TARGETING U.S. TECHNOLOGIES

A TREND ANALYSIS OF REPORTING FROM DEFENSE INDUSTRY

2012

AGENDA

- Purpose
- Key Findings
- Overview
- Special Focus Area
- Regional Assessments
  - East Asia and the Pacific
  - Near East
  - Europe and Eurasia
  - South and Central Asia
- Outlook
- Conclusion

PURPOSE

- 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 2011 (FY11), industry reporting led to more than 485 investigations or operations against known or suspected collectors

KEY FINDINGS

- East Asia and the Pacific and the Near East remain the most active collecting regions, with the most attributed attempts at collecting U.S. technologies in FY11
- Commercial entities are the most common collectors, residing at the top of the ranking in five of six regions
- Collectors rely heavily on request for information (RFI) and attempted acquisition of technology (AAT)
  - DSS redefinition of AAT led to a different apportionment of cases in FY11
- Collectors targeted all categories of the Militarily Critical Technologies List (MCTL), but remained most interested in information systems technology

OVERVIEW - REGIONAL TRENDS

FY 2011

EAST ASIA AND THE PACIFIC

NEAR EAST

EUROPE AND EURASIA

SOUTH AND CENTRAL ASIA

FY 2010

EAST ASIA AND THE PACIFIC

NEAR EAST

EUROPE AND EURASIA

SOUTH AND CENTRAL ASIA

OVERVIEW - COLLECTOR AFFILIATIONS

FY 2011

COMMERCIAL
Entities whose span of business includes the defense sector

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

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

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

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

FY 2010

COMMERCIAL
Entities whose span of business includes the defense sector

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

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

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

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

OVERVIEW - METHODS OF OPERATION

FY 2011

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

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

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

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

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

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

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

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

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

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

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

FY 2010

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

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

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

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

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

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

OVERVIEW - TARGETED TECHNOLOGIES

FY 2011

- INFORMATION SYSTEMS TECHNOLOGY
- LASERS, OPTICS, AND SENSORS TECHNOLOGY
- AERONAUTICS SYSTEMS TECHNOLOGY
- ELECTRONICS TECHNOLOGY
- ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY
- SPACE SYSTEMS TECHNOLOGY
- MARINE SYSTEMS TECHNOLOGY
- POSITIONING, NAVIGATION, AND TIME TECHNOLOGY
- MATERIALS AND PROCESSES
- GROUND SYSTEMS TECHNOLOGY
- INFORMATION SECURITY TECHNOLOGY
- PROCESSING AND MANUFACTURING

FY 2010

- INFORMATION SYSTEMS TECHNOLOGY
- LASERS, OPTICS, AND SENSORS TECHNOLOGY
- AERONAUTICS SYSTEMS TECHNOLOGY
- ELECTRONICS TECHNOLOGY
- MARINE SYSTEMS TECHNOLOGY
- POSITIONING, NAVIGATION, AND TIME TECHNOLOGY
- INFORMATION SECURITY TECHNOLOGY
- ARMAMENTS AND ENERGETIC MATERIALS TECHNOLOGY
- SPACE SYSTEMS TECHNOLOGY
- MATERIALS AND PROCESSES
- GROUND SYSTEMS TECHNOLOGY
- PROCESSING AND MANUFACTURING

SPECIAL FOCUS AREA - RAD-HARD

- Radiation-hardened (rad-hard) microelectronics have commercial and military applications
  - Protect microelectronics and electronic systems from the effects of ionizing radiation
  - Ionizing radiation is present during high-altitude flights and space operations and in proximity to fission or fusion reactions
  - Failure of microelectronics in space is costly and can result in the total abandonment of a space system
- Primary regions targeting rad-hard technologies:
  - East Asia and the Pacific
  - Near East
  - Europe and Eurasia
- Particularly strong interest from regions with active or maturing space programs

RAD-HARD OUTLOOK

- Rad-hard microelectronic technology will remain of significant interest to countries with emerging space activities and operations
- Economic growth and military modernization will move terrestrial communication and ISR activities into space, further stimulating demand
- Collecting entities will use a variety of MOs to attempt to collect rad-hard technology in the immediate future
- RFI and AAT will likely be the MOs of choice

Rad-hard Applications

Increased reliability and effectiveness of manned and unmanned space activities that facilitate:

- Commercial and military telecommunication
- Command and control
- Intelligence, surveillance, and reconnaissance (ISR) platforms

RAD-HARD CASE STUDY

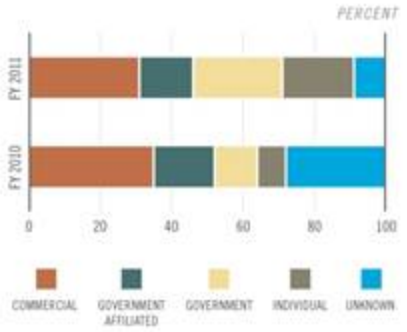
- In September 2011, Chinese nationals Hong Wei Xian and Li Li were sentenced to 24 months in prison for attempting to acquire rad-hard microchips
- Between 2009 and 2010, they attempted to purchase thousands of rad-hard programmable read-only memory (PROM) units in an effort to sell to China Aerospace and Technology Corporation
- Xian and Li sought PROMs specifically designed to withstand radiation bombardment in space, despite knowing that the hardware was export-controlled

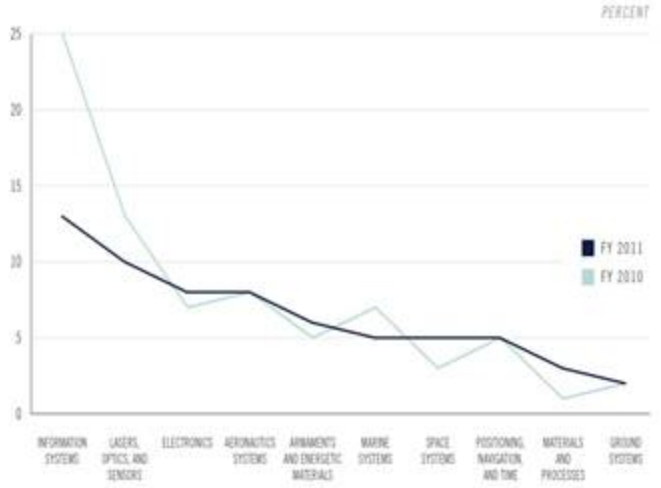
Conclusion:

China Aerospace researches, designs, develops, and produces strategic and tactical missiles and exo-atmospheric launch vehicles. Xian and Li did not seek export-control licenses because doing so would have revealed China Aerospace as the ultimate end user.

EAST ASIA AND THE PACIFIC OVERVIEW

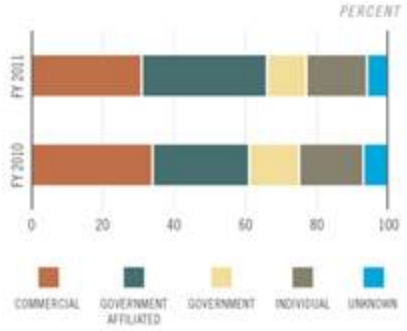
- Significant increase in the number of SCRs in FY11
- Collector Affiliations
  - Commercial
  - Government
- Targeting U.S. Technologies
  - Demonstrated interest in information systems technology and lasers, optics, and sensors technology
  - Favored SNA, AAT, and RFI as approaches
- Outlook
  - Continued use of commercial collectors
  - Continued use of SNA, AAT, and RFI

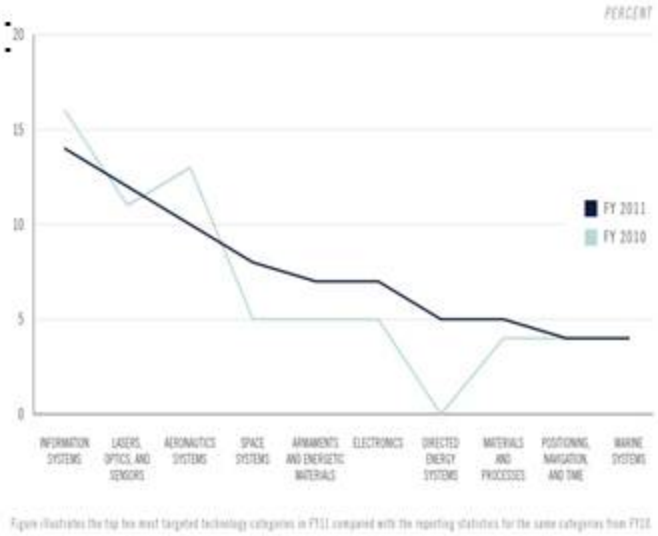




NEAR EAST OVERVIEW

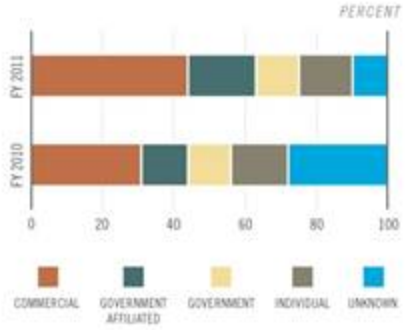
- Number of SCRs increased by 75 percent in FY11
- Collector Affiliations
  - Government affiliated
  - Commercial
- Targeting U.S. Technologies
  - Primary targeted technology included: information systems; lasers, optics, and sensors; aeronautics systems
  - Most frequent MOs were academic solicitation and AAT
- Outlook
  - Long-term goal to achieve self-sufficiency in defense industries





EUROPE AND EURASIA OVERVIEW

- SCRs increased 60 percent in FY11
- Collector Affiliations
  - Commercial
  - Government affiliated
- Targeting U.S. Technologies
  - Primary targeted technology included: aeronautics systems; lasers, optics, and sensors; information systems; electronics systems
  - AAT and RFI accounted for roughly half of Europe and Eurasian MOs
- Outlook
  - Will need to continue to augment indigenous technology development



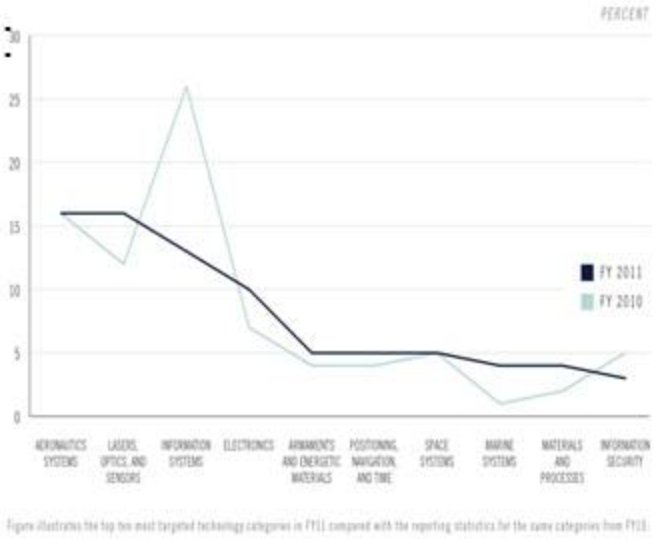
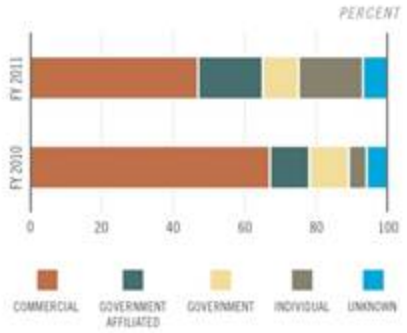


Figure illustrates the top two most targeted technology categories in FY11 compared with the reporting statistics for the same categories from FY10.

SOUTH AND CENTRAL ASIA OVERVIEW

- SCRs more than doubled in FY11
- Collector Affiliations
  - Commercial
  - Unknown
- Targeting U.S. Technologies
  - Primary targeted technology included: information systems; lasers, optics, and sensors; aeronautics systems; electronics systems
  - Frequently used AAT and RFI as approaches
- Outlook
  - Regional instability will continue to drive efforts to obtain U.S. information and technology



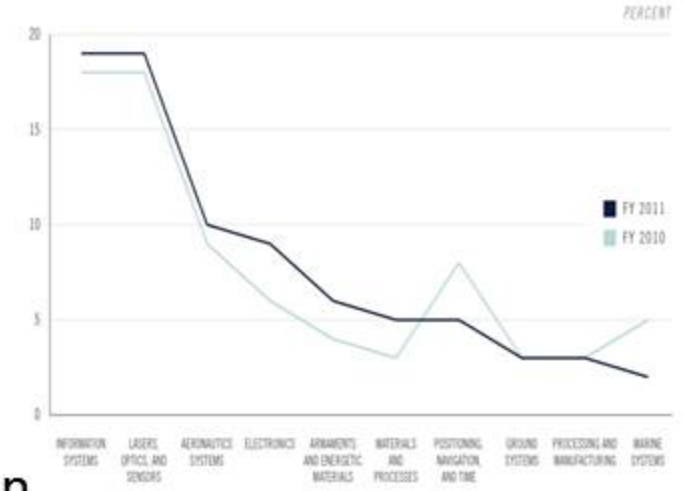


Figure illustrates the top ten most targeted technology categories in FY11 compared with the reporting statistics for the same categories from FY10

CONCLUSION

- Number of SCRs increased 75 percent in FY11
- East Asia and the Pacific and the Near East remain the most prolific collector regions, responsible for 61 percent of reported collection attempts in FY11
- Commercial entities were the most common affiliation in five of the six regions
- Upward trends can be partially attributed to an increase in awareness and reporting by cleared contractors
- Continued vigilance constitutes the first line of defense against those who would do us harm

OUTLOOK

- Collectors from East Asia and the Pacific will almost certainly remain the most prolific at targeting information and technology resident in cleared industry
- While MOs used by collectors will continue to evolve, AAT and RFI will likely remain most prominent
- The following technologies will likely remain priority targets:
  - Information systems: command, control, communications, computers, intelligence, surveillance, and reconnaissance; modeling and simulation programs
  - Lasers, optics, and sensors: radar associated with missile defense; optics and sensors associated with unmanned aerial vehicles (UAVs) and autonomous underwater vehicles
  - Aeronautics: Joint Strike Fighter, UAV programs
  - Electronics technology: Communication systems, electronic warfare systems

Defense Security Service

Counterintelligence Directorate

QUESTIONS?