Defense Security Service

TARGETING U.S. TECHNOLOGIES

A Trend Analysis of Cleared Industry Reporting

2016

Date of Information: October 1, 2015

Product coordinated with: AFOSI, DTRA, and MCIA

TABLE OF CONTENTS

PAGE INTENTIONALLY LEFT BLANK

PREFACE

During fiscal year 2015, foreign collectors continued to work to erode U.S. economic and military advantages through the theft of cleared industry's investment in expensive research and development efforts. These collectors applied the complete spectrum of collection methods in order to identify and exploit vulnerabilities in cleared industry's security measures. During the year, they targeted a wide array of technologies resident in the cleared industrial base.

The Defense Security Service (DSS) is charged with overseeing the protection of U.S. and foreign classified technologies and information resident in the cleared industrial base under the authority of the National Industrial Security Program and its assigned counterintelligence mission. DSS uses its unique partnership with cleared industry to establish and improve best security practices, monitor security programs, and evaluate the evolving threat to information and technology. As cleared contractors identify and report potential collection attempts, DSS analyzes and identifies the foreign collectors who target U.S. cleared industry and works with other government agencies to disrupt the activities of our adversaries.

This annual publication, *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting*, reflects the compilation and analysis of the suspicious contact reports received from cleared industry during FY15. In FY15, DSS received over 39,000 reports from industry, a 15 percent increase from the prior fiscal year. Based on these reports, DSS, in coordination with other government agencies, identified 1,020 subjects of operations or investigations.

DSS has a responsibility to our industry partners to provide a clear picture of the threat posed by foreign collectors targeting cleared facilities and personnel. If foreign entities are able to penetrate our defenses, exploit classified information and technology, and target personnel, we lose our technological advantage and compromise our warfighters. It is our intention for this publication to provide an overview of the threat picture and identify the best areas for additional protection.

DSS supports cleared industry, government agencies, the Intelligence Community, and law enforcement community in establishing effective defensive networks to protect classified information and technology.

Daniel E. Payne
Director
Defense Security Service

BACKGROUND

THE ROLE OF THE DEFENSE SECURITY SERVICE

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 Counterintelligence (CI) Directorate identifies threats to U.S. technology and programs resident in cleared industry and seeks to stop foreign collection attempts to obtain unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. DSS CI 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 and report any suspicious contacts to DSS. The process that begins with initial reporting 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 suspicious contact reports from cleared contractors. DSS categorizes these reports as a suspicious contact report (SCR), unsubstantiated contact report (UCR), or assessed no value. For each reported collection attempt, DSS data aggregation and analytical 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. The analysis of this information 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 warranted, DSS refers cases of CI concern to its partners in the law enforcement and intelligence communities for potential exploitation or neutralization. DSS follows up with remedial actions for industry to 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 (CPI) Protection within the Department of Defense*, dated May 28, 2015, requires DSS to provide unclassified and classified all-source analyses, to include annual analyses of suspicious contacts and activities occurring within cleared industry that could adversely affect the protection of CPI. This report details the findings

of the annual analyses required by this DoD instruction, and focuses on efforts to compromise or exploit cleared personnel or to obtain unauthorized access to classified information or technologies resident in the U.S. cleared industrial base.

In this report, the 18th annual *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting* (or *Trends*), DSS provides a snapshot of its findings on foreign collection attempts. It provides a statistical and trend analysis that covers the most pervasive foreign collectors targeting the cleared contractor community during fiscal year 2015 (FY15), compares that information to the previous year's report, and places that comparison into a larger context.

DoD Instruction 5200.39 requires DSS to disseminate its reports to cleared industry and DoD component heads. This report constitutes part of DSS' ongoing effort to assist in better protecting the U.S. 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 and CI professionals in their efforts to detect, deter, mitigate, or neutralize the effects of foreign targeting. DSS previously released a classified version of the report.

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, DSS bases this publication on SCRs and select UCRs. The analyses also incorporate references to all-source reporting. The *Trends* is organized first by region, then by targeted technology, method of operation (MO), and collector affiliation. It incorporates statistical and trend analyses on each of these areas.

DSS analysts review SCRs and UCRs to determine if a report is of CI concern. They further determine the level of threat the incident posed to have actually compromised cleared industry personnel, or obtained actual access to technology or information resident in cleared industry. The analysts assess each incident based on the actor, action, and targeted

DSS REPORT TYPES

DSS assigns 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.

TABLE 1: FY15 REGIONAL ENHANCED THREAT DATA

Region	Percentage of Reports	Threat Score
East Asia & the Pacific	35%	40%
Near East	21%	22%
South & Central Asia	20%	16%
Europe & Eurasia	11%	9%
Western Hempisphere	6%	6%
Africa	1%	1%
Unknown	6%	6%

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.

For the second year, DSS 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. Prior to the 2015 *Trends* report, 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 FY15. For example, entities from the East Asia and the Pacific region accounted for 35 percent of all reports in FY15; however, the threat score for reports associated with this region represented 40 percent of the total weighted score. Only the top two collecting regions, East Asia and the Pacific and the Near East, had threat scores exceeding their percentage of raw reporting. This indicates that incidents related to entities from these regions posed a greater threat to obtaining access to information or technology or compromising a cleared employee.

The weighted ranking system did not cause a shift in the order of the regions as collectors. Instead, the threat scoring created a greater separation of the top two most prolific collector regions from the other four regions. The Near East was the second most common collector region identified in 21 percent of overall incidents, while entities from South and Central Asia accounted for 20 percent of the incidents. When comparing the threat score, the 1 percent difference in raw number of incidents increases to 6 percent, with Near East accounting for 22 percent of the overall aggregate threat score and South and Central Asia accounting for 16 percent.

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 annually examines and makes changes to the list, as required. The End User Review Committee includes representatives from the Departments of Commerce, Defense, Energy, State, and, when appropriate, Treasury.

ESTIMATIVE LANGUAGE AND ANALYTIC CONFIDENCE

DSS employs the Intelligence Community (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.

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

In FY15, DSS saw a marked increase in industry reporting of foreign collection attempts to obtain sensitive or classified information and technology resident in cleared industry. Reports from industry partners in FY15 showed a 15 percent increase from the previous year.

For the fourth year in a row, the top four collector regions remained the same. DSS saw the most reporting associated with collectors in the East Asia and the Pacific region, followed by the Near East, South and Central Asia, and Europe and Eurasia. The Western Hemisphere remained the fifth region in FY15, while Africa region collectors remain the sixth most prolific.

Electronics; command, control, communication, and computers (C4); and aeronautic systems remained the top three most often targeted technologies in FY15. Both the electronics and C4 sectors showed a slight increase from FY14. Reporting of energy systems increased by a third in FY15, moving this technology category up from tenth to fourth. Software remained one of the top five targeted technologies, although it dropped from fourth to fifth in FY15.

The use of academic solicitation as an MO remained the most reported for the third year in a row. However, the seeking employment MO showed a significant increase and moved up from the sixth most reported in FY14 to second in FY15. Together, academic solicitation and seeking employment accounted for more than 40 percent of all reports. Attempted acquisition of technology (AAT) remained in the top three, although it showed a slight decrease in FY15. Requests for information (RFI) and suspicious network activity both experienced a decrease in FY15, though they remain in the top five MOs.

Foreign collectors' steady use of academic solicitation to target sensitive or critical defense-related research at U.S. universities provides a low-risk, high-reward method for acquiring knowledge or technology. Collectors from East Asia and the Pacific, the Near East, and South and Central Asia use academic solicitation to target information and knowledge that can be applied to knowledge gaps within each region. The predominant use of academic solicitation to target cleared industry is addressed in the Special Focus Area.

Consistent with the past 6 years, commercial collectors remained the most often reported collector affiliation. The next four collector affiliation categories also retained their rankings with government-affiliated second, unknown in third, individual collectors fourth, and government collectors in fifth. The distribution of collector affiliations demonstrates the wide array of entities targeting cleared industry, as no affiliation accounted for over one-third of the incidents.

KEY POINTS

DSS based the key points on analysis of FY15 cleared industry reporting.

EAST ASIA AND THE PACIFIC

- Maintained its position as the most prolific collector region
- Electronics remained the most targeted technology
- Entities frequently attempted to leverage joint ventures with cleared contractors
- Commercial affiliates such as businesses or research institutes with ties to the military were among the top collectors
- Posed a CRITICAL threat to cleared industry using a variety of cyber and human-enabled tactics to acquire information and technology

NEAR EAST

- Collectors continued to seek a wide variety of military and dual-use technologies, such as energy systems
- Academic solicitation and seeking employment were the most common MOs
- At 43 percent, government-affiliated collectors were the most often reported
- Posed a HIGH threat to U.S. cleared industry owing to entities attempts to acquire sensitive technologies from U.S. cleared contractors

SOUTH AND CENTRAL ASIA

- Electronics continued to be the most targeted technology in FY15 with 15 percent of the total
- Résumé submissions to cleared industry continued to surge in FY15
- Reports of commercial and individual entities made up over half of reported incidents
- Posed a MEDIUM threat to cleared industry owing to the heavy reliance on seeking employment and academic solicitation MOs instead of more invasive approaches including attempted acquisition of technology to target critical technologies in cleared industry

EUROPE AND EURASIA

- Continued focus on modernization and technologies that can be used across numerous military platforms
- Request for information and attempted acquisition of technology accounted for 40 percent of all Europe and Eurasia reporting
- Commercial firms represented over two-and-a-half times the requests as the next most common collector affiliation
- Posed a HIGH threat to U.S. cleared industry due to continued targeting of electronics and C4 and apparent attempts to obfuscate end user and end-use information

FIGURE 1: FY15 REPORTING SUMMARY

Each region legend illustrates the threat score associated with that region, the threat level DSS attributed to the region, and the top technology, method of operation, and collector affiliation. 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 FY15 reporting.

TOP TARGETED TECHNOLOGIES

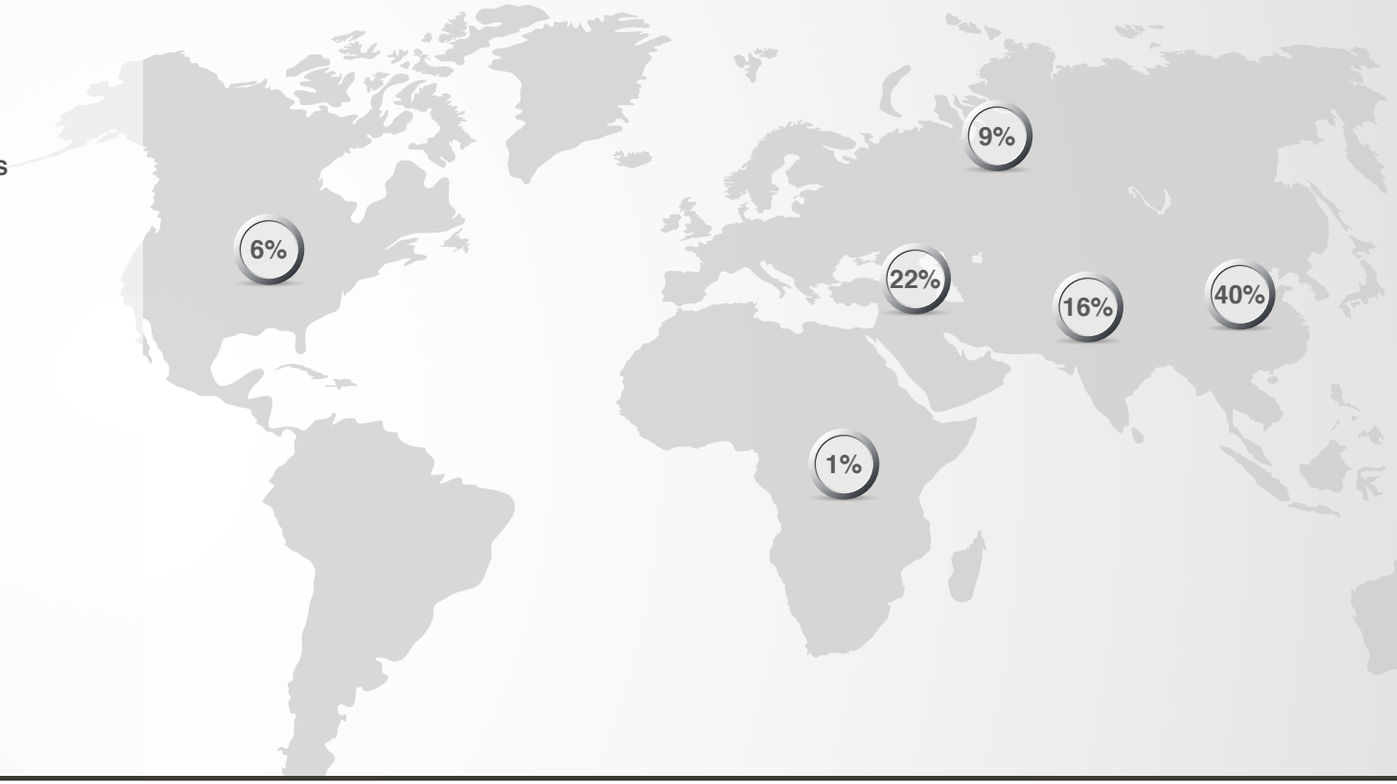
- Electronics
- Command, Control, Communication, & Computers
- Aeronautic Systems
- Energy Systems
- Software
- Radars
- Optics
- Armament & Survivability
- Marine Systems
- Materials: Raw & Processed

TOP METHODS OF OPERATION

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

TOP COLLECTOR AFFILIATIONS

- Commercial
- Government Affiliated
- Unknown
- Individual
- Government



EAST ASIA & THE PACIFIC

40%

THREAT LEVEL
Critical

TOP TARGETED TECHNOLOGY
Electronics

TOP METHOD OF OPERATION
Academic Solicitation

COLLECTOR AFFILIATION
Commercial

NEAR EAST

22%

THREAT LEVEL
High

TOP TARGETED TECHNOLOGY
Energy Systems

TOP METHOD OF OPERATION
Academic Solicitation

COLLECTOR AFFILIATION
Government Affiliated

SOUTH & CENTRAL ASIA

16%

THREAT LEVEL
Medium

TOP TARGETED TECHNOLOGY
Electronics

TOP METHOD OF OPERATION
Seeking Employment

COLLECTOR AFFILIATION
Commercial

EUROPE & EURASIA

9%

THREAT LEVEL
High

TOP TARGETED TECHNOLOGIES
Electronics & Command, Control, Communication, & Computers

TOP METHODS OF OPERATION
Request for Information & Attempted Acquisition of Technology

COLLECTOR AFFILIATION
Commercial

WESTERN HEMPSPHERE

6%

THREAT LEVEL
Low

TOP TARGETED TECHNOLOGIES
Command, Control, Communication, & Computers & Electronics

TOP METHOD OF OPERATION
Request for Information

COLLECTOR AFFILIATION
Commercial

AFRICA

1%

THREAT LEVEL
Low

TOP TARGETED TECHNOLOGY
Aeronautic Systems

TOP METHOD OF OPERATION
Seeking Employment

COLLECTOR AFFILIATION
Commercial

SPECIAL FOCUS AREA:

OVERVIEW

Foreign student academic requests represent an ongoing threat to cleared industry. Access to U.S. cleared academia involved in sensitive and critical defense-related research offers the opportunity for foreign entities to bridge gaps in technical knowledge. Although not every résumé submission is directed by a foreign government, each one is an opportunity to gain greater technological know-how and leverage students' access to proprietary or export-controlled information and technology to fill collection requirements. Academic solicitation presents a threat to technology resident in U.S. cleared industry and to the United States' technological edge.

Academic solicitation involves attempts by foreign students, professors, scientists, or researchers to obtain sensitive export-restricted basic and applied research or classified information. The requests include information on post-graduate degree programs, research internships, thesis assistance, and review of technical publications—all under the guise of legitimate research. Successful placement at a cleared contractor or exchange of information offers an opportunity to not only satisfy foreign technology collection requirements, but also create better educated scientists and researchers who can improve indigenous technology development.

FY15 saw another year of focused interest by foreign students on cleared contractors. The number of solicitations to cleared contractors with an academic nexus remained constant from the previous year. The Near East and East Asia and the Pacific continue to represent the majority of academic solicitation reporting, with 41 and 36 percent of the total in FY15, respectively, while South and Central Asia maintained its third place position with 18 percent of total cleared reporting.

Energy systems and nanotechnology were the most targeted technologies among foreign students in FY15, ranking first or second for each of the top academic solicitors. The increased emphasis on energy systems and nanotechnology among the top targeted technologies reflects the broader trend in research and development (R&D) priorities and collection requirements.

Since 1999, foreign students have overwhelmingly pursued advanced degrees in Science, Technology, Engineering, and Mathematics (STEM) fields. U.S. companies, including cleared contractors, feel the pressure to provide quality products and services, and U.S. companies may turn to U.S.-educated foreign nationals with STEM backgrounds to fill positions. As U.S. companies and cleared contractors fill important high-tech jobs with better trained and educated foreign substitutes, the foreign collection and transfer threat to the United States' most critical defense technologies increases.

THE NEAR EAST

Based on industry reporting to DSS, Near East entities were the most active in contacting cleared personnel at U.S. academic and research institutions. Over the last 5 years, the reported number of academic solicitations from the Near East

has continued to rise and in FY15 outnumbered reported academic solicitations from East Asia and the Pacific. The rise in industry reporting mirrors the increase of students from the Near East in the United States over the last 10 years. According to the Institute of International Education, there were over 103,000 students from the Near East in the United States during the 2014-15 academic year, an 11 percent increase over 2013-14. A majority of Near East students were enrolled in STEM programs, most often at the graduate level.

Seventy-three percent of academic solicitations from the Near East came from students attending or recently graduated from government-affiliated universities that conduct R&D on behalf of their respective militaries. Following solicitations from government-affiliated entities, individual affiliation was the next most represented in reporting. These individuals nearly always were Near East students in the United States or Canada who expressed interest in graduate programs at cleared contractor facilities after completing an undergraduate program. In FY15, students from the Near East primarily targeted cleared facilities focused on energy systems, nanotechnology, materials: raw and processed, and C4 R&D.

EAST ASIA AND THE PACIFIC

The number of academic solicitations from East Asia and the Pacific remained strong in FY15. Over the last 3 years East Asia and the Pacific's share of foreign-born students in the United States has grown dramatically, dovetailing with cleared industry's reporting of academic solicitation submissions for the region. The 2014-15 academic year witnessed a 6 percent increase in the number of students attending U.S. universities from East Asia and the Pacific, up from 446,904 the previous year. During the 2013-14 academic year, more than 886,000 foreign students were enrolled at U.S. universities, half of them originating from East Asia and the Pacific.

Government-affiliated entities conducted 79 percent of the academic solicitation originating in East Asia and the Pacific, with many of these entities having strong connections to government-sponsored and/or directed research programs intended to address critical technology requirements.

In addition to direct links to foreign government research institutions, a large number of East Asia and Pacific résumé submissions from FY15 were from students with ties to scholarship programs funded and directed by

TABLE 3: FY15 ACADEMIC SOLICITATIONS AT A GLANCE

Top Regions	Top Targeted IBTL Categories	Top Degree Programs	Top Collector Affiliation
41% Near East	14% Energy Systems	22% Mechanical Engineering	73% Government Affiliated
36% East Asia & the Pacific	7% Nanotechnology	12% Electrical Engineering	
18% South & Central Asia	7% Materials: Raw and Processed	9% Electronics	
	5% Command, Control, Communication, & Computers	7% Aerospace Engineering	
	5% Optics	6% Energy Systems Engineering	

foreign governments. Foreign governments use scholarship programs for a variety of reasons. The prospect of 100 percent funding coverage increases the likelihood U.S. universities will accept foreign scholarship-sponsored students at a time when universities are cost-conscious and looking to defray costs associated with graduate and PhD programs. While elite, top performing foreign students are highly attractive to U.S. academic institutions eager to gain a competitive edge in a research environment where funding is tied to results, the scholarship ties students to the foreign government, creating leverage and a sense of obligation to report research information.

In FY15, East Asia and the Pacific-originating individuals primarily targeted cleared facilities focused on energy systems, nanotechnology, and materials-related R&D.

SOUTH AND CENTRAL ASIA

The number of students attending U.S. universities from South and Central Asia rose 24.5 percent in the 2014-15 academic year, up from 127,301 the previous year. South and Central Asia students primarily focused on STEM graduate programs in the 2014-15 academic year, which was reflected in the academic backgrounds of students contacting cleared contractors in FY15. South and Central Asia students were overwhelmingly represented by mechanical, electronics, communication, electrical, or materials engineering degree holders

Students associated with government-affiliated South and Central Asia academic institutions remained very active in FY15, accounting for 61 percent of academic solicitations originating from the region. South and Central Asia mirrored the types of technology East Asia and the Pacific targeted in FY15, with energy systems-related R&D the leading targeted technology. Directed energy-related technology was third. A number of students from South and Central Asia hailed from university systems that have strong links to foreign government or government-affiliated institutions focused on filling R&D collection requirements.

CONCLUSION

As long as the United States remains a leader in R&D of advanced technologies, foreign collectors will very likely target U.S. technologies, in part, by encouraging their citizens to access U.S. educational opportunities. While it is not known to what extent foreign governments or foreign intelligence entities task specific students to gain placement at particular institutions, it is very likely these governments expect these students to gain knowledge related to restricted technology and return with improved skills in research and application of critical technologies. Because of the potential for long-term technological and perhaps intelligence gain, foreign entities will very likely continue to use academic solicitations to gain access to U.S. information and technology. (Confidence Level: High)

PAGE INTENTIONALLY LEFT BLANK

EAST ASIA & THE PACIFIC

Despite a slight decrease in FY15 reporting, East Asia and the Pacific remained a persistent threat as the most active collector region of sensitive or classified information and technology resident in the cleared industrial base. Regionally, East Asia and the Pacific continues to represent a growing economic force that is focused on military modernization, particularly defense technology. Tensions between countries in the East Asia and the Pacific region remained high in FY15 based in part by ongoing turmoil regarding territorial claims. As a result, East Asia and the Pacific countries continue to target technologies that benefit regional military superiority.

In FY15, countries in the East Asia and the Pacific region pursued further research, development, and fielding of indigenous systems, while also targeting technology and information related to similar Western systems. Governments in this region view modern U.S. military technologies as a useful source of information.

For the fourth consecutive year, East Asia and the Pacific collectors targeted electronics most often. There was a significant difference between the number of reports related to electronics and C4, the second most targeted technology. The disparity between the first and second targeted technologies was also evident in FY14; data from FY14 revealed the same pattern of electronics being targeted 50 percent more often than the second most targeted technology.

FY15 reporting revealed a continued trend of East Asia and the Pacific entities using the academic solicitation and solicitation or marketing services MOs to attempt to obtain component systems and enabling technologies.

Commercial collectors remained the most prolific collector affiliation with 34 percent of all reports. Similar to FY14, government-affiliated was the second most reported collector affiliation. Together, the top two collector affiliations accounted for more than two-thirds of all reported collectors in FY15.

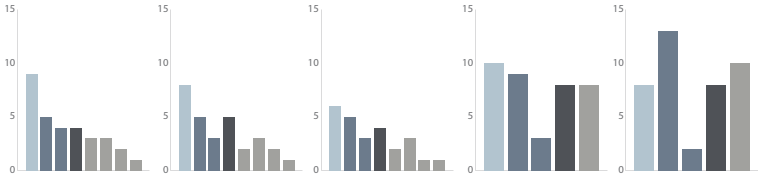
TARGETED TECHNOLOGIES

East Asia and the Pacific entities targeted all of the categories on the IBTL in FY15. The top four targeted technologies remained the same as FY14. Reports of electronics being targeted were the most prevalent, followed by C4, software, and aeronautic systems. These technologies all play a role in military modernization.

As space programs continue to be an area of focused modernization, reports often cited requests for components that contributed to bolstering indigenous efforts. Space-related technologies included gyroscopes, accelerometers, and electronic components including radiation-hardened integrated circuits, Gallium Nitride amplifiers, and monolithic microwave integrated circuits. Many of these components have applications in both military and commercial systems.

Analyst Comment: Electronics, particularly space-qualified, will likely continue to be a top collection priority for East Asia and Pacific entities in the near-term. This is the result of a continued inability to manufacture

FIGURE 2: EAST ASIA & THE PACIFIC TOP TARGETED TECHNOLOGIES

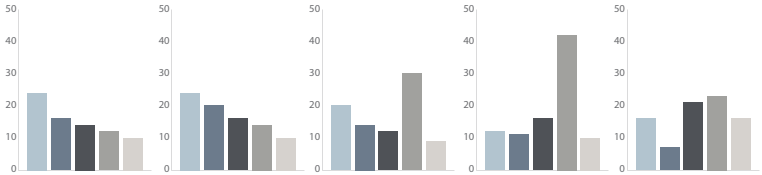


	FY15	FY14	FY13	FY12	FY11
	INDUSTRIAL BASE TECHNOLOGY LIST			MILITARILY CRITICAL TECHNOLOGIES LIST	
Electronics	9%	8%	6%	10%	8%
Command, Control, Communication, & Computers	5%	5%	5%	Information Systems 9%	13%
Software	4%	3%	3%	Information Security 3%	2%
Aeronautic Systems	4%	5%	4%	8%	8%
Optics	3%	2%	2%		
Radars	3%	3%	3%		
Sensors (Acoustic)	2%	2%	1%	Lasers, Optics, & Sensors 8%	10%
Lasers	1%	1%	1%		

radiation-hardened components suitable for space-based systems. (Confidence Level: High)

Just as in FY14, C4 remained the second most targeted technology sector. Many C4 technologies, such as satellite communications and software platforms, contribute to enhancing anti-access/area denial (A2/AD) capabilities. Modernizing A2/AD could allow East Asia and the Pacific countries to deter U.S. intervention or regional aggression in a possible conflict. In addition to A2/AD, East Asia and the Pacific entities also sought C4 components that would enhance battlefield communication.

FIGURE 3: EAST ASIA & THE PACIFIC MOST USED METHODS OF OPERATION



	FY15	FY14	FY13	FY12	FY11
Academic Solicitation	24%	24%	20%	12%	16%
Solicitation or Marketing Services	16%	20%	14%	11%	7%
Attempted Acquisition of Technology	14%	16%	12%	16%	21%
Suspicious Network Activity	12%	14%	30%	42%	23%
Request for Information	10%	10%	9%	10%	16%

East Asia and the Pacific entities continued to target aeronautic systems in FY15. Collectors often attempted to target information and technology on fighter aircraft and unmanned aerial vehicles (UAVs). East Asia and the Pacific countries sought information that could be reverse-engineered and used to modernize aviation industries. Additionally, East Asia and the Pacific entities continued to leverage commercial joint ventures with U.S. cleared industry to attempt to collect sensitive aerospace information and technology.

Software remained one of the top five targeted technologies for the third year in a row. In FY15, East Asia and the Pacific entities sought software technologies with dual uses that could be implemented on multiple platforms. For example, East Asia and the Pacific academics and individuals with ties to regional militaries conducted various aggressive collection efforts against U.S. modeling and simulation software.

It is worth noting that in FY15, 20 percent of all reported technologies targeted remained unknown. This category increased by 8 percent of reporting from FY14. East Asia and the Pacific collectors continued to use suspicious network activity (SNA) to collect large amounts of information from cleared industry. Due to the magnitude of the data exfiltrated, it is hard to ascribe specific technology categories to every piece of information East Asia and the Pacific collectors target through SNA.

METHODS OF OPERATION

FY15 reports concerning East Asia and the Pacific entities revealed a continued use of academic solicitation as the most common MO. Further, the top five MOs—academic solicitation, solicitation or marketing services, AAT, SNA, and RFI—remained the same as FY14. Together, these four MOs accounted for over 75 percent of all reports from East Asia and the Pacific entities in FY15.

The academic solicitation MO accounted for 24 percent of reports from East Asia and the Pacific. Collectors requested positions in universities or research programs with military applications and continued to leverage positions in fields associated with electronics, communications, aeronautics, and naval technology. Continued use of this MO falls in line with the strategic defense, military modernization, and self-sufficiency goals of East Asia and the Pacific countries.

East Asia and the Pacific collectors find academic solicitation rewarding because countries have a continuous need for R&D knowledge, and positions in academia provide access to critical and emerging technologies. There is even financial support and incentives from East Asia and the Pacific countries for students that study in the United States.

The use of the solicitation or marketing services MO revealed East Asia and the Pacific countries continue to exploit commercial opportunities. In FY15, collectors attempted to establish business relationships with cleared contractors by soliciting joint ventures or partnerships. An additional use of solicitation or marketing services to target cleared industry was evident at conferences in the East Asia and the Pacific region. It was not uncommon for members of cleared industry to be invited to all-expenses paid conferences as visitors or speakers. By attending technical conferences, members of cleared industry were at risk of further exploitation by East Asia and the Pacific entities.

Analyst Comment: East Asia and the Pacific companies frequently attempted to exploit joint ventures with cleared contractors by trying to gain access to information or technology outside the scope of the business agreement. In addition, these companies likely often attempt to obscure ties to their indigenous military programs and claim any information or technology gained through the joint venture would be used for civilian purposes. (Confidence Level: Moderate)

Attempted acquisition of technology remained the third most prevalent form of MO in FY15. Collectors continued to use direct requests to attempt to illicitly acquire technology and information from cleared contractors, particularly focusing on dual-use technology.

FY15 data reflected a continued use of SNA by East Asia and the Pacific collectors, with 12 percent of all reports attributed to this MO. This was the third consecutive year with a decline in reporting of SNA originating from this region. While East Asia and the Pacific entities improved their CNE tactics, techniques, and procedures, cleared contractors also became more aware of these activities.

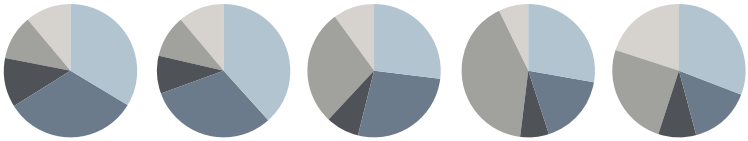
Analyst Comment: An enhanced security posture within cleared industry may account for less reporting, since security protocols block many attempts that would have been suspicious in previous years. (Confidence Level: Moderate)

East Asia and the Pacific collectors continued to use phishing/spear phishing emails to deliver malware and target cleared industry. Additional methods of SNA targeting included network and host vulnerability scanning. These tactics allow East Asia and the Pacific entities to collect intellectual property, proprietary information, business data, personally identifiable information, contract data, and anything else stored on corporate information systems and networks.

Request for information attempts included email and web-card requests for price quotes, export requirements, or product specifications. While the requester often obfuscated end user and end-use information, occasionally the submissions listed the end use as civilian or commercial.

East Asia and the Pacific collectors made use of the foreign visit MO in FY15. While foreign visits often began with legitimate purposes to discuss existing agreements or explore additional opportunities, East Asia and the Pacific entities sometimes attempted to exploit the visit by addressing subjects outside the bounds of the approved subject matter. In

FIGURE 4: EAST ASIA & THE PACIFIC COLLECTOR AFFILIATIONS



	FY15	FY14	FY13	FY12	FY11
Commercial	34%	>38%	27%	28%	31%
Government Affiliated	33%	>31%	27%	17%	15%
Unknown	<12%	9%	8%	7%	9%
Government	11%	>10%	28%	41%	25%
Individual	<11%	11%	10%	7%	20%

numerous reported cases in FY15, visiting delegations also included known or suspected intelligence officers.

COLLECTOR AFFILIATIONS

Though there was a slight decrease in the percentage of reports related to commercial collectors, from 38 to 34 percent, this collector affiliation remained the most prevalent in FY15. Commercial affiliates were often non-traditional collectors such as businesses or research institutes with ties to the military. FY15 reports also revealed numerous instances where East Asia and the Pacific commercial entities requested to purchase U.S. information and technology but did not provide end-use or end user data.

The second most prevalent collector affiliation, government-affiliated collectors, increased from 31 to 33 percent in FY15. Reports of government-affiliated collectors were often tied back to East Asia and the Pacific university researchers and students. Academics seeking internships or research positions targeted positions with ties to U.S. defense programs.

While reported cases attributed to unknown and government affiliations were the third and fourth most prevalent respectively. The number of individual collector affiliations decreased and contributed to this affiliation moving from third in FY14 to fifth in FY15.

Analyst Comment: The low number of reports attributed to individual collectors is likely due to DSS' ability to link individuals to a commercial company, government, or government-affiliated research institute. (Confidence Level: High)

PAGE INTENTIONALLY LEFT BLANK

NEAR EAST

Regionally, the Near East continued to experience a great deal of turmoil, which influenced the technology and information sought by Near East collectors. With little-to-no change in collection priorities, FY15 reporting revealed that Near East entities continued to seek a wide variety of military and dual-use technologies.

Industry and IC reporting reflected that Near East collectors actively attempted to obtain unauthorized access to sensitive or classified U.S. information and technology resident in the U.S. cleared industrial base. Near East entities targeted information and technology that would be useful in maintaining and developing military and defense programs. Regional collectors used procurement agents, front companies, foreign visits, and the direct pursuit or acquisition of technology and information.

The Near East region encompasses aspiring states, regional powers, and world players. Some of the most active collector countries have continuous conflict with other countries in the region. With this underlying tension, regional collectors target U.S. information and technology that will benefit each state's defense and military capabilities. While the individual states have different relationships with the United States, all seek to acquire an advantage from whatever access they can gain to U.S. sensitive or classified technology.

Despite a slight decrease in the number of reports attributed to Near East collectors, in FY15, entities from the Near East remained the second most active in attempts to obtain unauthorized access to U.S. information and technology. Near East collectors focused on targeting energy systems most frequently in FY15. Energy systems often have dual uses, making this category an attractive target for foreign collectors.

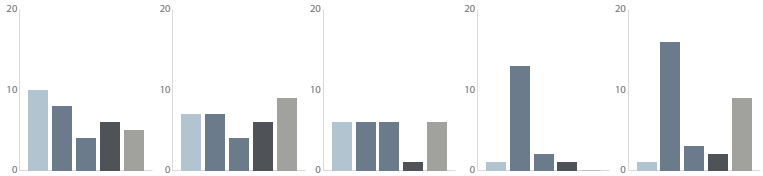
FY15 reporting revealed Near East entities continued use of academic solicitation as the most prevalent MO. Reports of academic solicitation were more than triple those of attempted acquisition of technology, the second most prevalent MO. The most significant change in MOs was related to seeking employment, which moved from seventh in FY14 to third in FY15.

For the fifth consecutive year, Near East collector affiliations remained in the same order, with government-affiliated collectors the most prevalent. Combined with the second most common collector affiliation, commercial entities, the top two affiliations accounted for more than two-thirds of reports with a Near East nexus.

TARGETED TECHNOLOGIES

Near East collectors most commonly targeted technology related to energy systems, C4, electronics, and aeronautic systems. Energy system programs have been one of the top five technologies targeted by Near East collectors for the past 3 years.

FIGURE 5: NEAR EAST TOP TARGETED TECHNOLOGIES



	FY15	FY14	FY13	FY12	FY11
	INDUSTRIAL BASE TECHNOLOGY LIST			MILITARILY CRITICAL TECHNOLOGIES LIST	
Energy Systems	10%	7%	6%	1%	1%
Command, Control, Communication, & Computers	8%	7%	6%	Information Systems 13%	16%
Software	4%	4%	6%	Information Security 2%	3%
Electronics	6%	6%	1%	1%	2%
Aeronautic Systems	5%	9%	8%	9%	9%

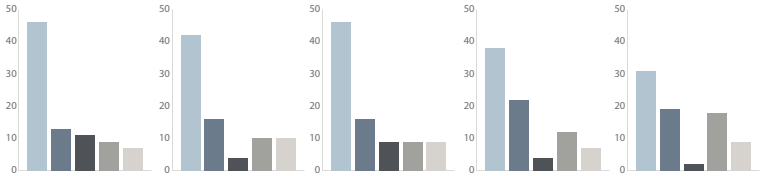
In FY15, the most reported technology sectors tended to be linked to student interest in gaining entry to specific U.S. research programs. Many of the energy system programs targeted by Near East collectors had dual uses that can be used in multiple military and defense platforms. As the United States remains a technological leader, sensitive and classified information regarding energy systems will be at risk from Near East collectors.

Consistent with previous years, Near East collectors continued to target C4 technologies, to include airborne and vehicle-borne platforms. These enabling technologies allow Near East states to enhance indigenous production capabilities and sustain a competitive edge with regard to military programs.

Near East collectors also focused on electronics, which showed a nominal increase in FY15. Many of the electronics technologies targeted have multiple uses. These components were the subject of collection efforts involving academia, front companies, third parties, and cyber operations.

Analyst Comment: DSS CI assesses Near East collectors will likely continue to focus on dual-use U.S. origin electronics due to the fact that many Near East countries lack the capability to produce electronics

FIGURE 6: NEAR EAST MOST USED METHODS OF OPERATION



	FY15	FY14	FY13	FY12	FY11
Academic Solicitation	46%	42%	46%	38%	31%
Attempted Acquisition of Technology	13%	16%	16%	22%	19%
Seeking Employment	11%	4%	9%	4%	2%
Request for Information	9%	10%	9%	12%	18%
Foreign Visit	7%	10%	9%	7%	9%

suitable for military applications that are on par with those of U.S. origin. (Confidence Level: Moderate)

METHODS OF OPERATION

While Near East entities continued to use a variety of MOs when targeting cleared contractors, academic solicitation has been the number one reported MO during the previous 4 years. The majority of academic solicitations to cleared industry involved Near East students seeking placement in research programs at U.S. universities involved in sensitive or classified research for the DoD. Near East regimes leverage placement in specific academic programs to facilitate collection or knowledge transfer efforts of critical technologies necessary to assist with internal knowledge gaps.

Just as in FY14, AAT remained the second most common MO. Near East entities attempted to acquire numerous export-controlled enabling technologies to bolster internal military and defense programs. Additional reporting indicates Near East procurement agents were often reluctant to provide end user or end-use information, obscuring the final recipient.

Reports of Near East entities seeking employment positions more than doubled in FY15. Near East collectors increasingly used indirect MOs such as seeking employment because it can bolster indigenous R&D.

Analyst Comment: The rise in individuals associated with Near East countries seeking employment is likely influenced by the growing number of foreign students from the region studying in the United States and subsequently seeking employment after graduation to remain in the United States. Seeking employment will likely remain one of the most commonly used MOs as Near East collectors seek to exploit non-traditional actors' potential

FIGURE 7: NEAR EAST COLLECTOR AFFILIATIONS

	FY15	FY14	FY13	FY12	FY11
Government Affiliated	43%	43%	44%	47%	35%
Commercial	<28%	26%	>22%	<28%	31%
Individual	12%	>13%	17%	11%	17%
Government	10%	>10%	11%	10%	11%
Unknown	<8%	>7%	>5%	<5%	6%

access to sensitive or classified information through employment at cleared contractors. (Confidence Level: Moderate)

While the number of reports of RFI and foreign visits decreased since FY14, these two MOs remained in the top five for FY15. Near East collectors often used foreign visits to aggressively probe for information not provided through official procurement programs or inserted intelligence officers into delegations at the last minute, affording them the opportunity to acquire classified information responsive to Near East collection requirements. In addition, Near East entities continued to solicit business partnerships with cleared contractors, presenting Near East companies an opportunity to exploit sensitive U.S. information and technology.

Analyst Comment: Near East entities will very likely continue to leverage foreign visits to solicit business partnerships with cleared contractors, presenting Near East entities an opportunity to exploit sensitive U.S. information and technology. (Confidence Level: Moderate)

Although reporting of SNA decreased in FY15, this MO remains useful for Near East entities. Near East entities continue to evolve their tactics, techniques, and procedures, which contributes to their increasingly sophisticated SNA attempts.

Analyst Comment: Due to past successes, Near East SNA actors are highly likely to continue to target cleared contractors in attempts to either compromise cleared employees' personal or work accounts or to acquire sensitive or critical technology and information. (Confidence Level: High)

COLLECTOR AFFILIATIONS

In FY15, DSS attributed 43 percent of reported collection activity to government-affiliated collectors, which was consistent with reporting from FY14. Government-affiliated collectors

remained the most active collectors for the last 5 years. These collectors continue to be associated with government-linked firms or public universities.

Analyst Comment: Some government-affiliated Near East actors likely target U.S. technology in an attempt to both fill government collection requirements and bolster profit margins. Near East governments likely indirectly leverage many of these actors to support military programs. (Confidence Level: Moderate)

Commercial collectors' share of reported incidents increased slightly in FY15. Similar to previous years, commercial collectors had ties to Near East procurement networks or front companies associated with defense industries. Industry reporting reflects that some of the commercial entities that target U.S. information and technology cooperate with national intelligence services.

Individual collectors accounted for 12 percent of the overall number of reports attributed to the Near East region. Individual collectors continued to account for academic solicitation and seeking employment MOs, focusing on U.S. academic programs or projects that had military applications.

It is worth noting that the unknown collector affiliation is largely attributed to Near East cyber activity and remained consistent with FY14's percentage. The use of SNA remains a key tactic for Near East collectors, but it often cannot be attributed to a specific type of collector.

PAGE INTENTIONALLY LEFT BLANK

SOUTH & CENTRAL ASIA

In FY15, South and Central Asia collectors continued to target a wide variety of sensitive or classified U.S. information and technology resident in the cleared industrial base. Reports with a South and Central Asia nexus increased by 22 percent in FY15, with this region remaining the third most attributed for the fourth year in a row.

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

While U.S. relations with South and Central Asia continued to improve in FY15, states in this region have been known to provide U.S. technology to third-party countries. These potential relationships with problematic third countries present a significant technology transfer risk to U.S. information and technology.

South and Central Asia remains a historically volatile region. States within this region are involved in long-standing inter- and intra-regional conflicts. South and Central Asia collectors may try to procure U.S. information and technology to offset technology acquisition by other countries within this region.

Electronics continued to be the most targeted technology in FY15 with 15 percent of the regional targeting. As South and Central Asia states focused on military modernization, electronics remained a prime target for collectors. Targeting of electronics can largely be attributed to academic solicitations to cleared research components of U.S. universities specializing in energy system-related programs.

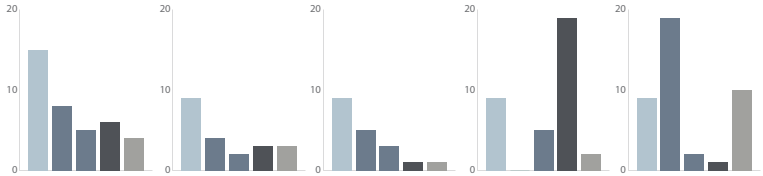
Seeking employment and academic solicitation remained the top two MOs for the third year in a row. South and Central Asia entities continued attempts to gain employment, internships, and research positions at cleared facilities or institutions associated with classified research. Although AAT experienced a slight decrease in the percentage of reporting from FY14, it remained the third-most prevalent MO.

While nearly all South and Central Asia contacts were attributed to individual or government-affiliated collectors, commercial remained the most prolific collector affiliation. Commercial collectors used the AAT and RFI MOs most frequently.

TARGETED TECHNOLOGIES

South and Central Asia states maintain a focus on military modernization and increasing indigenous production. These states seek to gain a military edge over rivals, boost their existing operational defenses, and bolster their defense industries. By targeting U.S. information and technology, regional collectors attempt to acquire technology that can fill near-term intelligence gaps. In addition, exploitation of these technologies through reverse engineering can enhance future R&D efforts with minimal investment.

FIGURE 8: SOUTH & CENTRAL ASIA TOP TARGETED TECHNOLOGIES



	FY15	FY14	FY13	FY12	FY11
	INDUSTRIAL BASE TECHNOLOGY LIST			MILITARILY CRITICAL TECHNOLOGIES LIST	
Electronics	15%	9%	9%	15%	9%
Command, Control, Communication, & Computers	8%	4%	5%	Information Systems 13%	19%
Software	5%	2%	3%	Information Security 8%	2%
Energy Systems	6%	3%	1%	1%	1%
Aeronautic Systems	4%	3%	3%	7%	10%

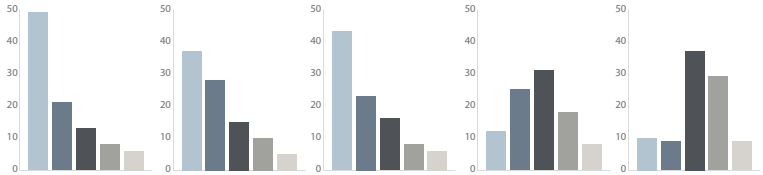
Electronics remained the top targeted technology sector for the fourth year in a row. South and Central Asia entities often showed an interest in acquiring enabling technologies within the electronic and C4 categories in an effort to upgrade aging military systems; C4 moved up from fourth most targeted to second. In FY15, reporting also revealed significant interest in technology that could support counterinsurgency operations.

It is noteworthy that energy systems made it into the top five targeted technologies in South and Central Asia for the first time since DSS began trend analysis of cleared industry reporting. This is largely attributed to academic solicitations to cleared research components of U.S. universities specializing in energy system-related programs. Conversely, reported incidents involving nanotechnology, experienced a considerable decrease in FY15, falling from 7 to 2 percent of total reporting.

METHODS OF OPERATION

Résumé and curriculum vitae submissions to cleared industry continued to surge in FY15 as seeking employment and academic solicitation MOs made up the majority of South and Central Asia reporting. Together these two MOs accounted for more than two-thirds of all reporting with a South and Central Asia nexus. Seeking employment and academic solicitation provides minimal risk opportunities for attempting to gain access to technology or information that is useful for military modernization.

FIGURE 9: SOUTH & CENTRAL ASIA MOST USED METHODS OF OPERATION



	FY15	FY14	FY13	FY12	FY11
Seeking Employment	49%	37%	43%	12%	10%
Academic Solicitation	21%	28%	23%	25%	9%
Attempted Acquisition of Technology	13%	15%	16%	31%	37%
Request for Information	8%	10%	8%	18%	29%
Solicitation or Marketing Services	6%	5%	6%	8%	9%

Reported incidents of seeking employment or academic solicitation primarily consisted of South and Central Asia entities applying to cleared contractors for positions requiring U.S. citizenship or a security clearance and requesting research positions or internships at cleared contractor components of academic institutions. Many of the prospective employees were information technology specialists; systems administrators; and mechanical, system, or electrical engineers.

The volume of South and Central Asia AAT and RFI reporting remained fairly consistent. Reported incidents in FY15 primarily consisted of South and Central Asia commercial or government-affiliated entities requesting information or attempting to acquire export-controlled technology on behalf of organizations on U.S. restricted end user lists.

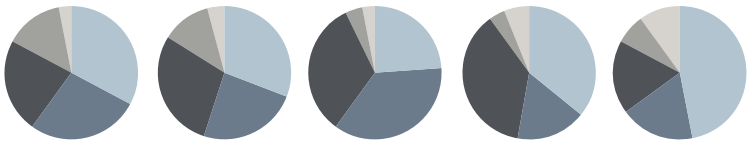
Solicitation or marketing services remained among the top five MOs used by South and Central Asia entities since FY11. These incidents primarily consist of solicitations via email to serve as representatives and market a cleared contractor's technology to regional customers. In some instances, these contacts expressed interest in collaborations and joint ventures with cleared industry.

Analyst Comment: Regional actors will likely continue to rely heavily on academic solicitations and seeking employment as an avenue of access to gain technological know-how for future indigenous production. However, it is likely that commercial entities will start to seek out partnerships and joint ventures with cleared industry to exploit access and relationships to assist in developing a more robust defense industry in the region. (Confidence Level: Moderate)

COLLECTOR AFFILIATIONS

Reports of commercial and individual entities made up more than half of reported incidents from South and Central Asia. Government-

FIGURE 10: SOUTH & CENTRAL ASIA COLLECTOR AFFILIATIONS



	FY15	FY14	FY13	FY12	FY11
Commercial	33%	31%	24%	36%	47%
Individual	27%	24%	36%	17%	18%
Government Affiliated	23%	29%	33%	37%	18%
Unknown	14%	12%	4%	4%	7%
Government	3%	4%	3%	6%	10%

affiliated entities, which were among the top two South and Central Asia collector affiliations since FY11, dropped to third in FY15 at 23 percent. The shift in the order of the top three collector affiliations is largely attributed to the rise in reported incidents of South and Central Asia entities seeking employment in cleared industry.

Analyst Comment: The majority of employment solicitations were likely legitimate attempts to gain employment in the United States. However, considering South and Central Asia regional objectives to modernize military forces, DSS cannot rule out that South and Central Asia entities have attempted to gain employment within cleared industry to obtain sensitive or proprietary information and technology to bolster indigenous production. (Confidence Level: Moderate)

For the first time since FY12, commercial collectors accounted for more than a third of all reports from South and Central Asia. South and Central Asia government and military organizations frequently use commercial companies to procure military technologies. A number of these commercial companies are typically legitimate businesses that also wittingly procure technology for South and Central Asia weapons developers or organizations on U.S. restricted end user lists.

As in previous fiscal years, reported incidents involving government-affiliated entities primarily consisted of students, researchers, and professors affiliated with public academic institutions. These entities frequently sought postdoctoral, research, and internship opportunities at cleared facilities, including university-affiliated research centers. Government-affiliated collectors also consisted of commercial companies attempting to fulfill tenders and procure technology on behalf of national military services or other governmental organizations.

EUROPE & EURASIA

Although industry reports of foreign collection attempts by Europe and Eurasia actors decreased slightly in FY15, multiple countries within the region continued to be active collectors. Europe and Eurasia remained the fourth most reported region, responsible for 11 percent of total reporting.

Many Europe and Eurasia states continue to focus on military modernization through upgrading and updating national defense equipment. Approaches to modernization vary within the region, but include substantial investments in indigenous military acquisition, R&D, acquisition via foreign purchase, or illicit acquisition of information or technology resident in the U.S. cleared industrial base. Regional and neighboring conflicts continued to be a motivation to develop or procure a range of top marine, aviation, space, and unmanned weapons systems.

The most commonly targeted technologies in FY15 were electronics and C4, each at 10 percent of all reporting. Aeronautic systems remained the third most common technology at 6 percent. Together, these three technologies made up more than a quarter of all reporting related to Europe and Eurasia.

Requests for information and AAT were the top MOs for FY15, each at 20 percent. Seeking employment showed the most growth, moving from eighth to third place in FY15. Solicitation or marketing services decreased by 38 percent and dropped this MO from second to fourth. SNA remained in fifth with 11 percent.

Europe and Eurasia entities continued to show an interest in cutting edge technologies and remain heavily dependent on their innovative commercial sectors. The commercial collector affiliation remained the top collector affiliation despite a 4 percent decrease in the percentage of reporting in FY15.

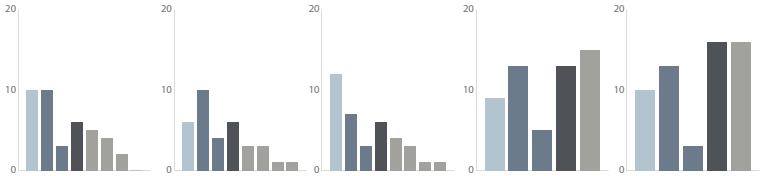
TARGETED TECHNOLOGIES

Europe and Eurasia states continued to focus on modernization and technologies they can use across numerous military platforms. For FY15, electronics, C4, and aeronautic systems made up the top three targeted technologies by Europe and Eurasia collectors. These three technologies were also the most commonly targeted in overall industry reporting.

Reports of Europe and Eurasia entities targeting electronics showed a marked rise in FY15, increasing from 6 to 10 percent of related reporting. Europe and Eurasia entities demonstrated a strong interest in sensitive or controlled U.S. microelectronics, since modern, highly capable microelectronics are integral to almost any state-of-the-art system.

Analyst Comment: It is very likely that Europe and Eurasia countries will continue to seek sensitive electronic components as they modernize their militaries. DSS assesses that many of these requests will come from legitimate actors, but DSS cannot rule out that some requests will ultimately be on behalf of nefarious end users. (Confidence Level: Moderate)

FIGURE 11: EUROPE & EURASIA TOP TARGETED TECHNOLOGIES



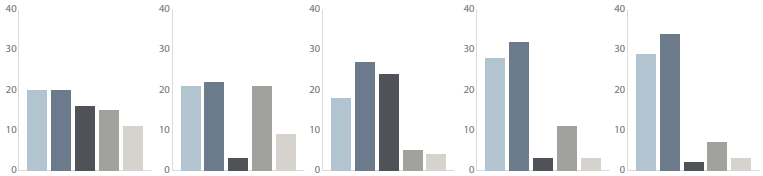
	FY15	FY14	FY13	FY12	FY11
	INDUSTRIAL BASE TECHNOLOGY LIST			MILITARILY CRITICAL TECHNOLOGIES LIST	
Electronics	10%	6%	12%	9%	10%
Command, Control, Communication, & Computers	10%	10%	7%	Information Systems 13%	13%
Software	3%	4%	3%	Information Security 5%	3%
Aeronautic Systems	6%	6%	6%	13%	16%
Radars	5%	3%	4%		
Optics	4%	3%	3%		
Lasers	2%	1%	1%	Lasers, Optics, & Sensors 15%	16%
Sensors (Acoustic)	0%	1%	1%		

Reports of Europe and Eurasia entities targeting C4 technologies remained at 10 percent in FY15. C4 technologies provide countries with platforms to modernize their militaries or improve a range of capabilities. Europe and Eurasia countries sought to speed up military decision cycles and improve communications security and situational awareness.

Aeronautic systems remained one of the top three targeted technologies in FY15. Europe and Eurasia countries continue to show an avid interest in UAV technology.

Analyst Comment: DSS assesses Europe and Eurasia will likely continue attempts to acquire sensitive U.S. UAV-

FIGURE 12: EUROPE & EURASIA MOST USED METHODS OF OPERATION



	FY15	FY14	FY13	FY12	FY11
Request for Information	20%	21%	18%	28%	29%
Attempted Acquisition of Technology	20%	22%	27%	32%	34%
Seeking Employment	16%	3%	24%	3%	2%
Solicitation or Marketing Services	15%	21%	5%	11%	7%
Suspicious Network Activity	11%	9%	4%	3%	3%

related technology and information to assist indigenous development efforts. (Confidence Level: Moderate)

METHODS OF OPERATION

RFI and AAT were the top two MOs used by Europe and Eurasia entities in FY15; together these MOs accounted for 40 percent of all reporting. RFIs and AATs consisted of commercial firms contacting cleared facilities via email and seeking to purchase or asking for information about specific systems. In some instances, the requesting entities provided limited-to-no end user or end-use information.

In FY15, there was a significant rise in reports of Europe and Eurasia collectors seeking employment positions requiring security clearances in cleared industry.

While solicitation or marketing services showed a drop compared to FY14 data, it was still one of the most prominent MOs reported in FY15. These requests generally concerned the business activities of the cleared contractor and a regional company, noting areas of overlap and often proposing a meeting for discussions, requesting collaboration, or asking to represent the U.S. firm in Europe and Eurasia.

Analyst Comment: Contacts between Europe and Eurasia entities and cleared contractors are concerning since closer ties likely could result in partnerships, supply chain operations, or joint ventures with countries of concern. It was of note that in some instances, the U.S. firm approached produced components in which the foreign country had shown interest. It is very possible that any such agreements would provide the foreign firms with opportunities to gain access to sensitive technology or information they would not otherwise have. (Confidence Level: Moderate)

FIGURE 13: EUROPE & EURASIA COLLECTOR AFFILIATIONS

	FY15	FY14	FY13	FY12	FY11
Commercial	43%	47%	38%	>43%	<45%
Government Affiliated	17%	14%	>15%	19%	19%
Individual	15%	14%	>31%	15%	<15%
Unknown	14%	11%	5%	>11%	10%
Government	11%	14%	10%	11%	<12%

Europe and Eurasia cyber activity increased 5 percent from FY14. In FY15, DSS received multiple reports from cleared industry involving spear phishing attempts by known regional state-sponsored cyber actors.

Analyst Comment: SNA is likely a serious threat to national security, despite the marginal increase in reporting. (Confidence Level: Moderate)

COLLECTOR AFFILIATIONS

FY15 data is consistent with previous years when it comes to the affiliation of Europe and Eurasia entities that approached cleared industry. By far the most common actors were commercial firms, representing over two-and-a-half times the requests as the next most common—government-affiliated collectors.

Government-affiliated collectors increased slightly, moving from third to second in FY15. These collectors consisted of research and educational institutions with government connections. Individual collectors also experienced a slight increase and moved from fourth to third. Many approaches from individuals entailed seeking employment with cleared contractors or submitting résumés to academic institutions.

The most significant change regarding collector affiliations involved government collectors. This affiliation decreased by 3 percent in the percentage of reports and moved from second in FY14 to fifth in FY15. Many of the countries from Europe and Eurasia are allies to the United States and are comparable in terms of economic development, industrial infrastructure, and innovative ability. Because of a close relationship with the United States, Europe and Eurasia entities willingly disclosed their affiliation with government organizations.

OTHER REGIONS

In FY15, entities from the Western Hemisphere and Africa regions collectively accounted for just 7 percent of overall reporting from cleared industry. While incidents attributed to entities from the Africa region increased, this was the first year since FY12 in which incidents attributed to entities from the Western Hemisphere decreased. The Africa region remained the least identified region in cleared industry reporting of suspicious incidents accounting for slightly more than 1 percent of all reporting.

WESTERN HEMISPHERE

Entities in the Western Hemisphere accounted for 6 percent of total cleared industry reporting in FY15; this accounted for nearly 15 percent fewer incidents. Collectors from the Western Hemisphere region have been consistent in their affiliation and the methods they employ to obtain information and technology from cleared industry since FY10. However, in FY15, these collectors had a noticeable shift in targeted technologies, as the incidents of targeting of electronics decreased by 40 percent from FY14.

Based on industry reporting in FY15, Western Hemisphere collectors most frequently targeted C4, electronics, aeronautic systems, armament and survivability, and optics technology sectors. For the previous 3 years, Western Hemisphere collectors most frequently targeted electronics; however, in FY15 there was a 40 percent decrease in related incidents. Although C4 became the most targeted technology in FY15, it also experienced over an 8 percent reduction in the number of incidents reported by industry. All three of the other top five technologies experienced similar decreases in reported targeting.

FY15 was the first year since FY11 that C4—then grouped with software in the information systems technology sector of the Militarily Critical Technologies List—was the most targeted technology. Collectors from this region targeted tracking and data link antennas associated with UAVs, Joint Tactical Radio System technology, satellite communications products, and satellite control computer equipment. Commercial entities accounted for over 60 percent of the targeting of C4 originating from this region, and most commonly used RFIs as their MO.

Although the second most frequently targeted technology, incidents targeting electronics tended to pose a greater risk of the collector gaining access to the technology than the incidents targeting C4. DSS analysts assessed 59 percent of these incidents as a moderate threat, which is considerably higher than the 37 percent of all reporting rated as moderate in FY15. Again, commercial entities were the most common collector affiliation from this region targeting electronics. RFI and AAT accounted for 90 percent of the incidents targeting electronics attributed to commercial entities from this region. Collector's targeting of electronics mirrored the collection from other regions including targeting of radiation-hardened integrated circuits.

FIGURE 14: WESTERN HEMISPHERE REPORTING OVERVIEW

Top Targeted IBTL Categories	Most Used Methods of Operation	Collector Affiliations
10% Command, Control, Communication, & Computers	33% Request for Information	49% Commercial
10% Electronics	16% Seeking Employment	21% Individual
8% Aeronautic Systems	14% Attempted Acquisition of Technology	19% Unknown
7% Armament & Survivability	12% Solicitation or Marketing Services	7% Government Affiliated
4% Optics	5% Suspicious Network Activity	3% Government

For the sixth consecutive year, RFI was the most frequent MO applied by collectors from the Western Hemisphere. Collectors from this region applied this approach in one-third of their attempts to collect information and technology from cleared industry. Along with RFI, seeking employment, attempted acquisition of technology, and solicitation or marketing services accounted for 75 percent of the incidents attributed to collectors from this region in FY15.

Similarly, the top three collector affiliations remained unchanged for the sixth consecutive year. In FY15, commercial remained the most common collector, accounting for 49 percent of the incidents, followed by individual and unknown, collectively accounting for 40 percent of the incidents. Commercial entities accounted for two-thirds of this region's targeting of aeronautic systems, commonly targeting quadrotor UAV technology. Government entities continued to account for the fewest incidents identified in just 3 percent of collection attempts in FY15.

Analyst Comment: The low frequency of government entities from this region targeting U.S. technologies is likely due in part to some nations in this region avoiding direct involvement in collection of U.S. technologies. In addition, the large volume of commercial and individual collectors very likely represent the front ends of illicit collection networks or commercial firms and independent brokers responding to tenders from other region's governments. Foreign entities may believe requests from private sector firms from this region will receive less scrutiny when requesting information or actual acquisition of restricted technology. (Confidence level: Moderate)

AFRICA

Collectors from the Africa region remained the least active with just over 1 percent of all suspicious incidents reported by cleared industry attributed to this region. In each of the past 6 years, DSS attributed approximately 1 percent of the suspicious incidents reported by cleared industry to collectors from the Africa region. FY15 was the fifth consecutive year that the number of reported incidents attributed to entities from Africa increased.

In half of the reported incidents in FY15, DSS could not identify the targeted technology or assessed the targeted technology was not included in the IBTL. The most commonly targeted technologies were aeronautic systems, C4, and ground systems. These three technologies combined for 25 percent of overall reporting. Collectors targeted aeronautic systems technology in 11 percent of the incidents originating from this region. In 78 percent of the incidents targeting aeronautic systems technology, commercial collectors from this region targeted UAV technologies, most commonly hybrid quadrotor UAV technology. These UAVs feature conventional flight mode with a vertical takeoff and landing capability for operation in restrictive terrain.

Although targeted in fewer incidents than aeronautic systems, collectors from this region posed a greater threat to C4 technologies. In 71 percent of the incidents targeting C4, DSS analysts assessed the incident posed a moderate or high threat to actual transfer of technology or information. Collectors from this region sought an array of C4-related technology including information systems and electronic warfare technologies.

Ground systems technology was the third most targeted by collectors from this region. In 60 percent of these incidents, collectors targeted sophisticated scanning systems commonly used for scanning of cargo and vehicles at ports and check points during counter smuggling and counterterrorism operations.

For the Africa region, seeking employment and AAT were the most common MOs in FY15. DSS identified the seeking employment MO in 40 percent of the incidents in FY15, a considerable increase from just 3 percent of incidents in FY14. This MO was also the most common in FY13 when collectors from this region used it in 51 percent of incidents. Collectors used attempted AAT in 22 percent of incidents in FY15. This was the third consecutive year that AAT was the second most common MO.

Analyst Comment: The large portion of incidents using seeking employment to target industry likely accounts for the high percentage of incidents where DSS could not identify the targeted technology or assessed the targeted technology was not included in the IBTL. In FY13 and FY15, seeking employment was the most common MO, and in both years DSS could not identify the specific targeted technology in half of the incidents originating from this region. Seeking employment often involved individuals sending résumés to cleared facilities with multiple defense technologies, or to corporate human capital management sites without identifying an interest in a specific position or program. (Confidence level: Moderate)

FIGURE 15: AFRICA REPORTING OVERVIEW

Top Targeted IBTL Categories	Most Used Methods of Operation	Collector Affiliations
11% Aeronautic Systems	40% Seeking Employment	42% Commercial
8% Command, Control, Communication, & Computers	22% Attempted Acquisition of Technology	31% Individual
6% Ground Systems	14% Request for Information	12% Unknown
5% Energy Systems	14% Academic Solicitation	10% Government Affiliated
4% Electronics	4% Suspicious Network Activity	5% Government

For 5 of the last 6 years, cleared industry reporting identified commercial entities as the most common collector in the Africa region. In FY15, DSS attributed 42 percent of the suspicious incidents in this region to commercial entities. This is consistent with commercial collectors accounting for no less than 36 percent each year since FY10. These commercial entities most commonly sought aeronautic systems, specifically UAVs and UAV components and equipment.

Analyst Comment: Entities from these two regions will very likely 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. Collectors from these regions will likely continue to most aggressively target C4, aeronautic systems, and electronics technologies. Commercial entities will very likely remain the most common collector affiliation. (Confidence level: High)

OUTLOOK

In FY15, cleared industry reported targeting of sensitive or classified information and technology from all regions of the world. The United States is an R&D leader of new technology in defense sectors and beyond. This diverse technological leadership makes U.S. cleared industry a prime target for foreign entities. Strategic and economic competitors target cleared industry in order to reduce time and expense in their indigenous production of cutting-edge technology. This pervasive threat against cleared contractors shows no sign of abating.

Spanning more than 10 years of industry reporting, entities from East Asia and the Pacific, Near East, South and Central Asia, and Europe and Eurasia have continued to be the top collectors. Actors from these regions will almost certainly continue using a variety of MOs in their attempts to acquire U.S. technology. Additionally, foreign entities' collection efforts will almost certainly continue to target sensitive or classified technologies encompassing the entire spectrum of the IBTL. (Confidence Level: High)

Aggressive military modernization programs across the top collectors will very likely continue to drive the targeting of technology in cleared industry. Electronics and C4 technologies will likely remain some of the most desired technology targets in cleared industry. Electronics and C4 technologies will continue to be vital to foreign entities because they are used in a variety of advanced systems, including missiles, satellites, radar, radios, and electronic warfare applications. Many of the technologies targeted have dual-uses and can have a variety of commercial and military applications, thereby commercial and government entities alike find them beneficial. (Confidence Level: Moderate)

With the application of the IBTL, DSS specifically identified the emerging technologies of nanotechnology, computation modeling of human behavior, synthetic biology, signature control, cognitive neuroscience, and quantum systems. Nanotechnology will continue to be the most sought after, accounting for more reporting than the other emerging technologies combined. Collectors will likely focus on processes for developing and applying nanotechnologies, vice seeking to obtain actual materials. Specifically, foreign entities will target processes for developing microstructures, including amorphous materials and nanocrystalline structures. With the foreign collection focus on processes, academic solicitation will likely remain the most prominent collection method. (Confidence Level: Moderate)

East Asia and the Pacific will almost certainly continue to be the most prolific collector of cleared industry information and technology targeting a variety of technologies consistent with priorities to increase anti-access/area denial capabilities. East Asia and the Pacific SNA targeting cleared industry will also almost certainly continue for the foreseeable future using a variety of methods, including phishing/spear phishing to illicitly acquire intellectual property, proprietary information, and personally identifiable information. (Confidence Level: High)

Academic solicitation and seeking employment are likely to remain pervasive MOs used by foreign entities. Academic solicitation was one of the top five MOs for entities from East Asia and the Pacific, Near East, South and Central Asia, and Europe and Eurasia. While these requests for positions are mostly legitimate, they still provide an opportunity to gain access to sensitive information. As long as the United States maintains a technological advantage over its adversaries, these regions will very likely attempt to close knowledge gaps, in part, by encouraging their citizens to access U.S. educational opportunities in fields that correspond to indigenous technology requirements. (Confidence Level: High)

The trend of decreased SNA reporting continued in FY15 for the third year. However, entities attempting to gain access to cleared contractor networks for access to sensitive U.S. technologies will almost certainly remain a significant threat. DSS attributes a decrease in reporting of successful SNA to cleared industry improving its ability to detect and defeat CNE, assisted by support and information from the government and private firms. Despite these defensive efforts, cyber actors from East Asia and the Pacific and the Near East will almost certainly continue to conduct spear phishing and network attacks against cleared industry targets, as well as continue adjusting existing tactics, techniques, and procedures and developing new ones. Cleared contractors must remain vigilant protecting their networks and educating their employees about this threat. (Confidence Level: Moderate)

Entities with close relationships to the United States and cleared industry will likely continue to exploit those relationships to collect sensitive or classified information and technology resident in cleared industry. Additionally, commercial entities will likely continue using solicitation or marketing services as a way to begin a business relationship with cleared contactors, which opens a potential avenue to access sensitive information, technology, and manufacturing processes. (Confidence Level: High)

Foreign collectors will continue targeting cleared employees to exploit the knowledge of cleared industry and academia and gain access to U.S. information and technology. Unfortunately, once this happens the information is lost forever to our adversaries and will likely result in a diminished advantage for the U.S. warfighter and economy as a whole. Securing U.S. cutting-edge technology remains the key to maintaining a military and economic advantage. Foreign entities will likely modify their methods of targeting, and over time the specific technologies targeted may change, but the persistence and aggressiveness of those entities will almost certainly remain consistent. (Confidence Level: High)

CATEGORY DEFINITIONS

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.

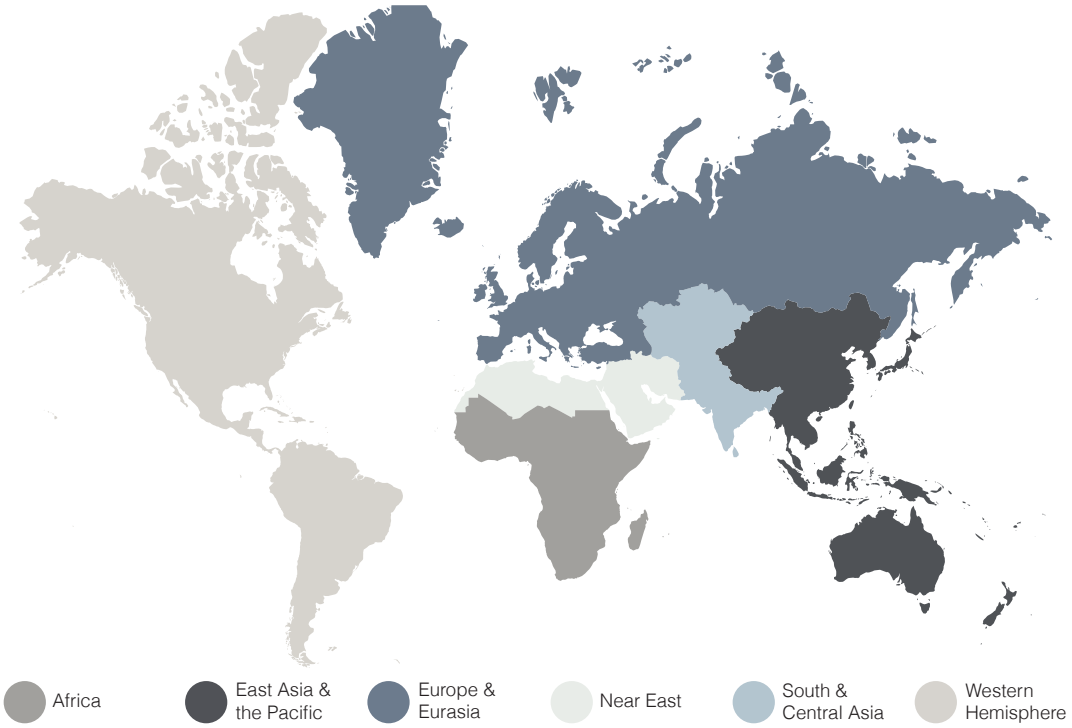
GOVERNMENT AFFILIATED
Research institutes, laboratories, universities, or contractors funded by, representing, or otherwise operating in cooperation with a foreign government agency.

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.

PAGE INTENTIONALLY LEFT BLANK

REGION BREAKDOWN



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

ACRONYMS & ABBREVIATIONS

anti-access/area denial	A2/AD
attempted acquisition of technology	AAT
assessed no value	ANV
command, control, communication, and computers	C4
counterintelligence	CI
Critical Program Information	CPI
Department of Defense	DoD
Defense Security Service	DSS
fiscal year	FY
Industrial Base Technology List	IBTL
Intelligence Community	IC
method of operation	MO
National Industrial Security Program Operating Manual	NISPOM
research and development	R&D
request for information	RFI
suspicious contact report	SCR
suspicious network activity	SNA
science, technology, engineering, and mathematics	STEM
unmanned aerial vehicle	UAV
unsubstantiated contact report	UCR