

# TARGETING U.S. TECHNOLOGIES

2017



**A Trend Analysis  
of Cleared  
Industry Reporting**

DEFENSE SECURITY SERVICE



Coordinated with: AFOSI, MCIA, and NCSC



# table of contents

<b>PREFACE</b>	<b>3</b>
<b>BACKGROUND</b>	<b>4</b>
<b>EXECUTIVE SUMMARY</b>	<b>8</b>
<b>SPECIAL FOCUS AREA</b>	<b>10</b>
<b>REGION ANALYSIS</b>	<b>14</b>
EAST ASIA AND THE PACIFIC . . . . .	14
NEAR EAST . . . . .	20
SOUTH AND CENTRAL ASIA . . . . .	24
EUROPE AND EURASIA . . . . .	28
OTHER REGIONS . . . . .	32
<b>OUTLOOK</b>	<b>36</b>
<b>ADMINISTRATIVE INFORMATION</b>	<b>38</b>
CATEGORY DESCRIPTIONS . . . . .	38
REGION BREAKDOWN . . . . .	42
ACRONYMS AND ABBREVIATIONS . . . . .	44

PAGE INTENTIONALLY LEFT BLANK

# PREFACE

The United States is facing the most challenging and significant foreign intelligence entity threat in its history. Adversaries use numerous methods to target technology and information critical to the United States' economic and military advantage. In fiscal year 2016, foreign collectors represented a persistent threat to the cleared industrial base, applying traditional and nontraditional tradecraft to target cleared industry.

Foreign investment in targeted industries to obtain manufacturing equipment, expertise, and intellectual property is just one example of nontraditional tradecraft. In particular, one foreign government funded the investment in or acquisition of companies involved in semiconductor production with the intent of establishing a self-sufficient semiconductor ecosystem and becoming the dominant or sole provider of select components, replacing the United States as the leader in the semiconductor industry.

In FY16, the Defense Security Service (DSS) received more than 46,000 reports from cleared contractors — an almost 18 percent increase from 2015. DSS uses these industry reports to develop analytical assessments to identify threats to U.S. information and technology. As cleared contractors identify and report potential collection attempts, DSS analyzes and identifies the foreign collectors who target U.S. cleared contractors 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 reports received in FY16. DSS provides this resource to improve cleared contractors' and U.S. Government agencies' awareness of who targets cleared industry, what they target, and how they attempt to gain access to sensitive information and technology.

DSS' application of the threat knowledge in the Trends publication and other DSS products is vital as we transition from a process focused on policy compliance to an intelligence-led, asset-focused, and threat-driven approach to protecting national security information and technology. DSS leverages its partnership with industry to provide a clear picture of the foreign adversary threat to cleared facilities and personnel. Through risk-based analysis and mitigation efforts, DSS supports cleared industry, the Intelligence Community, other Federal Government agencies, and the law enforcement community in establishing effective defensive networks to protect classified information and technology.



Daniel E. Payne  
Director  
Defense Security Service

# BACKGROUND

## THE CHARGE TO THE DEFENSE SECURITY SERVICE

The Defense Security Service (DSS) strengthens national security at home and abroad through our security oversight and education operations. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under the National Industrial Security Program. The DSS Counterintelligence (CI) Directorate identifies threats to U.S. technology and programs resident in cleared U.S. industry and seeks to deter, detect, and disrupt 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.

Through continual engagement across the NISP, cleared industry personnel work with DSS CI special agents (CISA) to identify foreign intelligence entities (FIE)-backed attempts to steal or compromise sensitive data, information and assets. In turn, our CISAs develop this information for appropriate referral to Intelligence Community (IC) and law enforcement agencies as well as for analysis,

production, and subsequent dissemination of products such as this report. Cleared industry's reports are an essential element in DSS CI's effort to identify the threat to cleared industry. DSS categorizes these reports as suspicious, unsubstantiated, or of no value.

## THE REPORT

Department of Defense (DoD) Instruction 5200.39, Critical Program Information (CPI) Protection within the Department of Defense, dated May 28, 2015, directs the Director of DSS to provide "unclassified and classified all-source analyses, to include, but not limited to, annual analyses of suspicious contacts and activities occurring within the defense contractor community that could adversely affect protection of CPI. Disseminates reports to the defense contractor community and DoD component heads." The focus of this report is to inform stakeholders 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.

Each year DSS publishes *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting*. In this report, the 19th annual Targeting U.S. Technologies (or *Trends*), DSS provides a snapshot of its findings on foreign collection attempts. It provides analysis that covers the most pervasive foreign collectors targeting the cleared contractor community during fiscal year 2016 (FY16) and places that comparison into a larger context. DSS intends the report to be a ready reference tool for security professionals in their efforts to detect, deter, mitigate, or neutralize the effects of foreign targeting.

## DSS REPORT TYPES

DSS assigns each report of suspicious contacts 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 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. DSS does not retain reporting assessed as ANV.

## SCOPE/METHODOLOGY

DSS considers all suspicious contact reports (SCRs) collected from the cleared contractor community. After sorting all reports into the three categories explained previously, DSS bases this publication on reports categorized as SCRs and on select UCRs. The analyses also incorporate reference to all-source IC reporting. We organize the Trends first by region, then by targeted technology, method of operation (MO), and collector affiliation. DSS analysts assessed the severity of each incident based on actor, action, and targeted technology to apply a threat rating of critical, high, medium, or low to each assessed report.<sup>i</sup>

For the third 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 FY16. For example, entities from the East Asia and the Pacific region accounted for 37 percent of all reports in FY16; however, the threat score for reports associated with this region represented 39 percent of the total weighted score. Only the East Asia and the Pacific and the Near East regions 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 active collector regions from the other four regions. The Near East was the second most common collector region identified in 22 percent of overall incidents, while entities from South and Central Asia accounted for 16 percent of the incidents. When comparing the threat score,

<sup>i</sup> DSS applies a four-tiered threat level system. A CRITICAL threat level indicates that DSS assesses an imminent risk of transfer of U.S. technology and information that could cause severe damage to national security. A HIGH threat level indicates that DSS assesses a likely risk of transfer of U.S. technology and information that could cause significant damage to national security. A MEDIUM threat level indicates that DSS assesses there is an even chance of transfer of U.S. technology and information that could cause limited to moderate damage to national security. A LOW threat level indicates that DSS assesses the risk of the transfer of U.S. technology and information is unlikely and that the damage to national security would be nominal.

the 6 percent difference in raw number of incidents increases to 10 percent, with Near East accounting for 23 percent of the overall aggregate threat score and South and Central Asia accounting for 13 percent.

This is the first year that DSS based the ranking within each section on the weighted threat score instead of solely based on the number of incidents. This is true for the overall assessed threat and within each of the region sections in this assessment. The most noticeable impact of ranking based on the assessed threat pertained to the MO in FY16. DSS analysts assessed attempted acquisition of technology (AAT) posed the greatest threat to actually have compromised information or technology in cleared industry; however, by volume of incidents, it was the fourth most common MO.

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 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, the assessments 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,

**TABLE 1: REGION RANKINGS**

	Top Collector Regions	FY16 Threat Score	FY16 Reports
	EAST ASIA & THE PACIFIC	39%	37%
	NEAR EAST	23%	22%
	SOUTH & CENTRAL ASIA	13%	16%
	EUROPE & EURASIA	11%	12%

the agency may not have evidence showing something to be a factor 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

This report reflects a continued rise in reported suspicious contact attempts to obtain sensitive or classified information and technology. Reports from cleared industry increased by almost 18 percent from FY15.

For the fifth year in a row, the top four collector regions remained the same. Collectors in the East Asia and the Pacific region, followed by the Near East, South and Central Asia, and Europe and Eurasia posed the most threat to information and technology resident in cleared industry. As in FY15, collectors from the Western Hemisphere and Africa posed the least threat in FY16, collectively accounting for just 7 percent of the overall threat.

For the fourth consecutive year, aeronautic systems; command, control, communication, and computers (C4); and electronics made up the top three targeted technologies. However, in FY16, aeronautic systems moved from third to first, while C4 remained second and electronics dropped to third. Radars and armament and survivability finished out the top five targeted technologies.

FY16 trends reflected a continuing threat to cleared contractors at conferences, conventions, and tradeshow (CC&Ts). CC&Ts provide an opportunity for foreign actors to use numerous illicit methods and employ constant aggressive targeting of cleared contractor personnel, information, and technology. The Special Focus Area provides more details on the threat to the cleared industrial base from foreign targeting at CC&Ts.

Based on the assessed threat, AAT was the top MO for FY16, at 20 percent. Although academic solicitation dropped from first to second, it still represented a significant threat to cleared industry.

Consistent with the previous 6 years, commercial continued to be the top collector affiliation. The distribution of the remaining collector affiliations remained similar to FY15, with government-affiliated second. However, individual moved to third and unknown dropped to fourth while government collectors remained fifth.

## KEY POINTS

DSS based key points on analysis of FY16 cleared industry reporting.

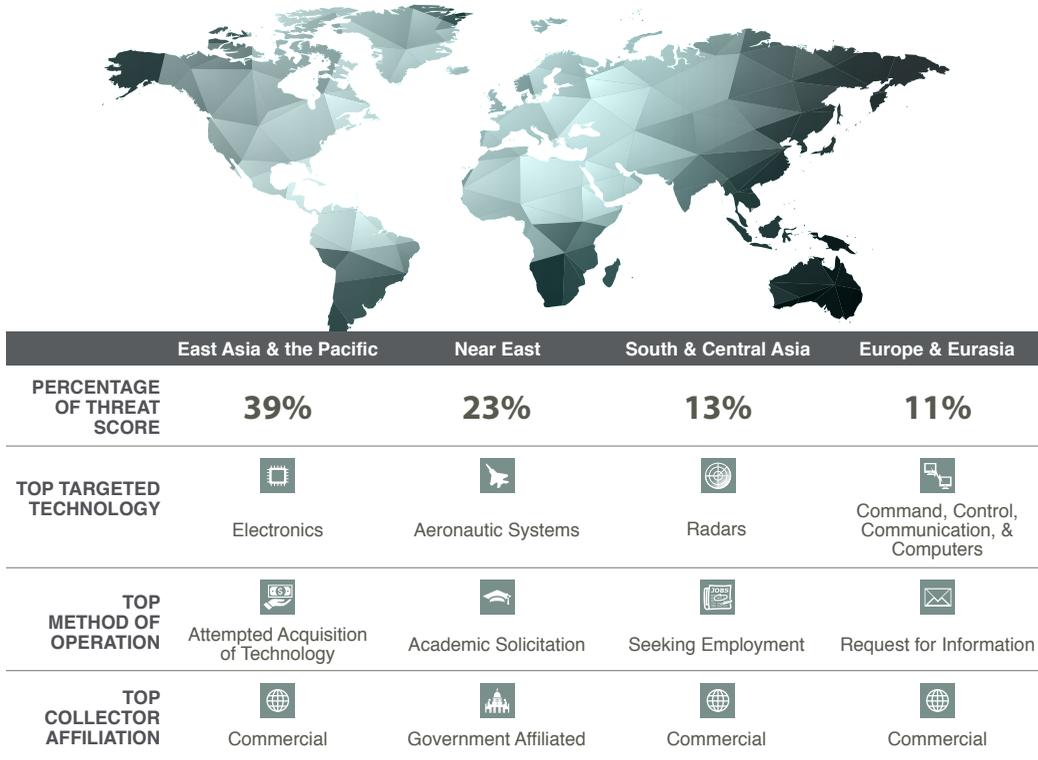
### EAST ASIA AND THE PACIFIC

- Maintained its position as the most active collector region
- Many of the technologies targeted supported established science and technology priorities
- Entities frequently attempted to leverage joint ventures (JVs) with cleared contractors
- Commercial and nontraditional government-affiliated entities were among the top collectors

### NEAR EAST

- Collectors continued to seek a wide variety of information and technology that would be useful in maintaining and developing military and defense programs
- Consistent with the previous 5 years, academic solicitation was the most common MO
- Government-affiliated collectors continued to be the most prevalent in FY16

**FIGURE 1: EXECUTIVE SUMMARY OF FY16 REPORTING**



**SOUTH AND CENTRAL ASIA**

- Entities targeted a wide variety of technologies, including enabling technologies that can be used in numerous platforms
- Continued to rely heavily on résumé submissions for seeking employment and academic solicitations
- South and Central Asia companies attempted to procure U.S. technologies for a variety of end users

**EUROPE AND EURASIA**

- Continued focus on modernization and technologies that can be used to bolster military programs
- Requests for information (RFIs) were the MO that posed the greatest threat to technology for the second consecutive year
- Commercial actors were the most prominent collectors in incidents associated to Europe and Eurasia

# SPECIAL FOCUS AREA: CONFERENCES, CONVENTIONS, AND TRADESHOWS

## EXPLOITING CONFERENCES, CONVENTIONS, & TRADESHOWS



Cleared contractors receive a number of email invitations to attend CC&Ts hosted around the world. While most of these invitations are nothing more than spam invites, some invitations are more targeted to a specific cleared contractor who is an expert on the topic of the event.

The solicitor who sent the email will often offer an all-expense paid trip to a given foreign country. Attending overseas CC&Ts provides additional opportunities for foreign actors to use other MOs, such as search/seizure, surveillance, exploitation of experts, and theft.

These methods are commonly employed while the cleared contractor employee is in transit, in residence at hotels, dining, or interacting with other conference attendees or host country nationals.

These engagements offer the opportunity to collect additional biographic information and entice attendees with alcohol, drugs, prostitutes, and cash inducements which could place the employee in a vulnerable situation for exploitation or blackmail.

## OVERVIEW

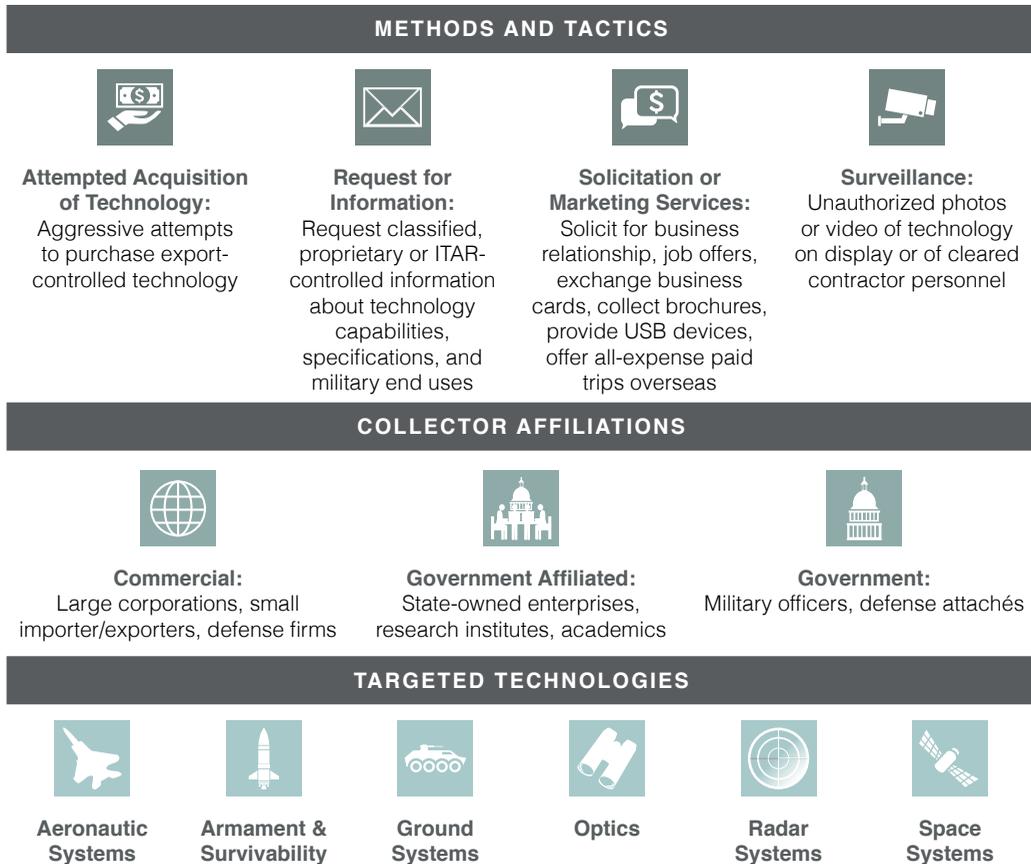
Conferences, conventions, and tradeshow (CC&Ts) allow cleared contractors to display their information and technology, interact with customers, and generate business. That being said, foreign actors – both favorable and those opposed to U.S. interests – can also leverage these open forums to collaborate/network and collect information that could be useful for research, development, and production efforts for military and commercial end use. These venues also provide an opportunity to spot and assess cleared contractor personnel for potential exploitation or future targeting.

Consistent with prior fiscal years, the affiliations of foreign actors targeting cleared contractor information and technology at CC&Ts primarily consisted of government (military officers/defense attachés), government affiliated (research institutes/academics), and commercial (company representatives). These actors conduct various tactics at CC&Ts, to include overt collection of exhibitor materials, direct questioning, elicitation, solicitation of business and services, unauthorized photography/video recording, and physical inspection of exhibits.

## EAST ASIA & THE PACIFIC

In FY16, countries from the East Asia and the Pacific region remained the most prominent threat to cleared contractors at CC&Ts. East Asia and the Pacific commercial entities were the most conspicuous actors exploiting CC&Ts by taking unauthorized photos, soliciting for business partnerships, and exchanging business cards with cleared contractor personnel. Alternatively, government and government-affiliated entities from this region—to include military officers, defense attachés, research institutes, and academics – were far more aggressive in their collection activities of technology and

**FIGURE 2: CONFERENCES, CONVENTIONS, & TRADESHOWS TARGETING OVERVIEW**



cleared contractor personnel in attendance. The government and government-affiliated entities appeared to more often target cleared personnel in attendance, rather than the technology on display. East Asia and the Pacific entities solicited the experts on the displayed technology, as well as other systems the cleared companies are involved in that were not on display. In addition, East Asia and the Pacific entities offered high paying jobs overseas and all-expense paid trips to cleared contractor employees who were either technical experts for a certain technology or had access to a variety of sensitive information and technologies within their respective company.

**Analyst Comment: Foreign entities very likely view CC&Ts as target-rich environments, which provide access to information and technology that could help fill military research and development (R&D) gaps, particularly for armament and survivability, aeronautic systems, optics, and C4 technologies. It is likely FIE from this region will continue aggressive solicitation of cleared contractor personnel at CC&Ts. Offers of all-expense paid trips and lucrative employment are becoming increasingly common. This tactic is an effective method to acquire proprietary or classified information from technical experts whose knowledge will greatly**

**FIGURE 3: PRACTICAL COUNTERMEASURES****THREAT AWARENESS BRIEFINGS**

Attend pre and post travel briefings from your company's security or counterintelligence office

**PACK WISELY**

Travel with sanitized electronic devices loaded with only software and information that is relevant and releasable

Anticipate that all personal belongings and electronic devices will be tampered with and exploited (frequently in hotel rooms)

**BE COGNIZANT OF YOUR SURROUNDINGS**

Assume that any conversations and/or actions occurring in hotel rooms, restaurants, and bars will be monitored

Limit sensitive discussions in public areas

**BE CONSCIOUS OF THE INFORMATION YOU SHARE**

Provide fewer details on your business cards; use a general company email address and phone number; shorten position description

Refrain from revealing personal information to individuals you meet

Ignore or deflect intrusive or suspicious inquiries or conversations about professional or personal matters

Do not post pictures or mention you are on travel on social media until you return

**ONLY DISPLAY APPROPRIATELY CLEARED TECHNOLOGIES**

Photos will be taken of the technology on display, ensure the mock-up displays do not show anything sensitive or export-controlled

### **assist foreign indigenous military R&D. (Confidence Level: High)**

#### **EUROPE & EURASIA**

In FY16, there was a notable presence of commercial and government entities from Europe and Eurasia countries at CC&Ts interacting with cleared contractors and conducting various levels of collection activities. Commercial representatives, linked to military R&D efforts, commonly attended CC&Ts to solicit cleared contractors for business opportunities, exchange business cards, ask specific questions about technology capabilities, and take unauthorized photos. Europe and Eurasia government defense attachés and military officers used similar methods at CC&Ts, to

include solicitations for business cooperation and exchanging business cards. While such solicitations are consistent with behavior at CC&Ts, the actors often leveraged these interactions to target cleared contractor personnel at a later date. Europe and Eurasia entities often targeted armament and survivability, aeronautic systems, ground systems, and space systems technologies.

**Analyst Comment: FIE will likely continue interactions with cleared contractors during CC&Ts and leverage such activity for follow-up meetings with cleared personnel. These encounters provide FIEs from this region the opportunity to build and develop both personal and business relationships for possible exploitation to acquire sensitive or classified information**

**from cleared contractors. (Confidence Level: High)**

## **NEAR EAST**

In FY16, Near East entities continued to represent a significant threat to cleared contractors attending CC&Ts. Both commercial and government entities frequently requested restricted information about U.S. defense technology and/or solicited for business partnerships with various cleared contractors. Near East defense firms were the most prominent actors in attendance at CC&Ts taking unauthorized photos, exchanging business cards, collecting brochures, and soliciting for sensitive or International Traffic in Arms Regulation (ITAR) information. Government, military, and embassy representatives often aggressively requested sensitive information on military system capabilities. Some of these incidents occurred at CC&Ts hosted in

Near East countries. Near East entities were primarily interested in technology focused on aeronautic, ground, and radar systems.

**Analyst Comment: FIE will likely continue aggressive requests for sensitive information from cleared contractors during CC&Ts. Acquiring this information would ultimately assist Near East defense firms conducting R&D for their respective governments and military. (Confidence Level: Moderate)**

**Analyst Comment: DSS assesses that FIE will almost certainly continue to use CC&Ts to target cleared contractor information, technology, and personnel. While the number of reported incidents of targeting at CC&Ts is relatively low compared to other contact methods, CC&Ts remain a lucrative venue for collection given the mindset to share information and meet individuals for business or personal relationships. (Confidence Level: High)**

# EAST ASIA & THE PACIFIC

## REPORTING OVERVIEW

In FY16, DSS received 6,193 reports of CI concern, down 3% when compared to last year



DSS attributed 37% of reports to East Asia & the Pacific



The number of reports attributed to this region rose by 3% compared to last year



## TOP TARGETED TECHNOLOGIES

Electronics



Aeronautic Systems



Command, Control, Communication, & Computers



## TOP METHODS OF OPERATION

Attempted Acquisition of Technology



Solicitation or Marketing Services



Academic Solicitation



## OVERVIEW

In FY16, East Asia and the Pacific entities remained the most significant collectors of sensitive or classified U.S. technology and information reported by cleared industry. In terms of the annual share of incidents involving illicit attempts to acquire defense information and technology among countries, East Asia and the Pacific remained the top collector region since at least 2004.

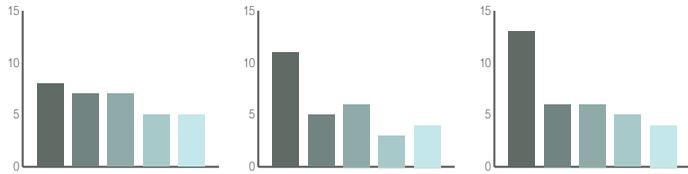
Due to existing rivalries and geopolitical conflicts over land and sea border claims, countries in this region continued to focus efforts on military modernization. East Asia and the Pacific countries remained committed to acquiring or developing technology deemed necessary to deter or defeat adversarial power projection within this region. Along with military modernization, entities showed an increased interest in enabling technologies that can be reverse-engineered and used in pursuit of indigenous R&D.

While East Asia and the Pacific entities targeted almost all technology areas of the IBTL, aeronautic systems, C4, and electronics have remained in the top three targeted technologies for the previous 4 years. Many of the technologies targeted by actors from this region support established science and technology priorities.

East Asia and the Pacific industry, academic, and government entities targeted U.S.-based individuals using a variety of methods, to include: delegation visits, attempts to establish business relationships, overt requests for technology, all-expenses-paid visits to conferences, and seeking employment or academic research positions. In FY16, AAT was the most commonly used MO when targeting cleared technology and information.

For the sixth consecutive year, commercial collectors remained the most prevalent in FY16. Additionally, government-affiliated collectors remained the second most prevalent collector affiliation for the fourth consecutive year. Combined, these two collector affiliations accounted for more than half of all reports from East Asia and the Pacific countries.

**FIGURE 4: EAST ASIA & THE PACIFIC TARGETED TECHNOLOGY OVERVIEW**



	FY16	FY15	FY14
Electronics	8%	11%	13%
Aeronautic Systems	7%	5%	6%
Command, Control, Communication, & Computers	7%	6%	6%
Marine Systems	5%	3%	5%
Radars	5%	4%	4%

**TARGETED TECHNOLOGIES**

Electronics, aeronautic systems, and C4 have been the top three most targeted technologies, in varying order, for each of the last 4 years, and they accounted for nearly 22 percent of the assessed threat to technologies in FY16. East Asia and the Pacific entities have placed an emphasis on developing counterspace, offensive cyber operations, and electronic warfare capabilities meant to deny adversaries the advantage of modern, information technology-driven warfare.

East Asia and the Pacific entities continued targeting electronics-related technology in FY16 with an emphasis on electronic components, particularly with regard to military modernization. These technologies have a number of commercial and military end uses, including missiles, radar, and space-based systems.

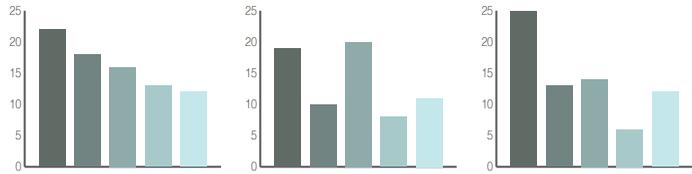
**Analyst Comment: East Asia and the Pacific entities will likely continue to heavily target electronics technologies as countries within the region experience**

**difficulty indigenously producing a wide-variety of electronic components. Therefore, the region relies heavily on procurement of foreign-manufactured components, in particular, U.S.-made components. (Confidence Level: High)**

Just as in FY14 and FY15, C4 technologies remained the second most targeted technology sector. C4 technologies targeted by East Asia and the Pacific entities included data links, satellite communication components, computers, and intelligence, surveillance, and reconnaissance (ISR) systems. East Asia and the Pacific entities use many of these technologies to enhance battlefield communication or deter U.S. intervention or regional aggression in a potential conflict.

In FY16, East Asia and the Pacific entities targeted a range of software-related technology and information. Although East Asia and the Pacific actors have attempted to acquire virtually every software suite available, they have focused efforts on

**FIGURE 5: EAST ASIA & THE PACIFIC METHOD OF OPERATION OVERVIEW**



	FY16	FY15	FY14
Attempted Acquisition of Technology	22%	19%	25%
Solicitation or Marketing Services	18%	10%	13%
Academic Solicitation	16%	20%	14%
Foreign Visits	13%	8%	6%
Request for Information	12%	11%	12%

acquiring different categories of software with the greatest long-term strategic impact on modernizing armed forces; in particular, modeling, simulation, and design software.

**METHODS OF OPERATION**

East Asia and the Pacific collectors most often used AAT, solicitation or marketing services, or academic solicitation when targeting cleared industry. These three MOs accounted for more than half of all reports in FY16. Notably, foreign visits increased from seventh to fourth in FY16. Additionally, suspicious network activity by East Asia and the Pacific entities continued to rank among the top MOs in FY16.

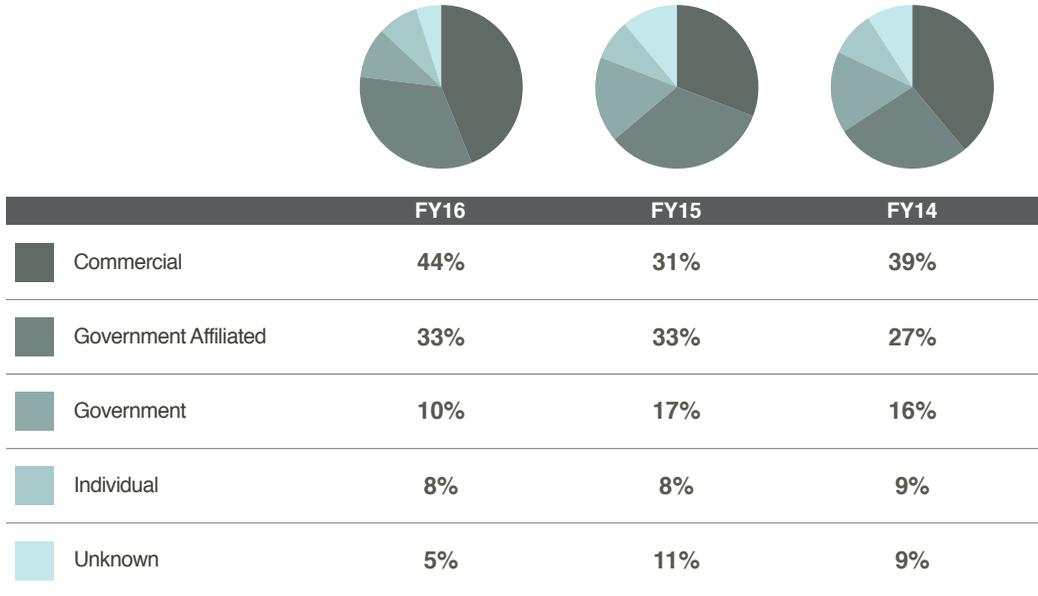
Entities from this region continued to solicit cleared contractors using the AAT MO and focused heavily on acquiring electronics-related information and technology. Entities using this MO sought to conceal the ultimate end user through the use of transshipment routes or front companies.

Actors from East Asia and the Pacific continued to exploit commercial opportunities

through the use of solicitation or marketing services. Entities employing this MO solicited cleared contractors to pursue business opportunities or JVs in attempts to acquire sensitive U.S. defense information and technology in exchange for obtaining access to the East Asia and Pacific market.

**Analyst Comment: The number of U.S. companies establishing business relationships with East Asia and the Pacific companies will most likely continue to increase. The growing commercial interdependence between the United States and the region and the growing capacity and complexity of the region’s economies portend considerable opportunities for U.S. companies to invest and develop. East Asia and the Pacific countries, mindful of U.S. companies’ strong desire to access their markets, will likely continue to exploit business relationships in order to acquire proprietary or sensitive U.S. defense information and technology. (Confidence Level: Moderate)**

**FIGURE 6: EAST ASIA & THE PACIFIC COLLECTOR AFFILIATION OVERVIEW**



East Asia and the Pacific actors exploited existing or proposed relationships with cleared industry, via foreign visits, in order to conduct illicit collection activities. Such visits ostensibly served a legitimate purpose; however, East Asia and the Pacific entities often attempted to exploit the visit to collect information outside the scope of the approved subject. Foreign visits also provided an opportunity for foreign intelligence services to insert an intelligence officer (IO) into a visiting delegation.

In FY16, cleared reporting showed a reduction in the number of East Asia and the Pacific nationals attempting to gain placement and access to cleared contractors through academic or employment positions. Students and researchers from East Asia and the Pacific, who are either current or future experts in their respective fields, gained valuable knowledge working alongside U.S. academics that can ultimately fill intelligence requirements back home.

The majority of RFIs originated from East Asia and the Pacific commercial entities and usually consisted of email or webcard

requests for price quotes or product specifications. Initial requests were typically innocuous, but after establishing contact, subsequent requests often led to unauthorized topics.

Given that collectors intended most computer network operations to be covert, it is virtually impossible to measure the true scale of East Asia and the Pacific state-sponsored cyber activity, which complicates efforts to understand the scope and maturity of their cyber operations and the full impact to cleared industry as a target. While the overall volume of reported, attributable incidents from cleared industry decreased from FY16, East Asia and the Pacific-associated computer network operations (CNO) targeting of cleared industry continued to be very active.

**COLLECTOR AFFILIATIONS**

For the third fiscal year in a row, commercial and nontraditional government-affiliated entities made up the majority of all industry reporting involving East Asia and the Pacific. The threat posed by incidents associated with

commercial entities from this region continued to increase. East Asia and the Pacific commercial entities played a critical role in the acquisition of foreign technology; business partnerships, JVs, company acquisitions, and product acquisitions are all designed to not only improve the competitiveness of industry in East Asia and the Pacific but also fill gaps in information and technology.

Government-affiliated collectors remained the second-most prevalent collector affiliation. Government-affiliated collectors were often tied back to university researchers and students. Academics seeking internships or

research positions were able to collect basic research information at U.S. universities.

Although East Asia and the Pacific entities engage in traditional forms of collection and espionage, nontraditional collectors who do not serve official intelligence roles continue to make up the majority of collection attempts.

**Analyst Comment: Countries within the East Asia and the Pacific region will likely continue to use nontraditional collectors when targeting cleared contractor information and technology. These entities include students and professors, commercial representatives, and defense researchers. (Confidence Level: High)**

PAGE INTENTIONALLY LEFT BLANK

# NEAR EAST

## REPORTING OVERVIEW

In FY16, DSS received 6,193 reports of CI concern, down 3% when compared to last year



DSS attributed 22% of reports to the Near East



The number of reports attributed to this region dropped by 1% compared to last year



---

## TOP TARGETED TECHNOLOGIES

Aeronautic Systems



Command, Control, Communication, &



Energy Systems



---

## TOP METHODS OF OPERATION

Academic Solicitation



Attempted Acquisition of Technology



Request for Information



## OVERVIEW

Overall, industry reporting of suspicious incidents in FY16 attributed to Near East entities demonstrated minor changes in collector affiliations, MOs, and targeted technologies when compared with three prior years of data. As the Near East continued to experience a significant amount of turmoil, collectors targeted a wide variety of military and dual-use technologies.

Near East entities targeted information and technology that would be useful in maintaining and developing military and defense programs. Countries in the Near East region comprise aspiring states, regional powers, and world players. In fact, some of the most active collector countries have enduring conflicts with neighboring states. This regional turmoil leads to continuous targeting of sensitive or classified technology and information resident in cleared industry.

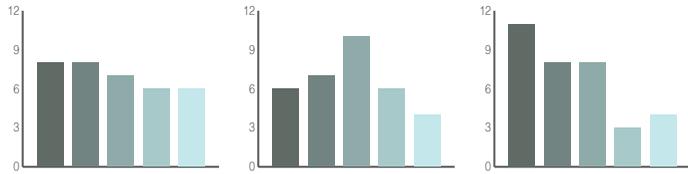
The Near East remained the second most active region based on reports to DSS for the fourth consecutive year. Collectors targeted information and technologies that would be helpful in maintaining indigenous defense operations and developmental programs. Additionally, entities from this region showed particular interest in aeronautic systems and C4.

Government-affiliated collectors continued to be the most prevalent in FY16. When combined with reports of commercial collectors, the second most prevalent, these two collector affiliations counted for more than 70 percent of the overall threat from Near East collectors. Collectors from this region focused on academic solicitation as the most used MO for the sixth year. The assessed threat from academic solicitation more than doubled that of AAT.

## TARGETED TECHNOLOGIES

In FY16, Near East entities most commonly targeted technology associated with aeronautic systems, C4, energy systems, and radars. Aeronautic systems continued as one of the top five technologies targeted by Near East collectors for the past 6 years. Many of the technologies Near East entities sought in FY16 could

**FIGURE 7: NEAR EAST TARGETED TECHNOLOGY OVERVIEW**



	FY16	FY15	FY14
Aeronautic Systems	8%	6%	11%
Command, Control, Communication, & Computers	8%	7%	8%
Energy Systems	7%	10%	8%
Radars	6%	6%	3%
Armament & Survivability	6%	4%	4%

NEAR EAST

fulfill regional countries' offensive or defensive requirements.

Near East entities continued to focus on unmanned aerial vehicle (UAV) technology in FY16. Keeping with trends since 2013, most collection attempts against UAVs focused more on associated technologies rather than actual platforms. These included digital enhanced data links, payload configurations, counter-UAV systems, and laser altimeters.

Consistent with regional goals to create a networked combat capability that can integrate and exploit information from multiple sources, Near East collectors continued their efforts to acquire relevant C4 technologies. These technologies allow Near East states to enhance indigenous production and focus on military programs.

Similar to previous years, Near East students continued attempts to gain access to various U.S. research programs related to energy systems. These research programs conduct advanced research in chemical kinetics,

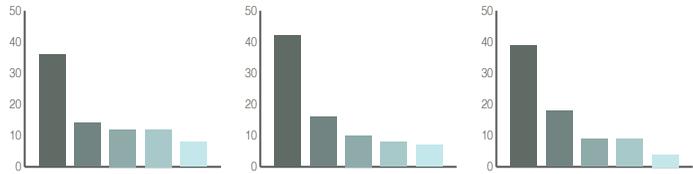
combustion, propulsion, and solid rocket propellants. Radar systems also led the targeted technology list due to Near East students' interest in U.S. research programs focused on digital signal processing, image processing, and radar systems.

**METHODS OF OPERATION**

Academic solicitations continued to be the most reported MO used by Near East entities. During the fiscal year, Near East students' request to U.S. academic and research institutions accounted for approximately 36 percent of the weighted score. This was consistent with the previous 5 years. Near East countries used Near East students and professors with science and engineering backgrounds in the United States to collect sensitive academic and scientific research to advance indigenous weapons programs.

**Analyst Comment: Academic solicitations will likely remain high as increasing numbers of Near Eastern students continue to target U.S. academic programs that can**

**FIGURE 8: NEAR EAST METHOD OF OPERATION OVERVIEW**



	FY16	FY15	FY14
Academic Solicitation	36%	42%	39%
Attempted Acquisition of Technology	14%	16%	18%
Request for Information	12%	10%	9%
Foreign Visits	12%	8%	9%
Seeking Employment	8%	7%	4%

**be directly linked to improving military capabilities. (Confidence Level: Moderate)**

AAT remained the second most reported MO for the fifth consecutive year. While Near East entities continued to rely on foreign assistance to obtain technologies for military and weapons programs, many requests for U.S. technology were routed through front companies, third-country intermediaries, and technology brokers located in countries outside of the Near East.

RFIs and foreign visits each accounted for 12 percent of assessed threat by MOs. Near East collectors often use RFIs and foreign visits to probe for information not provided through official procurement programs. Near East entities often exploited foreign visits during official delegation visits or at conferences or conventions.

Near East collectors continued to leverage CNO to enhance their strategic presence and military proficiency in the region. Key targets of interest to Near East cyber actors were U.S. government and military organizations,

regional adversaries, and members of the U.S. cleared industry.

**Analyst Comment: Cleared industry networks are at increased risk due to Near East computer network exploitation actors' enhanced operational security efforts and changes in network infrastructure. Near East entities will likely continue to leverage CNO for long-term campaigns targeting regional adversaries and U.S. government affiliates—to include cleared industry partners. (Confidence Level: Moderate)**

**COLLECTOR AFFILIATIONS**

Overall, collector affiliations remained consistent with the previous years. Government-affiliated collectors such as Near East students accounted for the vast majority of suspicious contacts to cleared industry. DSS attributed 36 percent of the assessed threat to government-affiliated collectors, consistent with reporting from FY15.

The commercial affiliation increased from 28 to 35 percent in FY16. Near East entities

**FIGURE 9: NEAR EAST COLLECTOR AFFILIATION OVERVIEW**



	FY16	FY15	FY14
Government Affiliated	36%	41%	43%
Commercial	35%	28%	25%
Government	11%	<14%	13%
Individual	<11%	<11%	12%
Unknown	<8%	7%	7%

continued to use front companies and procurement agents to target U.S. sensitive or classified information and technology. Near East collectors' use of commercial entities to collect U.S. technology and information provided placement and access.

Both government and individual collectors accounted for approximately 11 percent of the threat to industry posed by Near East collectors. A large percentage of suspicious contacts originated with current and former Near East students seeking employment

or requesting to join research programs. The individual collector category was also comprised of individuals submitting webcards for information and technology and individuals seeking to connect to cleared industry subject matter experts via social networking services.

**Analyst Comments: Near Eastern governments likely leveraged government-affiliated, commercial entities, and individual collectors in efforts to fulfill government collection requirements. (Confidence Level: Moderate)**

# SOUTH AND CENTRAL ASIA

## REPORTING OVERVIEW

In FY16, DSS received 6,193 reports of CI concern, down 3% when compared to last year



DSS attributed 16% of reports to South & Central Asia



The number of reports attributed to this region dropped by 24% compared to last year



---

## TOP TARGETED TECHNOLOGIES

Radars



Electronics



Aeronautic Systems



---

## TOP METHODS OF OPERATION

Seeking Employment



Attempted Acquisition of Technology



Academic Solicitation



## OVERVIEW

In FY16, South and Central Asia entities remained the third most significant collector of sensitive U.S. information and technology for the third consecutive year, based on industry reporting. Longstanding friction with neighboring states, regional instability, and continued counterinsurgency operations drive military modernization efforts for South and Central Asia countries.

Due to the need for military modernization, South and Central Asia collectors continue to have an interest in a wide variety of technologies, including enabling technologies that can be used in numerous platforms. South and Central Asia entities approach military modernization by procuring, both through legitimate and nefarious means, technologies that they can assimilate into major weapons platforms and upgrade regional military industrial capacity.

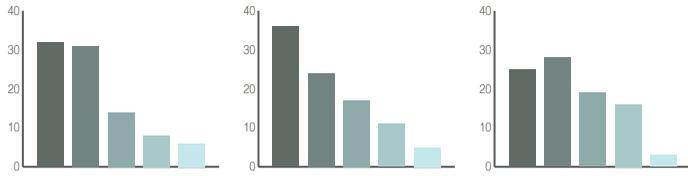
In FY16, South and Central Asia interest in radar and aeronautic systems increased, with specific interest in complete UAVs and associated systems. South and Central Asia government and military entities have also shown significant interest in acquiring enabling technologies within the electronic and C4 categories in an effort to upgrade aging military systems.

Consistent with previous years, South and Central Asia nationals continued to rely heavily on résumé submissions for seeking employment and academic solicitations. These MOs posed the greatest threat to information in cleared industry largely due to the volume of these contacts. Although lower in overall volume, reports involving AAT also posed a critical threat. These efforts consisted largely of commercial entities contacting cleared contractors via email and web card submissions requesting export-controlled technologies on behalf of unknown end users.

## TARGETED TECHNOLOGIES

For the second year in a row, cleared industry reported a significant interest in radar systems, specifically standoff-through-the-wall imaging radar systems from South and

**FIGURE 10: SOUTH & CENTRAL ASIA TARGETED TECHNOLOGY OVERVIEW**



	FY16	FY15	FY14
Radars	11%	5%	5%
Electronics	9%	18%	15%
Aeronautic Systems	7%	5%	3%
Command, Control, Communication, & Computers	7%	8%	7%
Optics	6%	5%	3%

Central Asia entities. Operators typically use these radars for hostage rescue, building surveillance, building clearance, and building search operations.

Reports of South and Central Asia collectors targeting aeronautic systems increased slightly in FY16. Entities from this region often made requests for UAVs and counter-UAV systems, while résumé submissions and academic solicitations related to aeronautical engineering.

Electronics remained one of the top five targeted technologies for the fifth year in a row. In FY16, email requests for various electronics technologies included attenuators, antennas, microcircuits, and x-band transmitters. Email requests from commercial entities frequently included “shopping lists” which listed technologies that could be used in a number of platforms, such as communications, electronic warfare, radar, and space systems.

South and Central Asia government and military entities have shown significant interest

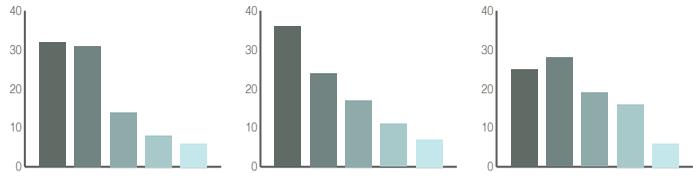
in acquiring enabling technologies within the electronic and C4 categories in an effort to upgrade aging military systems. Some of the most requested components included amplifiers, oscillators, antennas, and radio test sets.

**Analyst Comment: DSS assesses the procurement of enabling components from the electronics and C4 categories will likely continue to be a priority to support military modernization efforts for countries within the South and Central Asia region. These components are less expensive to procure and can be used in a wide variety of military platforms and weapons systems. (Confidence level: Moderate)**

**METHODS OF OPERATION**

Consistent with reporting in previous years, seeking employment and academic solicitations to cleared industry remained the most frequently used means to contact cleared contractors in FY16. Reported incidents primarily consisted of résumé

**FIGURE 11: SOUTH & CENTRAL ASIA METHOD OF OPERATION OVERVIEW**



	FY16	FY15	FY14
Seeking Employment	32%	36%	25%
Attempted Acquisition of Technology	31%	24%	28%
Academic Solicitation	14%	17%	19%
Request for Information	8%	11%	16%
Solicitation or Marketing Services	6%	7%	6%

submissions for employment within cleared industry and requests for research positions or internships at cleared university-affiliated research centers.

Academic solicitation remained one of the top three MOs for the fifth year in a row. Academic solicitation provides opportunities for gaining access to technology and information that is useful for indigenous military modernization efforts.

**Analyst Comment: It is unknown if individuals associated with South and Central Asia universities are tasked to obtain positions within cleared industry; however, it is likely that any technological know-how gained could be used to satisfy defense R&D requirements. (Confidence Level: Moderate)**

While the sheer volume of résumé submissions remained significant, reported incidents of AAT proved to be more concerning in FY16. Commercial and government-affiliated entities frequently

requested sensitive or export-controlled information.

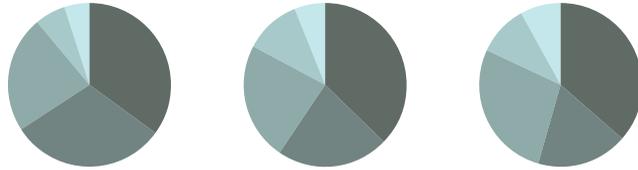
**Analyst Comment: These requests likely mirror regional defense requirements resulting from ongoing military modernization efforts. (Confidence Level: High)**

### COLLECTOR AFFILIATIONS

Commercial companies continued to account for the largest portion and represent the most significant threat of South and Central Asia collection activity reported by cleared industry. According to industry reporting, South and Central Asia companies attempted to procure U.S. technologies for a variety of end users – to include military, government, and restricted end users.

**Analyst Comment: DSS assesses restricted South and Central Asia end users and weapons developers will very likely continue to attempt to use commercial companies as witting or unwitting procurement agents as a means**

**FIGURE 12: SOUTH & CENTRAL ASIA COLLECTOR AFFILIATION OVERVIEW**



	FY16	FY15	FY14
Commercial	35%	37%	37%
Individual	31%	>22%	18%
Government Affiliated	23%	>23%	28%
Unknown	6%	11%	10%
Government	5%	6%	8%

**to obfuscate the real end users of export-controlled technologies. (Confidence level: High)**

Consistent with previous years, reporting attributed academic solicitations and résumé submissions for post-doctoral, research, and

internship opportunities at cleared facilities to individual and government-affiliated entities. Reported collection attempts attributed to government-affiliated entities largely consisted of students, researchers, and professors affiliated with regional academic centers.

# EUROPE AND EURASIA

## REPORTING OVERVIEW

In FY16, DSS received 6,193 reports of CI concern, down 3% when compared to last year



DSS attributed 12% of reports to Europe & Eurasia



The number of reports attributed to this region rose by 11% compared to last year



## TOP TARGETED TECHNOLOGIES

Command, Control, Communication, & Computers



Aeronautic Systems



Electronics



## TOP METHODS OF OPERATION

Request for Information



Attempted Acquisition of Technology



Solicitation or Marketing Services



## OVERVIEW

Multiple countries within Europe and Eurasia remained active collectors of U.S. information and technology. As the fourth most active collector region, Europe and Eurasia accounted for 11 percent of the assessed threat based on reporting in FY16.

FY16 industry reporting showed that Europe and Eurasia maintained an interest in a wide range of technology fields. As in previous years, Europe and Eurasia actors continued to most frequently target C4, aeronautic systems, and electronics.

Just as in FY15, RFI and AAT were the top MOs for FY16. Solicitation or marketing services increased slightly from FY15, moving from fourth to third. AATs, RFIs, and solicitation or marketing services similarly were the top MOs in FY15 and actors most often engaged in these MOs via email.

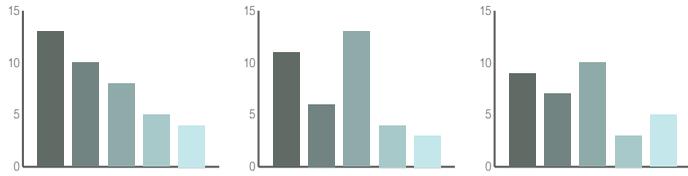
Commercial entities remained the most active collectors from Europe and Eurasia. They continued to show interest in pursuing cutting edge technology to bolster military modernization.

## TARGETED TECHNOLOGIES

In FY16, Europe and Eurasia continued to show at least nominal interest in most technology categories. There were also a noteworthy number of reports with no technology specified or ascertained; these were largely from companies or individuals marketing unspecified services, giving business cards to contractor employees at various locations, as well as cyber activities, which reporting did not attribute to targeting any particular technology. That said, Europe and Eurasia actors demonstrated their strongest interest in C4 components, followed by aeronautic systems and electronics.

As in previous years, C4 was a highly sought after technology area; this coincides with regional countries' modernization efforts to upgrade command and control systems. Reporting has also revealed Europe and

**FIGURE 13: EUROPE & EURASIA TARGETED TECHNOLOGY OVERVIEW**



	FY16	FY15	FY14
Command, Control, Communication, & Computers	13%	11%	9%
Aeronautic Systems	10%	6%	7%
Electronics	8%	13%	10%
Radars	5%	4%	3%
Armament & Survivability	4%	3%	5%

Eurasia collectors' interests in various types of antennas, as well as satellite communications systems.

In FY16, Europe and Eurasia actors again showed a high interest in aeronautics-related systems and information. Companies and government officials in particular sought information on UAVs and related systems.

While targeting of electronics decreased slightly in FY16, reporting revealed procurement agents and government organizations from Europe and Eurasia requested a wide variety of microelectronic components. While procurement actors often listed military and space organizations as end users for these components, there were other instances in which connections were made only through subsequent analysis.

**Analyst comment: Europe and Eurasian countries' interest in C4 aligns with ongoing efforts to modernize command and control systems. Interest in electronics likely can also be attributed to**

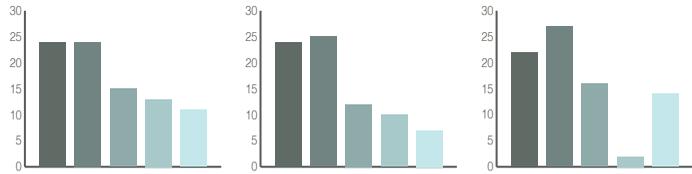
**modernization efforts as modern, capable microelectronics are necessary for most new platforms. Requests related to UAVs have increased largely due to observations of their operational utility in various situations around the world, to include zones of conflict. (Confidence Level: Moderate)**

**METHODS OF OPERATION**

In FY16, industry reporting reflected significant use of RFI, AAT, solicitation or marketing services, and seeking employment MOs. RFIs were the MO that posed the greatest threat to technology for the second consecutive year.

Europe and Eurasia entities contacted cleared facilities directly most often via email, in which they sought to purchase a technology or requested information on its capabilities. These contacts accounted for almost all of the RFIs and AATs originating from Europe and Eurasia. Similar to previous years, requestors at times either provided little-to-no end-use

**FIGURE 14: EUROPE & EURASIA METHOD OF OPERATION OVERVIEW**



	FY16	FY15	FY14
Request for Information	24%	24%	22%
Attempted Acquisition of Technology	24%	25%	27%
Solicitation or Marketing Services	15%	12%	16%
Seeking Employment	13%	10%	2%
Foreign Visit	11%	7%	14%

information or ignored such questions when posed.

Solicitation or marketing services also continued to be a commonly reported MO Europe and Eurasia collectors used in FY16. The requests in this category varied significantly, including offers to act as a cleared contractor’s distribution office in Europe and Eurasia, invitations to work on a technology, or solicitations for collaboration on an ongoing project or venture.

Europe and Eurasia cyber activity decreased in FY16, although DSS continued to receive reports from cleared industry involving web mail credential harvesting, watering holes, and routine spear phishing.

**Analyst Comment: Most Europe and Eurasia entities likely view the AAT and RFI MOs as normal means of attempting to obtain desired information and technology. An infrequent success can provide a significant reward. Such successes would obviate the need for more surreptitious methods. Request for joint business**

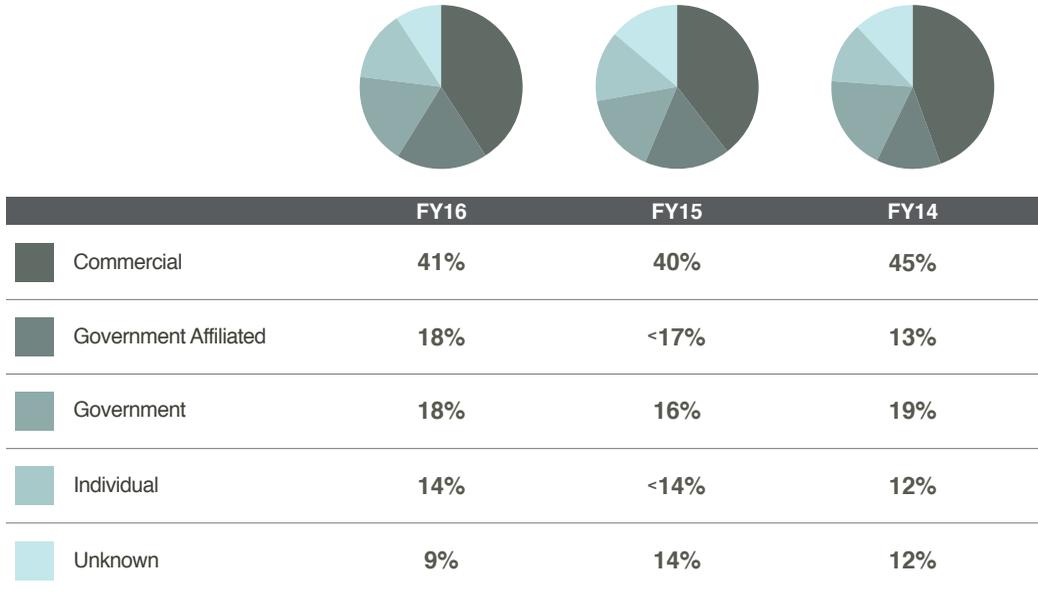
**activities fall into a similar category with the potential for significant gain with little risk. While most of these requests are likely legitimate, DSS cannot rule out that some of the requests are ultimately for the benefit of entities with interests unfriendly to the United States. (Confidence Level: Moderate)**

### COLLECTOR AFFILIATIONS

In FY16, according to industry reporting, commercial actors were the most prominent collectors in incidents associated to Europe and Eurasia, showing a nominal increase over FY15. Europe and Eurasia companies usually contacted cleared contractors attempting to acquire technology or requested information on specific systems. While many of these companies provided end-use information, to include listing government organizations, numerous did not and, at times, increased concern by ignoring requests for it.

Government-affiliated collectors often consisted of research and educational

**FIGURE 15: EUROPE & EURASIA COLLECTOR AFFILIATION OVERVIEW**



institutions with government connections. However, of significant concern in FY16 were reports associated with government actors. These collectors often targeted trade shows and symposiums, where Europe and Eurasia embassy or defense officials approached contractor employees to discuss symposium topics or even suggest follow-on meetings.

**Analyst Comment: DSS assesses most requests from commercial actors in Europe and Eurasia are legitimate. However, DSS cannot rule out that a portion of the interactions consist of nefarious activity, such as hiding end-use information to circumvent export control restrictions. (Confidence Level: Moderate)**

# OTHER REGIONS

The reporting from cleared industry identifying suspicious activities originating in the Western Hemisphere and Africa regions remained consistent over the past three fiscal years. Entities from the Western Hemisphere and Africa regions remained the fifth and sixth most active collectors in FY16, which is consistent with the previous two years. Collectively, entities from these regions represented slightly more than 7 percent of the threat score and volume of suspicious incidents reported by cleared industry.

## WESTERN HEMISPHERE

The reporting from cleared industry identifying suspicious activities originating in the Western Hemisphere slowed slightly in FY16 as compared to the previous 2 years. Collectors from the Western Hemisphere remained the fifth most pervasive collection threat to information and technology resident in the cleared industrial base. These collectors accounted for 6 percent of the threat score, as well as 6 percent of reporting from cleared industry. Targeting from this region remained constant over the past 3 years with electronics, C4, aeronautic systems, and armaments and survivability as the top four most targeted technologies not always in that order. RFI was the most pervasive MO, and commercial entities were the most common collector from this region each year since FY14.

In FY16, targeting from this region focused on electronics, C4, aeronautic systems, and armaments and survivability. These four technologies accounted for 40 percent of the assessed threat, while all other categories of the IBTL had 25 percent of the threat, and incidents where the technology was not part of the IBTL or analysts could not identify the specific technology represented 35 percent of the threat targeting. Commercial entities accounted for over 90 percent of the targeting of electronics. Accelerometers, magnetometers, and field programmable gate array integrated circuits were common electronics targeted by these collectors.

Within C4 technologies, antennas were a commonly targeted component. Hybrid quadrotor, micro, and vertical takeoff and landing UAV were the most aggressively targeted aeronautic systems in FY16.

Collectors from the Western Hemisphere applied RFIs, seeking employment, and solicitation or marketing services as the most effective collection methods. These three methods accounted for 75 percent of the assessed threat from this region. Commercial entities and individuals accounted for 85 percent of these collection attempts. Collectors used email as the vector for the contact in 86 percent of incidents involving RFIs. Email was also the most common vector in incidents of solicitation or marketing of services as the MO. Following email, personal contact was the next most common means of approaching cleared industry.

Commercial entities and individuals posed the most threat to information and technology at cleared facilities. These two affiliations posed 85 percent of the assessed threat from this region during FY16. By far, commercial entities were the greatest threat. They posed 68 percent of the assessed threat and accounted for 62 percent of the incidents associated with this region. Commercial entities most aggressively targeted electronics and armament and survivability technologies, followed by C4 and aeronautic systems. Commercial collectors applied RFIs in 44 percent of their attempts to collect information

and technology from cleared industry and sent 90 percent of these requests via email.

**Analyst Comment: Along with commercial and individual collectors targeting technology for commercial or market advantage, it is very likely that some of these entities are front ends or brokers working for procurement networks that originate in other regions. (Confidence Level: Moderate)**

**Analyst Comment: Collectors from this region will likely continue to account for a small portion of the threat cleared industry faces each year. Over the next 2 to 3 years, their activity will likely represent less than 10 percent of the foreign targeting of cleared industry. (Confidence Level: High)**

## AFRICA

Entities from this region were the sixth most aggressive collectors targeting cleared industry in FY16. Although the assessed threat of the incidents credited to entities from this region increase by over 12 percent, they accounted for slightly more than 1 percent of the overall threat. Collectors from this region primarily focused their efforts on C4 and aeronautic systems technologies. AAT and seeking employment were the most prevalent MOs used to target information and technology resident with the cleared industrial base. For the third consecutive year, commercial entities were the most aggressive collectors, and for the first year accounted for over half of the assessed threat from the region.

Collectors from the Africa region primarily targeted C4 and aeronautic systems technology. These two technologies accounted for nearly one-third of the assessed threat to technology from this region. The next two actively targeted technologies were software and ground systems and each accounted for 7 percent or less of the assessed threat. In FY16, entities from Africa represented a low volume of the incidents reported by cleared industry; however, their collection targeting C4 technologies was

significantly active. In over half of the incidents from this region's targeting of C4 technologies, DSS assessed the incident as presenting a high threat to that technology. DSS identified a government entity as the actor involved in 75 percent of these high threat incidents. Conversely, commercial entities represented the most effective collectors targeting aeronautic systems technology.

**Analyst Comment: The aggressive targeting of C4 technology by government entities from the Africa region is likely to improve indigenous military and security forces' counter-terrorism and security operations capabilities. It is very likely that these technologies are to support forces serving as part of the African Union Mission in Somalia (AMISOM). (Confidence Level: Moderate)**

The most pervasive MOs applied by entities from Africa were AAT and seeking employment. Each of these MOs represented 32 percent of the threat targeting from Africa. Although incidents of these MOs had the same threat score, AAT incidents were of greater concern. DSS assessed over half of the incidents involving AAT as being of high or moderate threat, while DSS assessed all incidents involving seeking employment as being of low threat. The number of incidents involving seeking employment was more than double the number of incidents of AAT. For each of these two MOs, in most incidents collectors used email to establish contact.

For the second year running, commercial entities and individuals were the most aggressive collector affiliations from this region. Commercial entities were responsible for 55 percent of the threat score and 54 percent of the volume of incidents originating in this region. Commercial entities most actively targeted aeronautic systems technology. The commercial entities applied the AAT MO sent via email in over half of the incidents. Individuals from this region relied on seeking employment MO in 74 percent of the incidents reported by cleared industry. Since applications to cleared facilities rarely

specify technologies, DSS could not identify the specific technology targeted in these incidents.

**Analyst Comment: Entities from Africa will likely continue to increase their targeting of U.S. technologies in cleared industry over**

**the next three years. However, even with a modest growth in the number of incidents originating from this region, it will almost certainly remain the least active collector region. (Confidence Level: High)**

PAGE INTENTIONALLY LEFT BLANK

# OUTLOOK

Foreign entities will almost certainly continue to target cleared industry through attempts to obtain unauthorized access to sensitive or classified information and technology in FY17 and beyond. Cleared industry reporting of suspicious incidents has increased for the past decade. As more companies continue to report, collaborative understanding between government and industry stakeholders of general and specific threats to cleared industry will improve. (Confidence Level: High)

Entities from regions identified in this report will almost certainly continue using a variety of MOs to acquire, steal, or interdict technologies critical to U.S. military advantage. Additionally, foreign entities' collection efforts will almost certainly continue to target a wide variety of sensitive or classified technologies, in development or production, in cleared industry, spanning the entirety of the IBTL. While their rankings might shift, it is unlikely there will be a change in the top collector regions in the next fiscal year. (Confidence Level: High)

Active military modernization programs will very likely continue to be a motivation for top collectors from East Asia and the Pacific, South and Central Asia, and Europe and Eurasia targeting cleared industry. The top regions are seeking to improve their indigenous defense industries to limit reliance on foreign acquisitions, improve their military technology for export, or ensure military strength in disputed regions. These modernization programs will likely drive the targeting of aeronautic systems, C4, electronics, radar, and armament and survivability technologies to fill perceived military technology gaps. (Confidence Level: High)

In the next 5 to 10 years, foreign collectors will likely increase targeting of artificial intelligence (AI) with applications for modeling and simulation software and autonomous systems. Foreign collectors will likely target information relating to AI that enables interdependent autonomous thought and action and that models human behavior for scenario-based decision making and training environments. Collectors will also target AI applications for existing autonomous systems, including marine reconnaissance and survey vehicles, fire-and-forget weapons, and weapons with loitering capabilities. As the requirements for remote and autonomous systems able to operate without human connection continue to increase, foreign collectors will target hardware, software, and systems with information related to AI to answer foreign collection requirements. These requirements seek to ensure parity with, enable indigenous production of, and enable countermeasures for reconnaissance systems, autonomous weapons systems, decision support simulators, and other AI reliant technologies that provide improved loiter time or enhance operations in denied areas. (Confidence Level: Moderate)

Foreign entities will likely continue to use various methods of contact to target U.S. cleared contractor information, technology, and personnel at CC&Ts. While the number of such targeting at CC&Ts is relatively low compared to other contact methods, these venues will likely remain a prime target of collection given that CC&Ts are setup to share information and meet individuals to develop business or personal relationships. It is possible that any and all information or technology obtained by these foreign entities at CC&Ts will assist in indigenous research

and development efforts for a military or government-related project. (Confidence Level: Moderate)

AAT, academic solicitation, and RFI have been in the top five MOs for the past 5 years; this is unlikely to change because they are minimal-risk, low-cost methods for targeting sensitive or classified U.S. information and technology. (Confidence Level: High)

Foreign entities will almost certainly continue to use suspicious network activity—likely through spear phishing attacks and attempted network intrusions—to target cleared contractor networks for access to sensitive U.S. technologies. Cleared contractors have improved their ability to detect and defeat cyber attacks; however, cleared industry must continue to advance cyber defenses and reduce cyber vulnerabilities since cyber actors will almost certainly continue to adjust existing exploitation techniques and develop new ones. (Confidence Level: High)

To remain competitive in a global market, U.S. industry continues to develop foreign partnerships and business opportunities. Entities from East Asia and the Pacific, the Near East, and South and Central Asia have close relationships with the United States and

cleared industry. Some entities from these regions will likely exploit those relationships to collect sensitive or classified information and technology resident in cleared industry. JVs and close partnerships can potentially leave contractors vulnerable to the exploitation of relationships and foreign visits. Additionally, commercial entities from these regions will likely continue using solicitation or marketing services as a way to begin a business relationship with cleared contractors, which opens a potential avenue to access sensitive information, technology, and manufacturing processes. (Confidence Level: High)

Foreign entities will continue to target cleared employees to exploit the resources of cleared industry and academia and gain access to U.S. information and technology. Unfortunately, if they are successful, the information is lost to our adversaries forever. The threat shows no sign of waning, and securing our cutting-edge technology remains the key to maintaining a military and economic advantage. Over time, the methods used or technologies targeted may change, but the persistence and aggressiveness of foreign entities attempting to illicitly obtain information from cleared industry will almost certainly remain unchanged. (Confidence Level: High)

# DSS CATEGORY DESCRIPTIONS

## 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 and 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 neuroscientific bases of cognition.

### **Command, Control, Communication, and Computers**

The hardware that comprises command, control, communication, and 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 and 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 and 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, and 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.

**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.

## 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 web form 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.

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

# ACRONYMS AND ABBREVIATIONS

AAT	attempted acquisition of technology	IBTL	Industrial Base Technology List
AI	artificial intelligence	IC	Intelligence Community
ANV	assessed no value	IO	intelligence officer
C4	command, control, communication, and computers	ISR	intelligence, surveillance, and reconnaissance
CC&Ts	conferences, conventions, and tradeshows	ITAR	International Traffic in Arms Regulation
CI	counterintelligence	JV	joint venture
CISA	counterintelligence special agent	MO	method of operation
CNE	computer network exploitation	NISPOM	National Industrial Security Program Operating Manual
CNO	computer network operations	R&D	research and development
CPI	Critical Program Information	RFI	request for information
DoD	Department of Defense	SCR	suspicious contact report
DSS	Defense Security Service	SNA	suspicious network activity
FIE	foreign intelligence entity	UAV	unmanned aerial vehicle
FY	fiscal year	UCR	unsubstantiated contact report

**For more information about the Defense Security Service, please visit  
[www.DSS.mil](http://www.DSS.mil) or [www.CDSE.edu](http://www.CDSE.edu)**

