Targeting U.S. Technologies
A Trend Analysis of Cleared Industry Reporting
• Purpose
• Key Findings
• Overview
• Special Focus Area
• Regional Assessments
  • East Asia and the Pacific
  • Near East
  • South and Central Asia
  • Europe and Eurasia
• Outlook
• Conclusion
• U.S. defense-related technologies and information are under attack from foreign entities: each day and every hour
• Each suspicious contact report (SCR) makes a difference
  • In fiscal year 2012 (FY12), industry reporting led to 657 investigations or operations against known or suspected collectors
• The Trends report is designed to be a reference tool for industry security professionals in their efforts to detect, deter, mitigate, or neutralize the effects of foreign targeting
Key Findings

- East Asia and the Pacific and the Near East remain the most active collecting regions, with East Asia and the Pacific alone responsible for half of all reported incidents.

- Commercial entities, though still the most common collectors, are now rivaled by government and government-affiliated entities.

- Suspicious network activity (SNA) is the predominant method of operation (MO) for collectors, especially those from East Asia and the Pacific.

- Collectors targeted all categories of the Militarily Critical Technologies List (MCTL), but remained most interested in information systems and electronics.
While commercial collectors remained most common affiliation world-wide, the portion attributed to this category fell from 34 percent in FY11 to 29 percent in FY12.

Reports of government and government-affiliated entities both increased in percentage.
Overview - Methods of Operation

- SNA became the most commonly reported MO in FY12
- Attempted acquisition of technology (AAT) dropped to second most commonly reported MO and request for information (RFI) slid from second down to fourth
- Academic solicitation was the third most common MO overall, and the most common MO for collectors from the Near East

Methods of Operation

- Suspicious Network Activity
- Attempted Acquisition of Technology
- Academic Solicitation
- Request for Information
- Solicitation or Marketing Services
- Foreign Visit
- Seeking Employment
- Exploitation of Relationships
- Surveillance
- Criminal Activities
- Search/Seizure
The technologies reported as targeted showed significant stability:

- Information systems; electronics; lasers, optics, and sensors; and aeronautic systems were the same top categories in FY11.

The most significant change was the surge in reported collection attempts targeting electronics:

- The number of incidents related to electronics increased by 93 percent.

Top Targeted Technologies:
- Information Systems
- Electronics
- Lasers, Optics, & Sensors
- Aeronautics
- Materials & Processes
- Space Systems
- Positioning, Navigation, & Time
- Marine Systems
- Information Security
- Processing & Manufacturing
Special Focus Area - Missile Technology

- U.S. cleared contractors lead the world in research, design, and engineering of offensive and defensive missiles

- Many different areas of expertise are required to master missile development
  - Each type of missile contains various subsystems that control its propulsion, guidance, and payload, all within a frame of composite materials

- Primary regions targeting missile technologies:
  - East Asia and the Pacific
  - Near East
  - Europe and Eurasia
Missile Technology Outlook

- Missile technology will remain of significant interest to countries with missile modernization needs.
- Countries with advanced missile programs will proliferate illicitly acquired technology through military sales and technical assistance.
- Collectors primarily rely on commercial entities to attempt to acquire U.S. missile technology.
- AAT will likely remain the predominant MO, although collectors will almost certainly increase the use of SNA.
East Asia and the Pacific

- Significant increase in the number of SCRs in FY12; accounted for half of all industry reporting
- Collector Affiliations
  - Government
  - Commercial
- Targeted Technologies
  - Electronics, information systems, and lasers, optics, and sensors (LO&S) most commonly targeted
  - SNA remained primary MO, increasing by almost three and a half times; AAT and Academic Solicitation next most favored MOs
East Asia and the Pacific - Outlook

Outlook

- Entities from this region will almost certainly continue to aggressively attempt to collect U.S. information and technology.
- Actors from this region will likely be number one adversary for cleared industry in cyber space.
- Spear phishing emails will remain the primary targeting method.
- Will continue to use of overt requests from government-affiliated and commercial collectors.
- For cyber actors from this region marine, information systems, and aeronautics will likely be the top collection priorities.

Case Study

- September 2011 - commercial entity requested two different types of solid-state switches.
- Entity does business with an agency of his country’s government.
- According to another U.S. government agency, the government in question has been interested in the technology since 2004.
- Country hoped to develop a system similar to the to the U.S. product by 2012; likely collecting because of an unmet objective in the program.
- Number of SCRs increased by 40 percent in FY12
- Collector Affiliations
  - Government-affiliated
  - Commercial
- Targeted Technologies
  - Primary targeted technologies included: information systems; lasers, optics, and sensors; and aeronautics systems
  - Most frequent MOs were academic solicitation and AAT
Case Study

- July 2012 - Cleared contractor received multiple requests for microwave electronic components from entities in Europe and Eurasia, East Asia and Pacific, and Near East
- OGA reporting identified one of the individuals representing the East Asia and Pacific entity as connected to Near East entity, as well as Europe and Eurasia entity
- Likely an attempt to illicitly procure and transfer technology

Outlook

- Trade limitations and other economic difficulties may spur collection efforts, especially in critical areas, such as air defense
- Students will likely solicit assistance on research to acquire dual-use components
- Official delegations will likely exploit visits to cleared facilities
- Wide variety of technologies sought, including dual-use items for chemical and nuclear programs
South and Central Asia

- SCRs increased by more than two-thirds
- Collector Affiliations
  - Government-affiliated
  - Commercial
- Targeted Technologies
  - Primary targeted technologies included: electronics; lasers, optics, and sensors; and information systems
  - Frequently used AAT and Academic Solicitation as approaches
South and Central Asia - Outlook

Outlook

- Entities will likely exploit legitimate business relationships to acquire U.S. technology.
- Government entities will probably discreetly attempt to reverse-engineer legitimately acquired technology.
- Government affiliated entities will likely continue to use academic solicitations to target information resident in cleared industry.
- Electronics and LO&S systems will likely remain the top collection priorities for entities from this region.

Case Study

- Commercial representative requested quote for electronics system on behalf of unidentified end user.
- Cleared contractor requested end user identity; commercial agent refused and instead asked which programs used requested technology.
- Commercial agent also asked whether a third-country program used the technology.
- DSS unable to determine whether end user existed or whether only information gathering.
Europe and Eurasia

- SCRs increased 13 percent in FY11
- Collector Affiliations
  - Commercial
  - Government-affiliated
- Targeted Technologies
  - Primary targeted technologies included: lasers, optics, and sensors; aeronautics systems; information systems; and electronics
  - AAT and RFI accounted for 60 percent of Europe and Eurasian MOs
Case Study

- Europe and Eurasia national approached display booth at cybersecurity conference
- Identified himself as embassy personnel; expressed interest in restricted email security products
- Same individual had made unannounced visit to separate cleared contractor
- OGA reporting indicated individual was an intelligence officer
- Country likely hoping to devise countermeasures to acquired technology

Outlook

- Cuts to defense spending will probably increase incentive for illicit transfer of U.S. technology
- Will continue the exploitation of legitimate commercial exchanges
- Some intelligence entities will likely continue use of social networking sites to spot and assess cleared contractor employees
- Collection efforts will very likely continue to emphasize “component technology” categories of LO&S, aeronautics, and information systems
• Collectors from East Asia and the Pacific will almost certainly remain the most prolific at targeting information and technology resident in cleared industry
• Incidents of SNA will almost certainly continue to increase, and will be conducted primarily by East Asia and the Pacific entities
• The following technologies will likely remain priority targets:
  • Information systems: command, control, communications, computers, intelligence, surveillance, and reconnaissance; modeling and simulation programs; and advanced radio technologies
  • Microelectronics, specifically radiation-hardened
  • Missile systems technologies
  • Telecommunications technologies
  • Energy technologies: batteries, superconductors, biosynthetics
Conclusion

• Number of SCRs increased by 60 percent
• East Asia and the Pacific remained the most prolific collector region, responsible for over half of reported collection attempts in FY12; the Near East remained a distant second
• Commercial entities were again the most common affiliation, though their share of reported affiliations continued to decrease
• For the first time, SNA was the most commonly reported MO, with an increase of 183 percent in FY12
• Upward trends can be partially attributed to an increase in awareness and reporting by cleared contractors
Targeting U.S. Technologies
A Trend Analysis of Cleared Industry Reporting

Available at: http://www.dss.mil/

QUESTIONS?