S. technologies posed by entities from a region not just the volume of incidents associated to those entities.

The weighted ranking system did not cause a shift in the order of the regions as collectors; however, it did impact the comparative threat ranking. The Near East was the second most common collector region identified in 21 percent of the incidents, while the South and Central Asia region account for 15 percent of the incidents, just 6 percent fewer than the Near East. However, when comparing the threat score, the 6 percent difference in raw number of incidents increases to 14 percent, with Near East accounting for 25 percent of the overall aggregate score and the South and Central Asia entities accounting for just 11 percent. This indicates the incidents involving entities from the Near East tended to pose a greater actual threat of transfer of information or technology.

TABLE 1: REGIONAL ENHANCED THREAT DATA

	PERCENTAGE OF REPORTS	THREAT SCORE
East Asia & the Pacific	38%	41%
Near East	21%	25%
South & Central Asia	15%	11%
Europe & Eurasia	12%	9%
Western Hemisphere	7%	6%
Africa	1%	1%

To organize its targeting analysis, DSS applies a system of categories and subcategories that identify and define technologies. DSS analyzes foreign interest in U.S. technology in terms of the 29 sectors of the DSS-developed Industrial Base Technology List (IBTL). The IBTL is a compendium of the science and technology capabilities under development worldwide that have the potential to significantly enhance or degrade U.S. military capabilities in the future.

This publication also refers to the Department of Commerce's Entity List. This list 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) annually examines and makes changes to the list, as required. The ERC includes representatives from the Departments of Commerce, Defense, Energy, State, and, when appropriate, Treasury.

FIGURE 1: INDUSTRIAL BASE TECHNOLOGY LIST

FIGURE 2: METHODS OF OPERATION

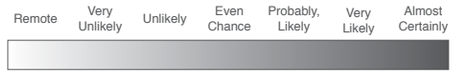
ESTIMATIVE LANGUAGE AND ANALYTIC CONFIDENCE

DSS employs the IC estimative language standard. The words of estimative probability used, such as *we judge*, *we assess*, or *we estimate*, and terms such as *likely* or *indicate*, represent the agency'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, nor do they represent empirically based certainty or knowledge. Some analytical judgments are based directly on collected information, others rest on previous judgments, and both types serve as building blocks. In either variety 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 used to each other.



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

FIGURE 3: COLLECTOR AFFILIATIONS

DSS uses words such as *may* and *suggest* to reflect situations in which DSS is unable to assess the likelihood of an event, 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 made 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

FY14 saw a continued increase in reported foreign collection attempts to obtain sensitive or classified information and technology resident in the U.S. cleared industrial base. The number of reports submitted to DSS rose to over 34,000, an 8 percent increase from FY13.

The six collector regions remained in the same relation to each other in FY14 as in FY13 with regard to the frequency they appeared in industry reporting to DSS. East Asia and the Pacific remained the top collector region in FY14, although the percent of reports attributed to East Asia and the Pacific decreased 6 percent from FY13.

The diminished proportion of reports attributed to East Asia and the Pacific entities was primarily the result of a decrease in reports associated with suspicious network activity (SNA). A temporary decrease occurred during and following a series of public reports released by expert private sector cyber sources that detailed cyber collection operations from East Asia and Pacific entities. Conversely, DSS analysis disclosed East Asia and the Pacific countries possibly used this slow down to refine and hone collection actions as the information identified in these attacks appeared to be of greater value.

The continued decrease in reports of SNA allowed academic solicitation, which slightly increased from FY13, to remain the top reported MO at 23 percent. Reports linked to attempted acquisition of technology (AAT) also increased slightly and made this MO the second most common in FY14. SNA dropped from second to third place in FY14. Solicitation or marketing services' share of reporting increased by 5 percent accounting for this MO moving into the top four.

With regards to the IBTL, the top five targeted technology sectors remained the same as FY13. The electronics sector topped the list at 7 percent, with command, control, communication, and computers (C4) (6 percent); aeronautic systems (6 percent); software (4 percent); and marine systems (3 percent) finishing out the top five.

The remaining reported collection efforts targeted a variety of technologies covering 24 additional sectors; however, none of these individually accounted for more than 3 percent. With associations to six different IBTL categories, gray-market microelectronics pose a critical threat to U.S. military system readiness. The special focus area of this publication addresses counterfeit microelectronic devices in further detail.

In FY14, commercial remained the top collector affiliation at 34 percent of overall reporting. The government-affiliated category experienced no change in FY14, remaining in second place with 27 percent. The most notable change in collector affiliations was evident in the unknown category, which moved from fifth to third place.

KEY POINTS

Key points are based on FY14 cleared industry reporting

EAST ASIA AND THE PACIFIC

- Continued to be the most prolific collector region, accounting for 38 percent of all reports
- Emphasized targeting electronics, C4, and aeronautic systems
- Though it remains a top threat, SNA reports dropped more than 50 percent in FY14 while academic solicitation increased
- Commercial entities were the most common collectors in FY14, experiencing an 11 percent increase in share of reporting

NEAR EAST

- Continued to leverage a network of intermediaries, procurement agents, and front companies to obtain information resident in cleared industry
- Aeronautic systems technology was the most targeted category in FY14, and collection attempts focused on platforms that would enhance indigenous capabilities
- Academic solicitation remained the most prominent MO used by Near East collectors
- Government-affiliated collectors remained the most prevalent, accounting for 43 percent of the total

SOUTH AND CENTRAL ASIA

- Military modernization continued to influence the technologies targeted by South and Central Asia collectors; electronics remained the technology targeted most often
- Seeking employment and academic solicitation remained the top two MOs, as entities from this region continued attempts to gain employment, internships, and research positions at cleared facilities or institutions associated with classified research
- A significant increase in reports linked to commercial collectors led to this affiliation's move from third to first

EUROPE AND EURASIA

- The top three targeted technologies – C4, aeronautic systems, and electronics – made up almost a quarter of all reporting related to Europe and Eurasia
- AAT remained the most reported MO, but solicitation or marketing services quadrupled and became the next most common
- Commercial entities were the most reported collector

FIGURE 4: FY14 REPORTING SUMMARY

Each region legend illustrates the percentage of reporting associated with that region; the threat level DSS attributed to the region; the percentage of change in reporting compared to last year; and the top technologies, methods of operation, and collector affiliations. This information is explained in greater detail within the respective region sections of this publication. Regions and categories are listed in order of prevalence based on overall FY14 reporting.

Top Targeted Technologies

- Electronics
- Command, Control, Communication, & Computers
- Aeronautics
- Software
- Marine Systems
- Armament & Survivability
- Optics
- Materials: Raw & Processed
- Radars
- Energy Systems

Top Methods of Operation

- Academic Solicitation
- Attempted Acquisition of Technology
- Suspicious Network Activity
- Solicitation or Marketing Services
- Request for Information
- Seeking Employment
- Foreign Visit
- Exploitation of Relationships

Top Collector Affiliations

- Commercial
- Government Affiliated
- Unknown
- Individual
- Government

EAST ASIA & THE PACIFIC 38%

Threat Level: **CRITICAL**

No change in reporting

Top Targeted Technology: **Electronics**

Top Method of Operation: **Academic Solicitation**

Top Collector Affiliation: **Commercial**

NEAR EAST 21%

Threat Level: **HIGH**

Reporting increased by **34%**

Top Targeted Technology: **Aeronautic Systems**

Top Method of Operation: **Academic Solicitation**

Top Collector Affiliation: **Government Affiliated**

SOUTH & CENTRAL ASIA 15%

Threat Level: **MEDIUM**

Reporting increased by **11%**

Top Targeted Technology: **Electronics**

Top Method of Operation: **Seeking Employment**

Top Collector Affiliation: **Commercial**

EUROPE & EURASIA 12%

Threat Level: **MEDIUM**

Reporting increased by **18%**

Top Targeted Technology: **Command, Control, Communication, & Computers**

Top Method of Operation: **Attempted Acquisition of Technology**

Top Collector Affiliation: **Commercial**

WESTERN HEMISPHERE 7%

Threat Level: **MEDIUM**

Reporting increased by **35%**

Top Targeted Technology: **Electronics**

Top Method of Operation: **Request for Information**

Top Collector Affiliation: **Commercial**

AFRICA 1%

Threat Level: **LOW**

Reporting increased by **35%**

Top Targeted Technology: **Aeronautic Systems**

Top Method of Operation: **Request for Information**

Top Collector Affiliation: **Commercial**

SPECIAL FOCUS AREA:
COUNTERFEIT MICROELECTRONICS

OVERVIEW

Counterfeit microelectronic devices represent a threat to DoD systems. Counterfeits that could significantly degrade, tamper, or disrupt the performance of DoD systems can enter the DoD's supply chain in various ways. For example, an unscrupulous employee can allow defective microelectronics to pass inspection and be sold as a properly performing device. Also, the DoD has a tremendous need for obsolete and rare microelectronics for sustainment activities. As the lucrative gray market develops into an essential source for obsolete and rare microelectronics, the DoD becomes proportionately more dependent on this market.

While it is rare that DoD or cleared contractors would turn directly to overseas gray market businesses, DSS has identified U.S. companies, primarily independent distributors and brokers, who are importing microelectronics from suspected counterfeiters overseas and are actively soliciting cleared contractors for business. Additionally, these same U.S. companies are also attempting to procure export-controlled microelectronics for various foreign government entities.

Private sector suppliers that provide the DoD with microelectronics obtained via the gray market are a significant CI concern. The introduction of counterfeit, non-conforming, and substandard materials and goods into DoD and cleared industry supply chains poses a threat to U.S. national security. The intent of this special focus area is to alert cleared industry to the supply chain, counterfeit, and export diversion threat posed by brokerage entities operating in the gray market.

DOD SUPPLY CHAINS INUNDATED BY COUNTERFEIT MICROELECTRONICS

In 2011, DSS began supporting the National Intellectual Property Rights Coordination (IPR) Center, which is charged with leading the U.S. Government response to intellectual property theft. In June 2011, the IPR Center, under leadership from Immigration and Customs Enforcement – Homeland Security Investigations, implemented a multi-agency law enforcement initiative named CHAIN REACTION with the objective of stemming the introduction of counterfeit goods into U.S. Government supply chains and a primary emphasis on the DoD and microelectronics.

To date, CHAIN REACTION Task Force efforts have led to the identification of numerous U.S. companies, primarily independent distributors and brokerage entities that import microelectronics from known or highly suspected overseas counterfeit shippers. Importers of counterfeit microelectronics are mostly small businesses operating as independent distributors or brokers, many of which publicly associate themselves with the DoD and pride themselves as being able to provide obsolete or rare microelectronic components.

After reviewing reporting from cleared industry, DSS identified multiple interactions between cleared contractors and the U.S. companies identified as part of CHAIN REACTION. Many of these interactions were attempts to solicit cleared contractors for business or attempts to procure export-controlled microelectronics for various foreign government entities. Many of these U.S. companies are under criminal investigation for either counterfeit importation or export violations; eight have been debarred and three convicted in criminal court.

TERMS USED IN THIS SECTION

Gray Market: The trade of a commodity primarily via independent distributors and brokers that, while legal, is unofficial, unauthorized, or unintended by the original manufacturer

Counterfeits: Substandard, substituted, or cloned microelectronics that are often of low quality and unable to perform to required specifications.

FIGURE 5: PREVALENCE OF OBSOLETE MICROELECTRONICS

Microelectronics obsolescence is not just a sustainment issue. A recent Institute for Defense Analyses study found that a significant number of technologies in the development and production phases incorporate obsolete microelectronics.

DEVELOPMENT AND PRODUCTION

During the initial acquisition process,
at least 21% of microelectronics
are either discontinued or at risk of being discontinued.

SUSTAINMENT

During the sustainment phase,
at least 63% of microelectronics
are either discontinued or at risk of being discontinued.

EXAMPLES FROM CLEARED CONTRACTORS

After examining reporting from cleared industry, DSS cataloged numerous interactions between cleared contractors and entities suspected of doing business at the behest of foreign government end users. Notable examples include:

- A commercial broker that has contracts with the DoD has provided counterfeit microelectronics to a cleared contractor and openly conducts business with foreign customers. In one incident, this entity attempted to procure export-controlled microelectronics, likely for a foreign government-affiliated end user.
- Multiple cleared contractors have had interactions with a known foreign government procurement agent. This entity also imports microelectronics from known or suspected overseas counterfeiters.
- One microelectronics brokerage entity attempted to procure export-controlled radiation-hardened integrated circuits. The individual who requested the parts previously plead guilty to willfully engaging in brokering activities or facilitating the export and transfer of defense articles and defense services, specifically brokering the export of thermal imaging and infrared technology to entities in the East Asia and the Pacific region. This microelectronics brokerage entity also has multiple DoD contracts.
- Several independent distributors or brokerage entities contacted a

FIGURE 6: MICROELECTRONIC SECURITY TIPS

Cleared contractors should place greater scrutiny or increased awareness in the following areas:

BE WARY OF LOW PRICES

Microelectronic parts offered at prices significantly lower than prices offered at authorized distributors.

BE WARY OF SHORTER LEAD TIMES

Microelectronic parts offered with lead times significantly shorter than those from the original equipment manufacturer (OEM).

VET EXTERNAL TESTING HOUSES

When using an external testing house for counterfeit detection, ensure that the facility is an established, trusted entity.

VISUAL DETECTION MAY NOT BE ENOUGH

Counterfeiting techniques have advanced significantly over the last 5 years; visual detection or solvent testing may not be enough to determine whether a part is counterfeit or genuine.

CONSIDER LIFETIME BUYS

Contractors should consider lifetime buys. OEMs publicize that they will discontinue a part roughly 1 year in advance. If those parts may be needed in the future, the upfront costs of a lifetime buy may outweigh the risks and overall costs of doing business in the hard-to-find and obsolete microelectronics gray market.

cleared contractor and attempted to fraudulently purchase microelectronics. These entities also used the cleared contractor's corporate identity in attempt to spoof real business.

CONCLUSION

It is essential that cleared industry remains vigilant and continues to report these types of suspicious interactions originating from independent microelectronics distributors and brokerage entities.

As the reporting from cleared industry indicates, location alone does not define what is suspicious. Foreign intelligence services and research institutes are using U.S.-based independent distributors and brokerage entities to acquire export-controlled microelectronics. Often, these same U.S.-based businesses are supplying counterfeit or otherwise substandard microelectronic parts to cleared contractors and the DoD.

Through increased CI awareness, vigilance, and commercial due diligence, cleared contractors can increasingly identify these illicit actors and reduce the overall threat posed by these entities.

Analyst Comment: DSS assesses it is almost certain foreign intelligence entities (FIEs) possess the capability to introduce non-conforming or malicious microelectronics into the supply chains of cleared industry. However, DSS lacks sufficient specific information to determine whether FIEs intend to exploit the vulnerabilities inherent within cleared industry's supply chains. (Confidence level: High)

PAGE INTENTIONALLY LEFT BLANK

EAST ASIA AND THE PACIFIC

Based on FY14 reporting, East Asia and the Pacific entities remained the most active collectors of sensitive or classified information and technology resident in the cleared industrial base. Although the share of reports attributed to East Asia and the Pacific decreased by 6 percent, the number of incidents reported remained the same. Collectors from this region continue to pose a significant threat to the United States.

The East Asia and the Pacific region represents a growing economic force and constitutes a competitive economic environment, especially concerning defense technology. Multiple countries in this region perceive neighboring states to be hostile, and geopolitical conflicts over land and sea border claims exacerbate existing rivalries. This situation motivates East Asia and the Pacific entities to target technologies that benefit their respective militaries.

As support for military modernization continues, East Asia and the Pacific states focus on research and development (R&D) of indigenous systems in parallel with targeting technology and information related to similar Western systems. East Asia and the Pacific entities perceive the United States as a source of useful military technology and information.

Reporting from FY14 revealed East Asia and the Pacific entities' interest in obtaining component systems and enabling technologies. Included in the targeting of these enabling technologies was the continued trend of targeting electronics that could be used in a variety of military or civilian projects.

While East Asia and the Pacific entities targeted almost all technology areas of the IBTL, the top five targeted technologies—electronics, C4, aeronautic systems, software, and marine systems—remained the same as FY13.

In FY14 industry reporting, the preferred MO was academic solicitation, representing 24 percent of the total. The other favored MOs included solicitation or marketing services, AAT, and SNA. The solicitation or marketing services and AAT MOs showed an increase from FY13, which continues the trend towards more human-enabled targeting.

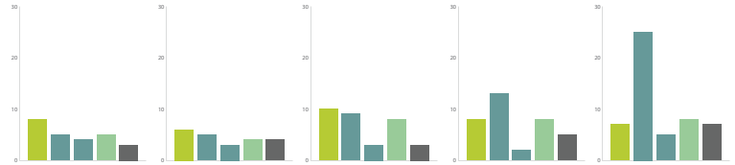
Collector affiliations for FY14 showed a significant change from FY13. In FY14, the number of cases attributed to commercial collectors increased by 11 percent. Another noteworthy change was an 18 percent decrease in the number of reports attributed to government collectors, which dropped this category from first to fourth place.

TARGETED TECHNOLOGIES

East Asia and the Pacific entities targeted virtually every category on the IBTL in FY14. The top targeted technology in FY14 remained electronics, followed in order by C4, aeronautic systems, software, and marine systems. Also of note, analysis identified no IBTL technology in 35 percent of cases, and the targeted technology remained unknown in 12 percent of cases.

Electronics remained the most targeted single technology sector in FY14 industry reporting related to East Asia and the Pacific. Reported requests often cited components that contribute to space programs since this

FIGURE 8: FIVE YEAR TOP TARGETED TECHNOLOGY OVERVIEW



	FY14	FY13	FY12	FY11	FY10
	INDUSTRIAL BASE TECHNOLOGY LIST		MILITARILY CRITICAL TECHNOLOGIES LIST		
Electronics	8%	6%	10%	8%	7%
Command, Control, Communication, & Computers	5%	5%	Information Systems 9%	13%	25%
Software	4%	3%	Information Security 3%	2%	5%
Aeronautic Systems	5%	4%	8%	8%	8%
Marine Systems	3%	4%	3%	5%	7%

is an area of focused modernization for the region. Cleared industry reported numerous requests for space-qualified electronics, including ones that are International Traffic in Arms Regulation (ITAR)-controlled. A variety of civilian and military space systems incorporate these electronics, including missiles, traveling wave tube replacements, and satellites.

Efforts within East Asia and the Pacific to modernize military technology, particularly satellite and naval programs that provide options against regional rivals, continue to be substantial. IC observers believe regional powers are actively pursuing an anti-access/area denial (A2/AD) capability to deter U.S. intervention in a possible regional conflict. Broader goals of modernization include enhancing naval capabilities to defend territorial claims in the South and East China Seas and ensure maritime sovereignty.

In order to achieve space and naval superiority along with A2/AD capabilities, East Asia and the Pacific states are upgrading their C4 systems. This focus is evident as C4 was the second most commonly targeted technology sector in FY14. East Asia and the Pacific entities often sought C4 components that would enhance battlefield communication, including airborne data acquisition systems, antennas, and connectors.

After the technology categories of electronics and C4, East Asia and the Pacific collectors targeted aeronautic systems most often. Within this category, collection efforts focused on fighter aircraft and unmanned

aerial vehicles (UAVs). East Asia and the Pacific entities continue to target U.S. technology in an attempt to reverse-engineer any advanced technology they may obtain. In addition, states in this region target U.S. technology in order to develop countermeasures and increase domestic R&D by integrating Western technology and expertise.

East Asia and the Pacific commercial entities have been known to share facilities, personnel, and research institutes (RIs) with government entities while simultaneously maintaining relationships with U.S. aviation companies for developmental work related to indigenous aircraft. East Asia and the Pacific government entities have leveraged these joint ventures to attempt to collect sensitive aerospace information and technology.

Analyst Comment: The purpose behind some of these attempts is likely two-fold. Not only do East Asia and the Pacific militaries probably view these technologies as responsive to collection requirements for integration into mission critical systems, but they also provide information on U.S. capabilities to improve their targeting and evasion capabilities for near-term conflicts. Targeted technology components are likely destined for integration in military and commercial products for domestic use and export. (Confidence Level: Moderate)

Software was another technology category that saw an increase in targeting in FY14. While the software targeted is primarily used in satellites, it can also be used in aircraft, missiles, and other exo-atmospheric vehicles. In FY14, cleared industry reporting documented that East Asia and the Pacific academics and individuals tied to regional militaries conducted various aggressive collection efforts against U.S. modeling and simulation software.

Armament and survivability technologies experienced a slight increase in FY14. East Asia and the Pacific collectors continued to focus their efforts on specific technologies that could be useful for responding to a conventional military conflict. These technologies included guns, missiles, rockets, and personal protective equipment.

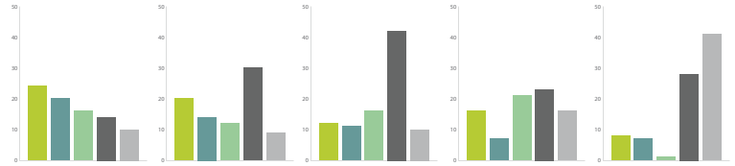
The East Asia and the Pacific practice of using the academic solicitation MO as part of long-term efforts to develop a knowledge base that can support development of emerging technologies was apparent in relation to many of the targeted technologies. Many East Asia and the Pacific academics leverage their placement to gain knowledge that allows regional states to advance R&D cycles by integrating basic capabilities into advanced military research projects. These areas of research included marine systems, nanotechnology, and materials: raw and processed. Access to U.S. information and technology through academic placement continues to be an area of concern.

METHODS OF OPERATION

The number of East Asia and the Pacific-connected academic solicitation cases increased by nearly 17 percent, its share of incidents increased by 4 percent in FY14, making it the most prevalent MO. The use of solicitation or marketing services and AAT also experienced slight increases in FY14, making these MOs second and third respectively. The most significant change in MOs was East Asia and the Pacific entities use of SNA, which dropped from the most common MO to fourth place.

FY14 reporting from cleared industry revealed an increase in East Asia and the Pacific collectors requesting positions in universities or research programs with a military focus. Continued use of this MO provided evidence of a long-range, forward-thinking approach to promoting indigenous technology development. A bulk of East Asia and the Pacific solicitations sought postgraduate research positions related to a variety of topics that included electronics, software, and aeronautic systems.

FIGURE 9: FIVE YEAR TOP METHOD OF OPERATION OVERVIEW



	FY14	FY13	FY12	FY11	FY10
Academic Solicitation	24%	20%	12%	16%	8%
Solicitation or Marketing Services	20%	14%	11%	7%	7%
Attempted Acquisition of Technology	16%	12%	16%	21%	*not assessed
Suspicious Network Activity	14%	30%	42%	23%	28%
Request for Information	10%	9%	10%	16%	41%

Analyst Comment: Access to cleared contractor information and technology related to these fields could further the long-term strategic defense goals of East Asia and the Pacific countries. These goals include developing indigenous capabilities that will likely reduce dependence on or vulnerability to U.S. technology and will enable such a country to dominate its region. (Confidence Level: Moderate)

Solicitation or marketing services was the second most common MO in FY14. East Asia and the Pacific collectors pursued business opportunities with cleared contractors in order to exploit U.S. information and technology. With an increase in AAT, the third most common MO, FY14 saw a marked increase in human-enabled targeting. These methods of targeting cleared industry put sensitive or classified technology and information at risk.

Analyst Comment: Although many instances of cleared industry exploitation, particularly counterfeiting, are probably profit-motivated, others likely represent an effort to obtain U.S. technology to advance military R&D capabilities or degrade critical U.S. military systems. (Confidence Level: Moderate)

There was a marked decrease in East Asia and the Pacific entities' use of the SNA MO in FY14. However, even as East Asia and the Pacific collectors seemingly relied less on SNA, regional actors remain the top cyber threat to cleared industry.

The U.S. government and commercial entities continued to publicize computer network exploitation (CNE) attacks from

FIGURE 10: FIVE YEAR COLLECTOR AFFILIATION OVERVIEW

	FY14	FY13	FY12	FY11	FY10
Commercial	>38%	27%	28%	31%	35%
Government Affiliated	>31%	27%	17%	15%	17%
Individual	11%	10%	7%	20%	8%
Government	>10%	28%	41%	25%	12%
Unknown	9%	8%	7%	9%	28%

East Asia and the Pacific actors, which resulted in the temporary cessation or reduced use of existing SNA tactics and infrastructure. Reporting cataloged much of the infrastructure; command and control protocols; and tactics, techniques, and procedures East Asia and the Pacific cyber actors used. Other government agencies also provided industry with additional technical indicators that can help identify suspicious activity.

East Asia and the Pacific CNE tactics constantly evolve as various sets of regional cyber actors learn from previous efforts, progress in their skills, and become more active. East Asia and the Pacific methodologies reflect increasingly sophisticated technical capabilities and intelligence practices. East Asia and the Pacific actors continue to defeat cleared industry network defenses. Fortunately, community reporting of SNA against cleared contractors provides indications and warnings to aid in mitigating and alerting others to planned or ongoing activity.

In FY14, spear phishing remained a common cyber activity used by East Asia and the Pacific actors to gain initial access to networks. Other activities included website exploitation, compromised credentials, network scanning, brute-force attacks, and distributed denial of service. It is important for network defenders to determine the method used to deliver malware since knowing the delivery method allows network defenders to defeat some attacks.

Many of the request for information (RFI) collection attempts consisted of email or web-card requests for price quotes, export requirements, or product specifications. In many cases, the requestor did not identify the end user or was vague about the intended application. East Asia and the Pacific entities also continued to use the foreign visit MO. Countries from the region that succeed in establishing favorable trade relationships with the United States gain significant access to cleared industry. In numerous reported cases in FY14, visiting delegations included known or suspected intelligence officers (IOs).

COLLECTOR AFFILIATIONS

Reports attributed to commercial entities were the highest they have been in the last 5 years. Commercial collectors can serve as nonofficial collectors of U.S. technology, often with ties back to RIs or state militaries. Another pattern in cleared industry reporting involved various East Asia and the Pacific companies that requested to purchase U.S. information and technology but resisted providing end-user and end-use data, often in an attempt to mask a military-affiliated end user.

Compared to the commercial affiliation, government-affiliated rose in share by about 4 percent. In FY14, reports citing the government-affiliated category often resulted from East Asia and the Pacific university researchers and students submitting resumes. Academics seeking internships and postdoctoral positions continuously submitted resumes for positions within U.S. defense programs.

Analyst Comment: Many East Asia and the Pacific academics likely exploit their placement and access with a cleared contractor, both wittingly and unwittingly, to benefit their nation's R&D efforts by obtaining basic research information or directly acquiring and transshipping sensitive U.S. technology. (Confidence Level: Moderate)

In FY14, government-affiliated entities also included RIs and state-owned enterprises. Although many RIs work on commercial or dual-use technologies, they are also primary contributors to their countries' military R&D. The IC assessed that any technology shared with them is at risk and could be incorporated into the production lines of one or more East Asia and the Pacific militaries.

Reported cases attributed to individual collectors experienced only a slight increase in FY14. Even with a slight increase in cases, this affiliation's share of the total remains relatively low because DSS is often able to identify some connection between individuals and a commercial company, government, or government-affiliated RI. The group with the greatest change was government collectors. Reports linked to government collectors decreased more than 18 percent in FY14, dropping this affiliation from first to fourth.

Analyst Comment: The drop in government collectors could be explained through a similar decrease in SNA. In FY14, U.S. government and commercial firms continued to publicize East Asia and the Pacific CNE activity. This attention could account for the decrease in SNA conducted by government entities. (Confidence Level: Moderate)

NEAR EAST

As a region, the Near East is subject to a great deal of turmoil. FY14 was no different and regional concerns and struggles continued to influence the technology and information sought by Near East collectors. Reflecting existing and potential conflicts, FY14 Near East reporting corroborated IC assessments that Near East entities continued to seek a wide variety of military and dual-use technologies.

Industry and IC reporting indicated that Near East collectors actively attempted to obtain unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. These foreign entities targeted information and technologies that would be helpful in maintaining indigenous defense operations and developmental programs. Near East collectors leveraged procurement agents, front companies, personal contact during foreign visits, and the direct pursuit or acquisition of defense technology information.

The Near East region contains aspiring states, regional powers, and world players in various categories of achievement. Some of the most active collector countries in the region have active enmities with other countries in the region or nearby. Many of the states in this region consider it imperative to maintain capable militaries. While the various states have different relationships with the United States, all seek to gain as much advantage from whatever access to U.S. sensitive or classified technology they can gain.

Based on industry reporting to DSS in FY14, entities tied to the Near East were the second most active in attempts to obtain unauthorized access to information and technology resident in the cleared industrial base. The number of reported collection efforts linked to the Near East increased by 34 percent from FY13.

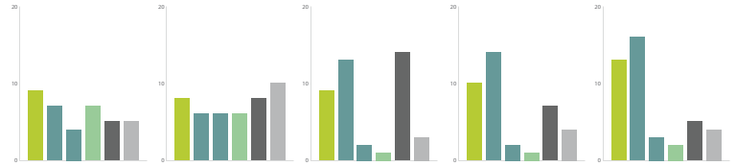
In FY14, government-affiliated collectors remained the most prevalent collectors while academic solicitation was the most common MO. Near East collectors targeted aeronautic systems most frequently in FY14; however, the Near East spread its collection efforts over a wide range of technologies.

TARGETED TECHNOLOGIES

In FY14, Near East collection efforts spanned most categories of the IBTL. Regional collectors most commonly targeted technology related to aeronautic systems, C4, and energy systems. The most noteworthy change from FY13 involved the targeting of marine systems, which dropped from the most targeted technology to fifth in FY14.

During FY14, academic solicitation heavily influenced which IBTL technologies were subject to targeting, as the most reported technology sectors tended to be linked to student interest in gaining entry to specific U.S. research programs. Aeronautic systems technology was the Near East collectors' most targeted category in FY14. Near East collection attempts focused on platforms that would enhance indigenous capabilities and be useful in warfare against likely regional opponents. Documented Near East collection attempts often sought unspecified source code information dealing with airframe design software. Near East collectors also

FIGURE 11: FIVE YEAR TOP TARGETED TECHNOLOGY OVERVIEW



	FY14	FY13	FY12	FY11	FY10
	INDUSTRIAL BASE TECHNOLOGY LIST		MILITARILY CRITICAL TECHNOLOGIES LIST		
Aeronautic Systems	9%	8%	9%	10%	13%
Command, Control, Communication, & Computers	7%	6%	Information Systems 13%	14%	16%
Software	4%	6%	Information Security 2%	2%	3%
Energy Systems	7%	6%	1%	1%	2%
Electronics	5%	8%	14%	7%	5%
Marine Systems	5%	10%	3%	4%	4%

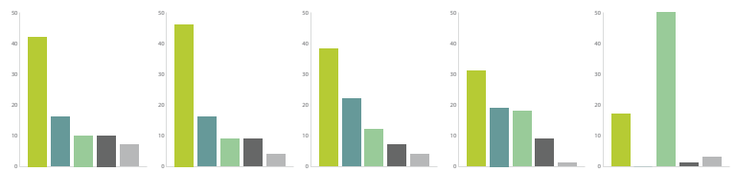
used academic solicitation to target energy systems.

Consistent with FY13, Near East entities continued to target C4 technologies, to include airborne and vehicle-based radio platforms. These enabling technologies allow Near East states to enhance indigenous production capabilities and sustain a competitive advantage with regard to military programs.

Near East entities continued to display an interest in electronics, although relevant FY14 industry reporting showed a decline in the number of cases and a 3 percent decrease in the share of the total, dropping the technology to fourth place. Near East collectors focused on a variety of dual-use components. These components became the subject of collection efforts involving academia, front companies and third parties, and CNE.

Analyst Comment: DSS assesses the drop in reporting related to electronics is likely more of an anomaly owing to the various techniques Near East collectors use to acquire such components. Owing to the MOs employed, electronics almost certainly will continue to represent a collection priority for Near East collectors. (Confidence Level: High)

FIGURE 12: FIVE YEAR TOP METHOD OF OPERATION OVERVIEW



	FY14	FY13	FY12	FY11	FY10
Academic Solicitation	42%	46%	38%	31%	17%
Attempted Acquisition of Technology	16%	16%	22%	19%	*not assessed
Request for Information	10%	9%	12%	18%	50%
Foreign Visit	10%	9%	7%	9%	1%
Suspicious Network Activity	7%	4%	4%	1%	3%

METHODS OF OPERATION

During FY14, and similar to the previous 3 years, academic solicitation remained the most prominent MO used by Near East collectors, accounting for 42 percent of industry submissions. The next nearest category was AAT at 16 percent.

The majority of academic solicitations to cleared industry involved Near East students seeking research positions at U.S. universities involved in sensitive and/or classified research for the DoD. According to IC reporting, Near East regimes leverage placement in academic positions in order to facilitate collection efforts against emerging U.S. DoD and civilian technical research.

As in FY13, AAT remained the second most common MO used in FY14, remaining at 16 percent. Near East entities attempted to acquire a variety of export-controlled enabling technologies, often focusing on aeronautic systems. Additional reporting indicates Near East procurement agents were often reluctant to provide end-user or end-use information, obscuring the ultimate recipient.

Analyst Comment: Restricted Near East end users almost certainly exploit third country procurement agents or lax export control systems to circumvent U.S. trade controls. (Confidence Level: Moderate)

The RFI and foreign visit MOs experienced a slight increase in FY14; however, the most significant change in MO was the employment of SNA. Near East CNE programs continue to evolve along with improving tactics, techniques, and procedures. While some Near East

FIGURE 13: FIVE YEAR COLLECTOR AFFILIATION OVERVIEW

	FY14	FY13	FY12	FY11	FY10
Government Affiliated	43%	44%	47%	35%	27%
Commercial	26%	>22%	<28%	31%	34%
Individual	>13%	17%	11%	17%	18%
Government	>10%	11%	10%	11%	14%
Unknown	>7%	>5%	<5%	6%	7%

CNE programs are associated with their governments, others are linked to information technology companies.

Analyst Comment: Based on recent employment of increasingly sophisticated technical exploits, Near East cyber actors have likely capitalized on experience gained from previous SNA attempts. This experience has probably led to an increase in the level of sophistication of CNE programs and an increase in SNA success. (Confidence Level: Moderate)

COLLECTOR AFFILIATIONS

In FY14, DSS attributed 43 percent of reported collection activity to government-affiliated collectors. While this was a slight decrease from FY13, government-affiliated collectors remained the most active—a consistent trend from previous years. These collectors continued to be associated with government-linked firms or public universities.

Near East reports saw a slight increase in commercial entities targeting U.S. technology and information. Similar to previous years, commercial collectors remained the second most active in the Near East at 26 percent, the lowest share among the four main collector regions.

It is worth noting that much of the collection activity traceable to the Near East has historically come through procurement networks consisting of front companies and third-party intermediaries. However, Near East collectors have also successfully employed several different MOs in order to acquire U.S. information and technology.

Industry reporting reflects that some of the commercial entities that target U.S. information and technology cooperate with national intelligence services. Some of these firms allow intelligence services to include IOs within delegations that visit cleared facilities.

Analyst Comment: DSS assesses foreign collectors very likely embed IOs within commercial delegations to provide a legitimate cover when visiting cleared contractor facilities. (Confidence Level: Moderate)

Individual collectors accounted for 13 percent of the overall number of reports attributed to the Near East region. While this is a decrease from FY13, individual collectors continued to be responsible for academic solicitation and seeking employment MOs. These collectors often focused on U.S. academic programs or businesses that had military applications.

PAGE INTENTIONALLY LEFT BLANK

SOUTH AND CENTRAL ASIA

Cleared industry reporting in FY14 showed that South and Central Asia collectors continued to target a wide variety of U.S. information and technology. The number of reported incidents tied to South and Central Asia entities increased by nearly 11 percent from FY13. South and Central Asia remained the third most attributed region in FY14 reporting of foreign collection attempts against technology and information resident in the U.S. cleared industrial base. This region accounted for 15 percent of the total reports of foreign collection attempts.

States within South and Central Asia continued to focus on military modernization. U.S. information and technology presented a prime target for South and Central Asia collectors as this knowledge could contribute to the development of indigenous military production capabilities and reverse-engineering of acquired foreign defense systems.

U.S. relations with South and Central Asia continued to improve in FY14. However, in the past, South and Central Asia countries have provided U.S. technology to third countries, and the ties between South and Central Asia and problematic third countries represents a continued significant threat to U.S. defense technology.

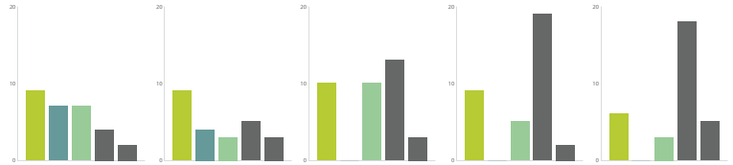
Long-standing regional frictions have made South and Central Asia a volatile region. Some state security and intelligence agencies may attempt to use ongoing or potential future conflicts to leverage support for aggressive collection activity against sensitive or classified information and technology resident in the U.S. cleared industrial base.

Electronics remained the most targeted technology in FY14 at 9 percent of the total. The continued focus on military modernization made electronics a prime target for collectors. Along with electronics, the next most commonly targeted categories – nanotechnology, materials: raw and processed, C4, and radars – account for one-third of all targeted technologies. Nanotechnology and materials: raw and processed both experienced an increase from FY13.

Seeking employment and academic solicitation remained the top two MOs for South and Central Asia collectors, as entities from this region continued attempts to gain employment, internships, and research positions at cleared facilities or institutions associated with classified research. The combined number of reports involving these two MOs accounted for 65 percent of the total. Although AAT experienced a slightly decreased share from FY13, it remained the third most prevalent MO. RFI and solicitation or marketing services finished out the top five. As in FY13, these cases mostly involved commercial entities serving as procurement agents by attempting to obtain technology for South and Central Asia militaries or government organizations.

In FY14, there was a significant switch in collector affiliations. While FY13 saw a large jump in the number of cases related to individual collectors, this affiliation experienced a 12 percent drop in share and a nearly 24 percent decrease in the number of incidents in FY14, moving it from first to third. On the other hand, reports linked to commercial collectors increased by 41 percent, making this the most frequently

FIGURE 14: FIVE YEAR TOP TARGETED TECHNOLOGY OVERVIEW



	FY14	FY13	FY12	FY11	FY10
	INDUSTRIAL BASE TECHNOLOGY LIST		MILITARILY CRITICAL TECHNOLOGIES LIST		
Electronics	9%	9%	15%	9%	6%
Nanotechnology	7%	4%	*not captured under MCTL		
Materials: Raw & Processed	7%	3%	Materials & Processes 10%	5%	3%
Command, Control, Communication, & Computers	4%	5%	Information Systems 13%	19%	18%
Software	2%	3%	Information Security 3%	2%	5%

reported collector affiliation in FY14, up from third in FY13. Government-affiliated collectors stayed the second most commonly reported collectors in FY14.

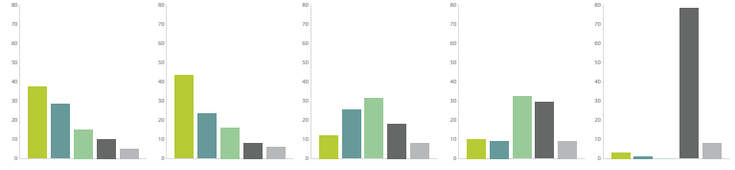
TARGETED TECHNOLOGIES

South and Central Asia states desire to enhance their countries' indigenous technological capabilities and continue to focus on military modernization. Regional states continue to prepare for potential conflicts with both intra- and extra-regional opponents. Overall, South and Central Asia states seek to gain a military edge over rivals, boost their existing operational defenses, and bolster their defense industries. Acquisition of foreign military technology can fill near-term gaps while exploitation of these technologies through reverse-engineering can enhance future R&D efforts.

Electronics remained the top targeted technology sector for FY14. Sought after electronics included space-qualified and enabling components. South and Central Asia entities often focused on these enabling components rather than entire systems. Many of the components can be assimilated into multiple weapon and military platforms, including communication, electronic warfare, and space systems.

The second and third most targeted technologies for FY14 included nanotechnology and materials: raw and processed. These technology sectors both experienced increases in the overall percentage of technology targeted by South and Central Asia collectors. C4 and radars

FIGURE 15: FIVE YEAR TOP METHOD OF OPERATION OVERVIEW



	FY14	FY13	FY12	FY11	FY10
Seeking Employment	37%	43%	12%	10%	3%
Academic Solicitation	28%	23%	25%	9%	1%
Attempted Acquisition of Technology	15%	16%	31%	32%	*not assessed
Request for Information	10%	8%	18%	29%	78%
Solicitation or Marketing Services	5%	6%	8%	9%	8%

accounted for the fourth and fifth targeted sectors, respectively.

Analyst Comment: The focus on C4 and radar technologies could reflect South and Central Asia state armies' efforts to upgrade their C4 and radar platforms because of tensions with rival neighbors. (Confidence Level: Moderate)

Marine systems were another target for South and Central Asia entities soliciting cleared contractors for research positions and postdoctoral degrees. Multiple littoral states admit their desire to dominate the Indian Ocean region and counter any current or emerging threats close to their coastlines. As a result, some South and Central Asia states are engaged in aggressive efforts to modernize their naval capabilities. Targeted cleared contractor programs were often involved in underwater acoustics or fluid dynamics.

METHODS OF OPERATION

There was not a significant change in the MOs used by South and Central Asia collectors for FY14. Seeking employment and academic solicitation remained the top two MOs. Although seeking employment decreased in the share of reporting, together these two MOs still account for 65 percent of all FY14 industry reports of incidents attributed to South and Central Asia entities. AAT and RFI remained commonly used MOs, accounting for 15 and 10 percent, respectively.

The reported incidents involving seeking employment and academic solicitation largely consisted of South and Central Asia

FIGURE 16: FIVE YEAR COLLECTOR AFFILIATION OVERVIEW

	FY14	FY13	FY12	FY11	FY10
Commercial	31%	24%	36%	47%	66%
Government Affiliated	29%	33%	37%	18%	11%
Individual	24%	36%	17%	18%	>5%
Unknown	12%	4%	4%	7%	6%
Government	4%	3%	6%	10%	>11%

collectors requesting research positions at cleared contractor components of academic institutions and applying for positions in cleared industry.

Analyst Comment: DSS assesses South and Central Asian entities' successful use of these two MOs could likely gain access to restricted knowledge and potentially pass this information back to their respective states. (Confidence Level: Moderate)

AAT and RFI incidents often consisted of South and Central Asia companies (both commercial and state-owned) emailing cleared contractors to request sensitive information, such as pricing or technical specifications, or to attempt to acquire export-controlled technology, usually specific components or platforms.

South and Central Asia companies in FY14 also employed the solicitation or marketing services MO. These incidents primarily consisted of solicitations to cleared industry to market a cleared contractor's technology to regional customers. In some instances, these contacts also expressed interest in technologies that could enhance indigenous research and development.

COLLECTOR AFFILIATIONS

In FY14, commercial collectors accounted for 31 percent of the total reported collection attempts by South and Central Asia. Contacts from commercial entities often consisted of RFIs and AATs directed toward cleared contractors via email messages and webcard submissions, and approaches during conferences, conventions, and trade shows. While many of these requests

appeared straightforward, some commercial companies attempted to obscure the ultimate end user to acquire technology on U.S. restricted end-user lists.

Commercial and government-affiliated entities were the top two collectors supplying restricted end users. While government-affiliated collectors remained the second most prevalent in FY14, this affiliation showed a 4 percent decrease in the share of reporting from FY13. Government-affiliated collectors often consisted of students, researchers, and professors from regional institutions of higher learning. Government-affiliated entities were also commercial companies attempting to fulfill tenders and procure technology on behalf of national military services or other governmental organizations.

The most noteworthy change in affiliations occurred in the individual category. Reports involving individual collectors decreased by nearly 24 percent in FY14, dropping this affiliation from first to third overall. Individual collectors primarily consisted of job seekers who applied for positions throughout cleared industry, often in response to vacancy announcements from cleared contractors that clearly state requirement for U.S. citizenship or a security clearance for sensitive positions.

Analyst Comment: An increase in academic solicitation from institutes supporting the government or requests from commercial companies with links to official government tenders likely attributes for the drop in the individual collector affiliation. (Confidence Level: Moderate)

PAGE INTENTIONALLY LEFT BLANK

EUROPE AND EURASIA

In FY14, industry reports of foreign collection attempts from Europe and Eurasia increased by nearly 18 percent. Multiple countries within the region continued to be active collectors. However, Europe and Eurasia remained the fourth most reported region, responsible for 12 percent of total reporting.

Many states within the Europe and Eurasia region are currently focused on campaigns to upgrade and update national militaries to retain their advantage. Approaches to modernization vary depending on the country and include substantial investments in indigenous military R&D, acquisition via outright foreign purchase, and illicit acquisition of technology resident in the U.S. cleared industrial base. Europe and Eurasia's militaries continue to develop or acquire a range of top quality marine, aviation, space, and unmanned weapons systems. This is especially evident in the face of conflicts and peacekeeping activities in which regional countries found themselves involved in during FY14.

Entities from Europe and Eurasia continued to show an interest in a diverse range of technologies. The most commonly targeted technology for FY14 was C4 at 10 percent. Aeronautic systems and electronics rounded out the top three targeted areas, accounting for 6 percent of FY14 reports each. Together these three categories made up over a fifth of all reporting related to Europe and Eurasia.

Militaries from Europe and Eurasia tend to be interested in cutting-edge technologies, and remain heavily dependent on their innovative commercial sectors. The commercial collector affiliation stayed the top collector affiliation and saw a 9 percent increase in the share of reporting from FY13. Many Europe and Eurasia states are allies with the United States, which presents ample opportunity for direct business or joint ventures.

While AAT remained the most commonly reported MO in FY14 industry reporting at 22 percent, solicitation or marketing services became the second most cited at 21 percent, up from 5 percent in FY13. The RFI and foreign visit MOs both experienced increases in FY14.

TARGETED TECHNOLOGIES

In FY14, C4, aeronautic systems, and electronics made up the top three technologies most targeted by Europe and Eurasia entities. States within the Europe and Eurasia region continue to focus their efforts on modernization, and these technologies can be used across numerous military platforms. These technologies were also the most commonly targeted in overall industry reporting.

The most targeted technology sector in FY14 was C4, accounting for 10 percent of all Europe and Eurasia-related industry reporting. Countries seeking to modernize their militaries or improve their defense capabilities technology often start with C4 systems to make their armed forces more mobile and adaptable. Additional goals include improving the ability to monitor and control military operations. These regimes seek to speed up decision cycles and improve communications security and situational awareness.

The aeronautic systems technology sector constituted the second most common technology area Europe and Eurasia entities targeted in FY14 industry reporting. Europe and Eurasia collectors continued to show a notable interest in UAVs.

Analyst Comment: Attempts to acquire information and technology related to aeronautic systems almost certainly fall in line with regional military modernization efforts. (Confidence Level: High)

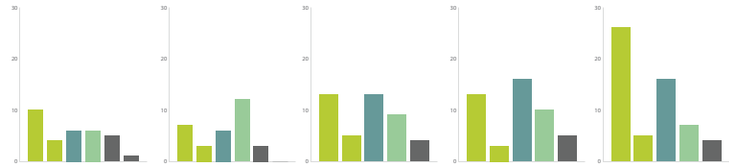
Despite a decrease from FY13 reporting and falling from first to third, electronics remained one of the top three targeted technologies. Much of the interest in the electronics sector concerned space applications, especially certain types of circuitry in which U.S. cleared contractors remain the world leaders. Europe and Eurasia entities also targeted ITAR-controlled technologies.

Analyst Comment: DSS assesses there is an even chance European organizations would use such electronics technology in indigenous R&D programs. DSS cannot rule out that some collectors would transfer such sensitive technology or information to third countries of concern. (Confidence Level: Moderate)

METHODS OF OPERATION

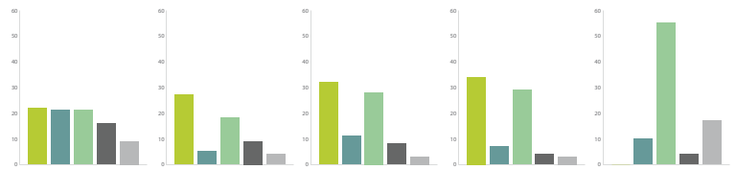
Based on industry reporting, AAT has been Europe and Eurasia entities' most commonly used MO for the last 4 years. Even with a

FIGURE 17: FIVE YEAR TOP TARGETED TECHNOLOGY OVERVIEW



	FY14	FY13	FY12	FY11	FY10
	INDUSTRIAL BASE TECHNOLOGY LIST		MILITARILY CRITICAL TECHNOLOGIES LIST		
Command, Control, Communication, & Computers	10%	7%	Information Systems 13%	13%	26%
Software	4%	3%	Information Security 5%	3%	5%
Aeronautic Systems	6%	6%	13%	16%	16%
Electronics	6%	12%	9%	10%	7%
Armament & Survivability	5%	3%			
			Armaments & Energetic Materials 4%	5%	4%
Energetic Materials	1%	0%			

FIGURE 18: FIVE YEAR TOP METHOD OF OPERATION OVERVIEW



	FY14	FY13	FY12	FY11	FY10
Attempted Acquisition of Technology	22%	27%	32%	34%	*not assessed
Solicitation or Marketing Services	21%	5%	11%	7%	10%
Request for Information	21%	18%	28%	29%	55%
Foreign Visit	16%	9%	8%	4%	4%
Suspicious Network Activity	9%	4%	3%	3%	17%

slight decrease in the number of cases, AAT's share was 22 percent of total reporting in FY14. Common approaches consisted of sending direct, forthright, and specific emails seeking to purchase technology. Europe and Eurasia employed the solicitation or marketing services MO almost as often as AAT in FY14, making it the second most common at 21 percent. The use of this MO increased its portion by 16 percent from FY13. In some instances, Europe and Eurasia companies contacted cleared contractors with offers to act as their agent or distributor in the region, while others proposed collaboration on R&D in overlapping areas or joint commercial ventures.

The next most commonly reported MO in FY14 was RFI, also at 21 percent. Europe and Eurasia entities generally used email for their RFIs, sending questions regarding the cleared contractor's technology. The subject matter of the inquiries ranged from pricing information to technical details and capabilities.

The foreign visit MO almost doubled its portion from FY13 to FY14; making it the fourth most common MO. Visitors to cleared contractors often comprised an official delegation that sometimes included known or suspected IOs.

Together, the top four MOs account for four-fifths of all reporting attributed to Europe and Eurasia. SNA showed a slight increase from FY13; however, its share of the reporting remained below 10 percent. Despite the numbers, Europe and Eurasia entities maintain highly sophisticated cyber programs that have a long history of conducting cyber operations at a level that

FIGURE 19: FIVE YEAR COLLECTOR AFFILIATION OVERVIEW

	FY14	FY13	FY12	FY11	FY10
Commercial	47%	38%	>43%	<45%	31%
Government	14%	10%	11%	<12%	12%
Government Affilaited	14%	>15%	19%	19%	13%
Individual	14%	>31%	15%	<15%	16%
Unknown	11%	5%	>11%	10%	28%

presents a persistent and primary threat to U.S. systems.

COLLECTOR AFFILIATIONS

For the past 5 years, commercial affiliated entities remained the top collectors. In FY14, the commercial affiliation experienced a 9 percent increase in the total share of reporting. Many countries from the region are allies of the United States and are comparable with regard to level of economic development, industrial infrastructure, and innovative ability.

Analyst Comment: Though largely legitimate, DSS cannot rule out that while Europe and Eurasia commercial companies often approach their U.S. counterparts directly, a portion of the interactions consist of nefarious activity.

At times, Europe and Eurasia entities have attempted to slip illicit requests in among the large volume of legitimate business exchanges with U.S. companies. (Confidence Level: Moderate)

The next three collector affiliations – government, government-affiliated, and individual – each accounted for 14 percent of total reporting. Government collectors experienced a slight increase, which moved this affiliation from fourth to second in FY14. Government-affiliated collectors included research and educational institutions with government connections.

The most notable change in collector affiliations involved the individual category. In FY14, the individual collector affiliation decreased its share of reporting by 17 percent, dropping it from the second most common collector affiliation in FY13 to

the fourth most reported in FY14. Many approaches consisted of individuals from Europe and Eurasia seeking employment with cleared contractors or soliciting academic institutions for research and similar positions.

Analyst Comment: Because of the close relationship with the United States, in many cases, Europe and Eurasia entities willingly disclosed their affiliation with government organizations. (Confidence Level: Moderate)

PAGE INTENTIONALLY LEFT BLANK

OTHER REGIONS

In FY14, entities from the Western Hemisphere and Africa regions increased the number of reported attempts to target U.S. technologies. The number of incidents associated with each region increased by more than a third. Collectively, entities from the two regions accounted for 8 percent of cleared industry's reporting. These regions' share of overall reporting in FY14 was the most since FY10, and this is the second consecutive year these regions increased their portion of attempted targeting of cleared industry.

WESTERN HEMISPHERE

Suspicious incidents reported by cleared industry associated with entities in the Western Hemisphere increased by 35 percent in FY14 over FY13. These entities accounted for 7 percent of cleared industry reporting in FY14. Western Hemisphere entities have been consistent in targeted technologies and the methods they employ in their attempts to obtain information and technology from cleared industry.

Based on industry reporting, Western Hemisphere collectors continued to most frequently target electronics, C4, and aeronautic systems. FY14 was the third consecutive year that DSS attributed these entities with most frequently targeting electronics. During the past 3 years, Western Hemisphere entities have targeted electronics in over 14 percent of their reported collection attempts. In FY14, commercial entities requesting information from cleared contractors or attempting to purchase technology accounted for over 70 percent of collection attempts originating in this region and targeting electronics.

Entities from this region have consistently targeted C4, and its Militarily Critical Technologies List (MCTL) predecessor information systems, as one of the top three most sought after technologies for the past 5 years. Similarly, aeronautic systems technology has remained one of the top four most targeted technologies by these entities in each of the past 5 years.

Western Hemisphere collectors relied heavily on RFI, as it has been the most used MO by these collectors in each of the last 5 years. In FY14, these collectors applied this approach in one-third of their attempts to collect information and technology from cleared industry. For the past 2 years, solicitation or marking services and AAT were the second and third most common approaches. Collectively, for the past 2 years these three MOs have accounted for over 65 percent of the suspicious contacts DSS attributed to collectors from the Western Hemisphere.

For the past 5 years, the top three affiliations for collectors from this region have remained consistent with commercial the most common affiliation, followed by individual, and unknown. In addition, collectors from these affiliations account for over 94 percent of the incidents originating in the Western Hemisphere targeting electronics, C4, and aeronautic systems.

Analyst Comment: The significant involvement of commercial, individual, and unknown entities from this region in targeting is very likely due in part to nations in this region not wanting government and government-affiliated entities to be identified targeting U.S. cleared industry. In addition, it is very likely some of these entities are the front end of collection networks originating in other regions, or independent brokers responding to tenders from other regions. (Confidence level: Moderate)

AFRICA

Africa remained the least active region in respect to targeting information and technology in cleared industry. Over the past 5 years, entities from Africa account for less than 1 percent of industry reporting. DSS attributed a 34 percent increase in the volume of incidents originating from Africa in FY14 over FY13, despite still accounting for just 1 percent of the total reporting in FY14.

In FY14, collectors from Africa demonstrated the greatest interest in C4, aeronautic systems, and armament and survivability technologies. During FY14, collectors from this region targeted C4 and aeronautic systems equally in terms of the number of reported incidents. However, these collectors demonstrated a more aggressive targeting of C4. The C4 category was the only targeted technology category to have an incident originating from this region assessed as a high threat. For the past 5 years, collectors from the Africa region have steadily pursued C4 as one of the top four most targeted technologies.

In each of the past 5 years, aeronautic systems technology has been the most or second most targeted technology in incidents DSS attributed to these collectors. Cleared industry reporting identified armament and survivability as the targeted technology in 8 percent of the collection attempts from this region. This is a noticeable change from FY13 when these collectors did not target armament and survivability in a single reported incident.

Analyst Comment: The renewed focus on armament and survivability along with a similar but less significant increase in collection targeting ground systems technology may be to meet requirements related to the regional response to Islamic terrorist organizations operating in the region. (Confidence level: Low)

Entities from Africa primarily used RFI, AAT, and foreign visits to target information and technology from cleared industry. These three MOs accounted for 82 percent of the incidents DSS attributed to this region. Entities used RFI in nearly 79 percent of the incidents targeting C4. In these instances, collectors most commonly requested information relating to cellular communication intercept and tracking systems or airborne radio intercept equipment.

Cleared industry reporting identified commercial entities in 49 percent of the suspicious incidents attributed to entities in Africa. This is consistent over the past 5 years with commercial collectors accounting for no less than 36 percent each year since FY10. These commercial entities most commonly sought aeronautic systems technology, specifically UAV components primarily for quad rotor UAVs.

Analyst Comment: The number of collection attempts DSS attributes to entities in the Western Hemisphere and Africa regions will likely continue to increase. However, entities from these two regions will continue to be less active collectors of U.S. technologies than those from the other four regions and will continue to collectively account for less than 10 percent of cleared industry reporting. (Confidence level: High)

OUTLOOK

DSS assesses that foreign entities will almost certainly continue to target cleared industry in efforts to obtain unauthorized access to sensitive or classified U.S. information and technology. Reporting from cleared industry has increased for the past decade, and there is little sign that foreign targeting will abate in the near future. (Confidence Level: High)

The most active collector regions will almost certainly remain the same, although their ranking may shift. For the last 8 years, entities from East Asia and the Pacific and the Near East have remained the top reported collectors. Entities from these regions will almost certainly continue using a variety of MOs in their illicit acquisition attempts. Additionally, foreign entities' collection efforts will almost certainly continue to target a wide variety of sensitive or classified technologies resident in cleared industry, spanning the spectrum of the IBTL. (Confidence Level: High)

East Asia and the Pacific, South and Central Asia, and Europe and Eurasia are all engaged in active and aggressive military modernization programs that will likely continue to influence targeting conducted by entities from those regions. These modernization programs will likely drive the targeting of marine systems, C4, electronics, and space systems technologies to fill perceived military technology gaps. Indigenous industries in those regions will likely use any technologies obtained to further their research and development and reverse-engineering programs. (Confidence Level: Moderate)

In 5 to 10 years, foreign collectors will likely increase targeting of the emerging technologies of computational modeling of human behavior, quantum systems, synthetic biology, and cognitive neuroscience. For the past 2 years targeting of these emerging technologies has represented less than one-tenth of a percent of all collection attempts. (Confidence Level: Moderate)

As the relevant sciences and technologies mature, spread from universities and research centers, and are applied to actual programs, these emerging technologies will likely increase their share of industry reporting but remain a small portion of overall collection. FIEs linked to the four top collector regions will likely increase their targeting of these technologies in order to enhance research and development efforts and to apply them to military applications. (Confidence Level: Moderate)

Academic solicitation, SNA, and AAT have topped the list of MOs for the last 3 years. While RFIs have dropped in overall percentage of reporting for the past 5 years, the actual number of reports still continues to rise. These MOs will very likely remain a top tactics because they are minimal-risk, low-cost methods for targeting sensitive or classified U.S. information and technology. (Confidence Level: High)

Academic solicitation will likely continue to grow in its share of industry reporting in coming years. Over the past 5 years, academic solicitation has steadily risen from less than 10 percent to almost a quarter of all reports from cleared industry. Entities from East Asia and the Pacific, the Near East, and South and Central Asia will likely continue to apply to university programs for positions in areas conducting research and development related to sensitive or classified U.S. technologies. Also, entities will likely continue to seek employment with cleared contractors; however, not at the same rate as academic solicitations based on the trend of past reporting. (Confidence Level: High)

While entities will almost certainly continue to use SNA to target cleared contractor networks for access to sensitive or classified U.S. technologies, DSS has observed a decrease in reporting of SNA over the past 2 years. Cleared contractors have improved their ability to detect and defeat cyber attacks, assisted by both government information and reports from private firms. Even given these defensive efforts, cyber actors will almost certainly continue to conduct spear-phishing attacks and attempt network intrusions, as well as continue to adjust existing exploitation techniques and develop new ones. Entities from East Asia and the Pacific and the Near East will very likely continue their attempts to exploit this avenue to potentially access cleared industry and government networks. (Confidence Level: High)

Given the global marketplace, cleared industry continues to develop foreign partnerships and business opportunities. Entities from East Asia and the Pacific, the Near East, and South and Central Asia will likely continue to exploit relationships with the United States and U.S. cleared industry to collect sensitive or classified information and technology. Joint ventures and close partnerships can potentially leave contractors vulnerable to the exploitation of relationships and foreign visits. (Confidence Level: High)

Increasing globalization has fostered advanced technology sales across borders where the end user cannot always be determined. The majority of these efforts will likely continue to be for legal and legitimate business purposes; however, hostile elements will almost certainly orchestrate a portion of these foreign endeavors to attempt to gain access to sensitive or classified U.S. technology for unauthorized transfer. (Confidence Level: High)

Foreign collectors will continue to target cleared employees to gain access to U.S. technologies and information, and "borrow" the brains of cleared industry. Unfortunately, once borrowed, the information is lost forever, and its loss over time will likely diminish a U.S. battlefield or economic advantage. The threat shows no sign of waning, and securing our cutting-edge technology remains the key to maintaining our military and economic advantage. Foreign entities will likely adapt their methods of targeting U.S. technologies, and while the specific technologies targeted may change, the persistence and aggressiveness of those entities will almost certainly remain. (Confidence Level: High)

WEIGHTED RANKING

APPLYING WEIGHTED RANKING TO DETERMINE RISK TO U.S. TECHNOLOGIES

As stated in the Background section of this report, in FY14, DSS analysts continued to assess each incident based on the actor, action, and targeted technology. Analysts also applied a threat rating of Low, Medium, High, or Critical to each of the three categories. The combined ranking of the three categories determined the threat score for each report. Therefore, each report that analysts consider of CI concern has an overall threat score of Low, Medium, High, or Critical. The threat score represents the likelihood that a foreign entity acquired the information or targeted technology, the value of the technology to the adversary, and the consequence of the loss to U.S. national security. This appendix explains the weighted ranking system and demonstrates the impact of threat scoring.

As this is the first year SCRs received a threat score, DSS did not use the threat score in FY14 to compare to data from previous years. Within each region, analysts continued to use the percentage of reported incidents to identify the top targeted technologies, MOs, and collector affiliation. However, DSS did apply the weighted threat score for ranking the regions' overall threat to U.S. technologies in FY14.

To apply the threat score to the overall data set, reports received a weighted rank based on the analysts' threat score for the reported incident.

In the weighted ranking, the aggregate of all the reports' threat scores replaces the total number of reports in determining the risk to a technology. The threat score for an individual region, or the risk posed to a specific technology, is the share of this aggregate score. For example, entities from the East Asia and the Pacific region accounted for 38 percent of all reports in FY14; however, the threat score for reports associated with this region represented 41 percent of the total weighted score for the reports in FY14. This higher threat score is due to DSS identifying entities from this region in a large portion of the incidents rated as Critical and High. Of all the reports DSS rated as critical, DSS associated 76 percent to the East Asia and the Pacific region. DSS also attributed 63 percent of the reports rated as High to this region.

Applying the weighted ranking to FY14 data further identified electronics as the targeted technology most at risk from foreign collectors. Electronics was the only IBTL category with a threat score that varied more than one point from the percentage of all reports. Foreign collectors targeted electronics in 7 percent of the incidents. However, electronics weighted threat score was 11 percent of the aggregate threat score.

Collectors targeting electronics more often applied MOs that posed a greater risk of actual transfer of technology or information. Foreign collectors used AAT in 57 percent of the incidents targeting electronics. AAT had the highest weighted threat score of any MO. This contributed to electronics, just one of 29 IBTL categories, being a targeted technology in 41 percent of the incidents rated as Critical.

Collectors using AAT or SNA posed a greater threat to U.S. technologies than those using the most common MO, academic solicitation. Both AAT and SNA's weighted threat score exceeded their percentage of incidents, while academic solicitation's threat score was significantly less than the percentage of incidents using this MO.

Academic solicitation is the most common MO; it largely involves individuals outside of the United States submitting applications to universities and research labs, or academic papers to subject matter experts. Rarely does academic solicitation involve an individual having direct access to information or technology in cleared industry. In FY14, DSS analysts rated no incidents involving academic solicitation as Critical, and academic solicitation was the MO in less than 2 percent of the incidents rated as High.

After DSS has several years of applying this new methodology it will be possible to assess the trends of targeting U.S. technologies based on the estimated risk posed to the technology. The application of weighted ranking should provide greater insight to the actual risk foreign collectors pose to specific technologies resident in cleared industry. It will likely improve threat awareness and place greater scrutiny on entities using the higher risk MOs.

TABLE 2: THREAT SCORE WEIGHTING

THREAT SCORE	CRITICAL	HIGH	MEDIUM	LOW
Weight	10	5	3	1

TABLE 3: THREAT SCORE TOP TARGETED TECHNOLOGY

	PERCENTAGE OF REPORTS	THREAT SCORE
Electronics	7%	11%
Command, Control, Communication, & Computers	6%	7%
Aeronautic Systems	6%	7%
Software	4%	4%
Marine Systems	3%	4%

TABLE 4: THREAT SCORE TOP METHOD OF OPERATION

	PERCENTAGE OF REPORTS	THREAT SCORE
Academic Solicitation	23%	18%
Attempted Acquisition of Technology	16%	22%
Suspicious Network Activity	14%	18%
Solicitation or Marketing Services	14%	10%
Request for Information	13%	14%

DSS CATEGORIZATION DESCRIPTIONS

To organize its analysis, DSS applies a system of categories and subcategories that identify, define, and organize collection attempts. DSS categorizes foreign interest in U.S. technology in terms of 29 technology categories, 11 methods of operation, and 5 collector affiliations.

INDUSTRIAL BASE TECHNOLOGY LIST

AERONAUTIC SYSTEMS
Aeronautic systems include combat and non-combat air vehicle designs and capabilities.

AGRICULTURAL
Technology primarily used in the operation of an agricultural area or farm.

ARMAMENT & SURVIVABILITY
Armaments are conventional munitions technologies designed to increase the lethality of ground, aeronautic, marine, and space systems. Conversely, survivability technologies provide various level of protection for ground, aeronautic, marine, and space systems from armaments.

BIOLOGICAL
Information or technology related to the use of biological (organic) agents for research and engineering – minus synthetic biology. Also included in this category are biological storage, biological agent detection, and biological agent protection technologies.

CHEMICAL
Information or technology related to chemical research and engineering (chemistry). Also included in this category are chemical storage, chemical agent detection, and chemical agent protection technologies.

COGNITIVE NEUROSCIENCE
Cognitive neuroscience is an academic field of research merging psychology and neuroscience. The goal of this research is to understand the fundamental aspects of human behavior and thought by investigating the psychological, computational, and nueroscientific bases of cognition.

COMMAND, CONTROL, COMMUNICATION, & COMPUTERS
The hardware that comprises command, control, communication, & computers is the backbone of almost all government functions from battlefield commanders to interagency communications. Monitors, computers, printers, phones, radios, and data links are all necessary in this network centric environment.

COMPUTATIONAL MODELING OF HUMAN BEHAVIOR
Computational modeling of human behavior is the research and study of individual decision making. In theory, known experience, social networks, genetics, and environmental stimuli can be modeled to predict individual's or groups' behavior.

DIRECTED ENERGY
Directed energy is the use of various forms of energy transferred from a system or weapon to a target to produce a lethal or non-lethal effect. Although a laser is considered directed energy, laser information and technology falls in a separate laser category.

ELECTRONICS
Electronics is the study and engineering of electrical circuits and components. Electronics are the building blocks for almost all technologies, and each system may contain hundreds if not thousands of electronics performing a specific function to ensure the operation of a system.

ENERGETIC MATERIALS
Energetic materials are a group of materials that have a high amount of stored chemical energy. Research in this category focuses on metamaterials and plasmonics.

ENERGY SYSTEMS
Energy systems provide power to use or propel equipment. Simply put, energy system technologies are engines, generators, and batteries.

GROUND SYSTEMS
Ground systems include combat and non-combat vehicle designs and capabilities. This includes the engines and transmissions used to maneuver ground systems.

LASERS
A laser is a device that emits focused, amplified light due to the stimulated emission of photons. The term laser is an acronym originating from the phrase light amplification by stimulated emission of radiation. Two critical components to lasers – energy systems and optics – are organized in other categories.

MANUFACTURING EQUIPMENT & MANUFACTURING PROCESSES
Equipment that machines, cuts, folds, shapes, or prints elements and materials to a technology design or engineered specifications. In addition, different machines serving different purposes may be organized in a manner to add efficacy to a manufacturing process.

MARINE SYSTEMS
Marine systems include combat and non-combat marine vessel designs and capabilities.

MATERIALS: RAW & PROCESSED
Raw material is the basic material from which a product is manufactured or made. Raw materials that undergo an industrial processing procedure before delivery to a consumer or customer are considered processed materials.

MEDICAL
Technology used to research, diagnose, and treat disease, medical, and genetic conditions affecting humans.

NANOTECHNOLOGY
Nanotechnology is the study and science of manipulating matter at the atomic or slightly larger molecular level. Nanotechnology has future application in a broad list of professions and industries: medicine, biology, electronics (including semiconductor physics), energy, etc. Most applications in this area are emerging; however, any technology engineered to function at a molecular scale is considered nanotechnology. Functions can be as simple as giving electrons a defined, less resistant path to travel.

NUCLEAR
Information or technology related to using atomic nucleuses to produce energy or weapons. Also included in this category are nuclear storage, nuclear detection, and nuclear protection technologies – minus radiation-hardened electronics.

OPTICS
Optics is the study of the behavior of light and its interactions with matter and the development of equipment to detect light. Although other portions of the electromagnetic spectrum exhibit similar refractive, reflective, and defractive properties of light, the optics categories refers to the study and detection of light in the visible, ultraviolet, and infrared portions of the electromagnetic spectrum.

POSITIONING, NAVIGATION, & TIME
Positioning is the ability of a technology or person to accurately and precisely determine one's location and orientation two dimensionally (or three dimensionally when required) referenced to a standard geodetic system (such as World Geodetic System 1984). Navigation is the ability

to determine current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position anywhere around the world, from sub-surface to surface and from surface to space. Timing is the ability to acquire and maintain accurate and precise time from a standard (Coordinated Universal Time), anywhere in the world and within user-defined timeliness parameters. Timing includes time transfer.

RADARS
Radar is a term derived from the U.S. Navy phrase radio detection and ranging. Using radio waves and microwaves, radars can detect objects and determine range, altitude, direction, or speed. Technology in this category is specific to the transmission and reception of radio waves and microwaves. Other detection and ranging technology is not included in this category. Information related to signal processing capabilities is included in this section. However, information related to signal processing software is categorized in the software category.

QUANTUM SYSTEMS
Quantum systems are engineered to predict the quantum states of atomic and subatomic particles. Physicists and engineers use quantum mechanics to conduct research in areas of quantum cryptography, quantum computing, and quantum teleportation.

SENSORS (ACOUSTIC)
Acoustic sensors are instruments that study and detect mechanical waves in gases, liquids, and solids. This category focuses on sound navigation and ranging in the very low and extremely high acoustic frequencies.

SIGNATURE CONTROL
Signature control technologies reduce or eliminate visual, signal, and auditory signs of other technologies or systems. Stealth is the common term used to describe technology in this category.

SOFTWARE
Software is a set of instructions written by engineers that become programs and operating systems that run computers.

SPACE SYSTEMS
Space systems include combat and non-combat space-based platform designs and capabilities.

SYNTHETIC BIOLOGY
Synthetic biology merges life science (biology) and physical science (engineering) to design and construct new biological parts, devices, and systems and the redesign of existing, natural biological systems for useful purposes.

METHODS OF OPERATION

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

ATTEMPTED ACQUISITION OF TECHNOLOGY
Via agency of front companies or third countries or direct purchase of firms, 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

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

EXPLOITATION OF RELATIONSHIPS
Via established 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 to gain unauthorized access

FOREIGN VISIT
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

REQUEST FOR INFORMATION
Via phone, email, or webcard approaches, these are attempts to collect protected information under the guise of price quotes, marketing surveys, or other direct and indirect efforts

SEARCH/SEIZURE
Via physical searches of persons, environs, or property or otherwise tampering therewith, this involves temporarily taking from or permanently dispossessing someone of property or restricting his/her freedom of movement

SEEKING EMPLOYMENT
Via résumé submissions, applications, and references, these are attempts to introduce persons who, wittingly or unwittingly, would thereby gain access to protected information that could prove useful to agencies of a foreign government

SOLICITATION OR MARKETING SERVICES
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

SURVEILLANCE
Via visual, aural, electronic, photographic, or other means, this comprises systematic observation of equipment, facilities, sites, or personnel

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

COLLECTOR AFFILIATIONS

COMMERCIAL
Entities whose span of business includes the defense sector

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

GOVERNMENT AFFILIATED
Research institutes, laboratories, universities, or contractors funded by, representing, or otherwise operating in cooperation with a foreign government agency

INDIVIDUAL
Persons who target U.S. technology for financial gain or ostensibly for academic or research purposes

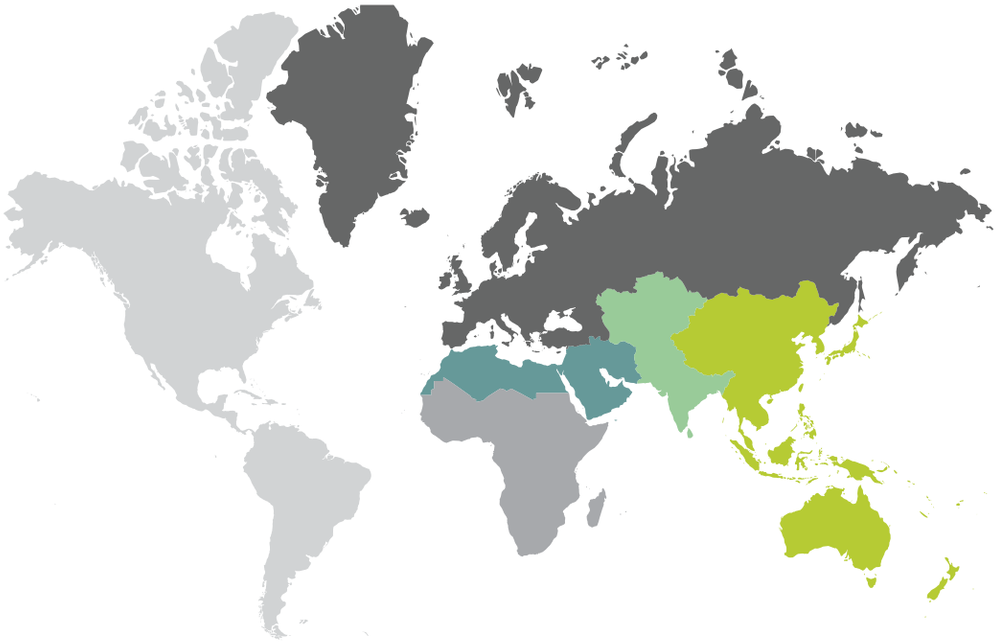
UNKNOWN
Instances in which no attribution of a contact to a specific end user could be directly made

ACRONYMS & ABBREVIATIONS

A2/AD	anti-access/area denial
ANV	assessed no value
AAT	attempted acquisition of technology
C4	command, control, communication, and computers
CI	counterintelligence
CNE	computer network exploitation
DoD	Department of Defense
DSS	Defense Security Service
ERC	End-User Review Committee
FIE	foreign intelligence entity
FY	fiscal year
IBTL	Industrial Base Technology List
IC	Intelligence Community
IO	intelligence officers
IPR	intellectual property rights
ITAR	International Traffic in Arms Regulation
MCTL	Militarily Critical Technologies List
MO	method of operation
NISPOM	National Industrial Security Program Operating Manual
R&D	research and development
RFI	request for information
RI	research institute
SCR	suspicious contact report
SNA	suspicious network activity
UAV	unmanned aerial vehicle
UCR	unsubstantiated contact report

PAGE INTENTIONALLY LEFT BLANK

REGIONAL BREAKDOWN



AFRICA

Angola
Benin
Botswana
Burkina Faso
Burundi
Cameroon
Cabo Verde
Central African Republic
Chad
Comoros
Congo, Democratic Republic of the
Congo, Republic of the
Cote d'Ivoire
Djibouti
Equatorial Guinea
Eritrea
Ethiopia
Gabon
Gambia, The
Ghana
Guinea
Guinea-Bissau
Kenya
Lesotho
Liberia
Madagascar
Malawi
Mali
Mauritania
Mauritius
Mozambique
Namibia
Niger
Nigeria
Rwanda
Sao Tome and Principe
Senegal
Seychelles
Sierra Leone
Somalia
South Africa
South Sudan
Sudan
Swaziland
Tanzania
Togo
Uganda
Zambia
Zimbabwe

EAST ASIA & THE PACIFIC

Australia
Brunei
Burma
Cambodia
China
Fiji
Indonesia
Japan
Kiribati
Korea, North
Korea, South
Laos
Malaysia
Marshall Islands
Micronesia, Federated States of
Mongolia
Nauru
New Zealand
Palau
Papua New Guinea
Philippines
Samoa
Singapore
Solomon Islands
Taiwan
Thailand
Timor-Leste
Tonga
Tuvalu
Vanuatu
Vietnam

EUROPE & EURASIA

Albania
Andorra
Armenia
Austria
Azerbaijan
Belarus
Belgium
Bosnia and Herzegovina
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Georgia
Germany
Greece
Holy See
Hungary
Iceland
Ireland
Italy
Kosovo
Latvia
Liechtenstein
Lithuania
Luxembourg
Macedonia
Malta
Moldova
Monaco
Montenegro
Netherlands
Norway
Poland
Portugal
Romania
Russia
San Marino
Serbia
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom

NEAR EAST

Algeria
Bahrain
Egypt
Iran
Iraq
Israel
Jordan
Kuwait
Lebanon
Libya
Morocco
Oman
Palestinian Territories
Qatar
Saudi Arabia
Syria
Tunisia
United Arab Emirates
Yemen

SOUTH & CENTRAL ASIA

Afghanistan
Bangladesh
Bhutan
India
Kazakhstan
Kyrgyzstan
Maldives
Nepal
Pakistan
Sri Lanka
Tajikistan
Turkmenistan
Uzbekistan

WESTERN HEMISPHERE

Antigua and Barbuda
Argentina
Aruba
Bahamas, The
Barbados
Belize
Bermuda
Bolivia
Brazil
Canada
Cayman Islands
Chile
Colombia
Costa Rica
Cuba
Curacao
Dominica
Dominican Republic
Ecuador
El Salvador
Grenada
Guatemala
Guyana
Haiti
Honduras
Jamaica
Mexico
Nicaragua
Panama
Paraguay
Peru
St. Kitts and Nevis
St. Lucia
St. Maarten
St. Vincent and the Grenadines
Suriname
Trinidad and Tobago
United States
Uruguay
Venezuela

PAGE INTENTIONALLY LEFT BLANK

DEFENSE SECURITY SERVICE