TARGETING U.S. TECHNOLOGIES

A REPORT OF FOREIGN TARGETING OF CLEARED INDUSTRY

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

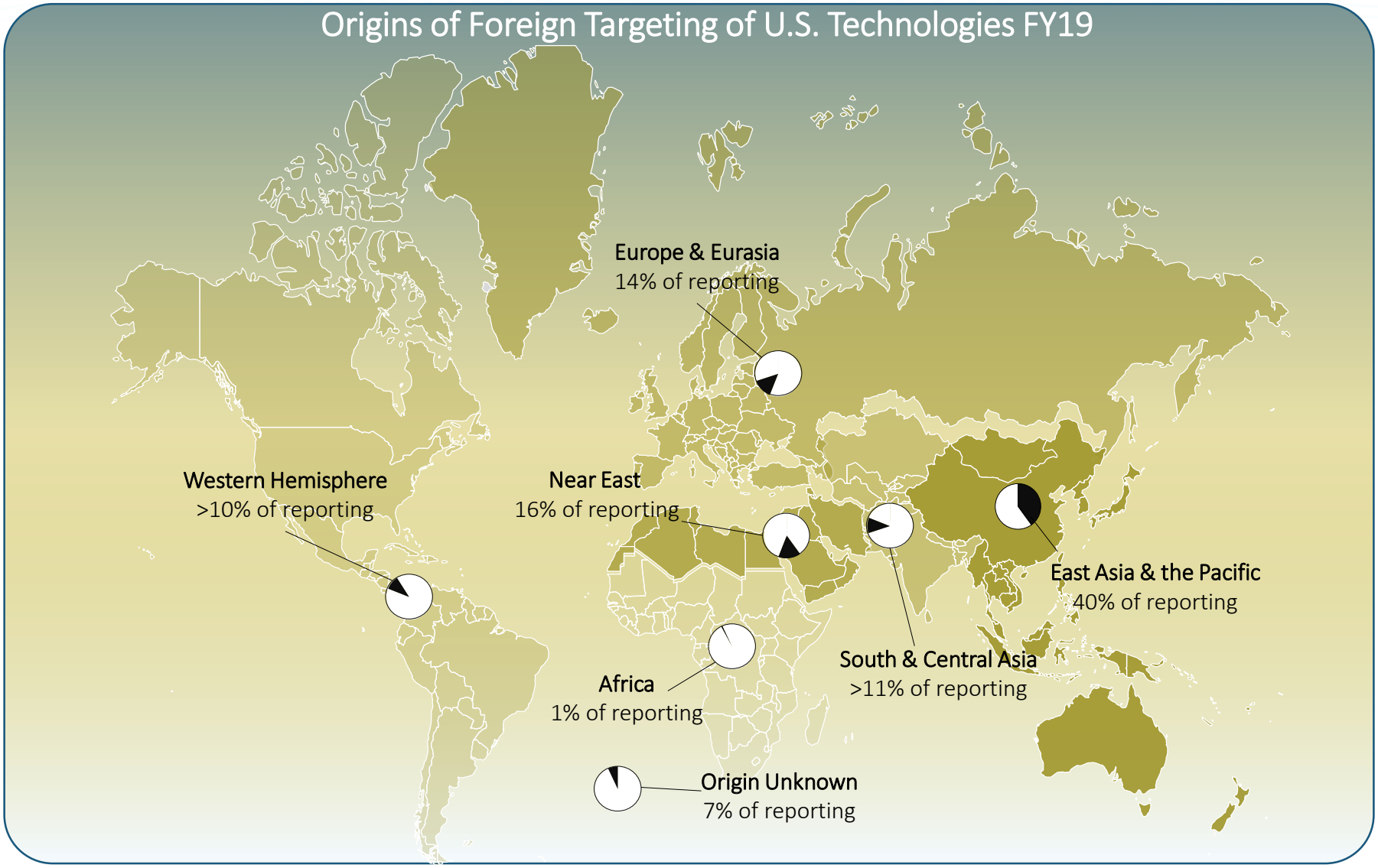
Agenda

- Agenda
- Background
- Executive Summary
- Targeting by Geographic Region
- Conclusion

Background

- FY19 cleared industry submitted 6,121 reports that the Defense Counterintelligence and Security Agency (DCSA) assessed as likely an attempt to obtain unauthorized access to classified or sensitive information and technology
- These suspicious contact reports (SCR) from cleared industry represent an incident of a likely foreign entity attempting to illicitly obtain access to information or technology at a facility
  - This presentation is not a holistic assessment of foreign intelligence targeting of cleared industry; DCSA cannot assess the volume foreign collection attempts that go unidentified or unreported
- Counterintelligence awareness and training sources:
  - DCSA https://www.dcsa.mil/; and
  - The Center for Development of Security Excellence (CDSE) https://www.cdse.edu/.

Executive Summary

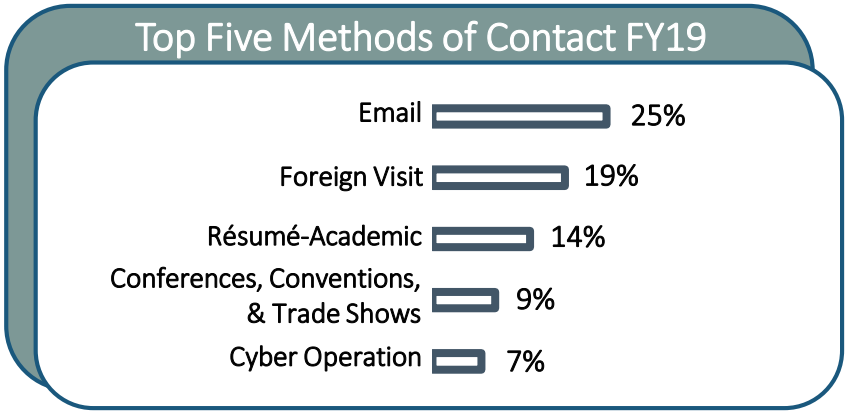


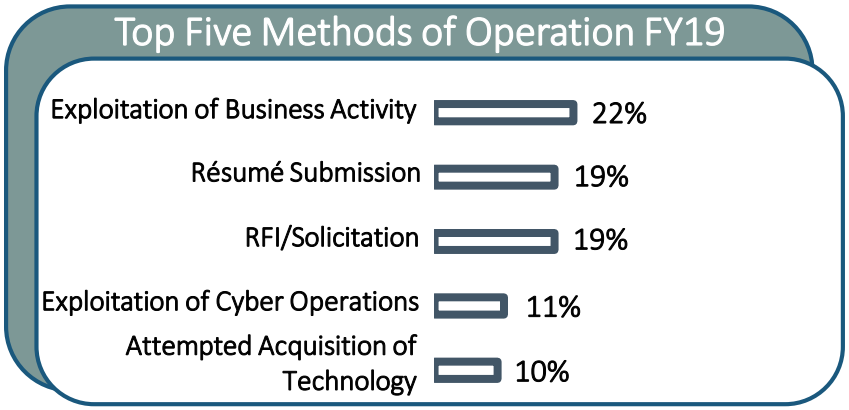
Executive Summary

Most Targeted Technologies	
Aeronautic Systems	11%
Electronics	8%
Armament & Survivability	5%
Command, Control, Communication, & Computers (C4)	5%
Manufacturing Equipment & Mfg Processes	3%
Software	3%
Marine Systems	2%
Radars	2%
Ground Systems	2%
Optics	2%

- The number of cleared industry reports that DCSA assessed to be suspicious contacts increased by 2% from FY18
- FY19 was the first year Manufacturing Equipment & Manufacturing Processes was in the top five most targeted technology categories
- Aeronautic Systems was the most commonly sought technology category:
  - Unmanned aerial vehicle (UAV) & Drones (counter-drone/anti-drone), fixed and rotary wing aircraft, and flight simulator software are commonly targeted sub-technologies
- 42% of reported suspicious contacts didn't involve a specified targeted technology

Executive Summary





- Email remained the most common method of contact (MC) in FY19
  - Including incidents of phishing operations (an attempt to send malicious code via an email) cleared industry received nearly 30% reported incidents via email
- Incidents occurring during foreign visits increased significantly over FY18

- The top five most common methods of operation (MO) accounted for 81% of incidents
- Exploitation of business activity increased by 126% over FY18
  - Seeking to leverage existing commercial relationships for unauthorized access to classified U.S. technology/information

Targeting by Geographic Region

East Asia & the Pacific

Top 10 Targeted Technologies

Electronics	10%
Aeronautic Systems	10%
Armament & Survivability	4%
C4	4%
Mfg Equip. & Mfg Processes	3%
Agriculture	3%
Software	3%
Marine Systems	3%
Radars	2%
Optics	2%

Top 5 Methods of Operation

RFI/Solicitation	22%
Résumé Submission	21%
Exploitation of Business Activity	21%
Exploitation of Experts	13%
Attempted Acquisition of Technology	9%

Top 5 Methods of Contact

Email	32%
Résumé - Academic	19%
Foreign Visit	18%
Conferences, Conventions, & Trade Shows	11%
Social Network Services	5%

Most Common MO + MC Combinations

Résumé Submission + Résumé - Academic	15%
RFI/Solicitation + Email	15%

- East Asia and the Pacific collectors remained the most active in FY19, accounting for 40% of reporting from cleared industry
- Volume of incidents related to this region remained consistent with FY18
- Electronics and aeronautic systems remained most targeted technology categories for this region in FY19, although manufacturing equipment/processes increased significantly
- 20% of reported exploitation of cyber operations incidents originate from this region

East Asia & the Pacific - Case Study

Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data

- Chinese intelligence officers and those working under their direction conducted or otherwise enabled repeated intrusions into private companies' computer systems in the United States and abroad for over five years
- Targeted intellectual property and confidential business information related to a turbofan engine being developed by a partnership between a French aerospace company and a U.S.-based company
- The charged intelligence officers and co-conspirators worked for the Jiangsu Province Ministry of State Security (JSSD), an arm of the Ministry of State Security (MSS)
- JSSD allegedly co-opted Chinese workers employed at the French aerospace company's Suzhou office to load malware on to the company's computers
- JSSD sponsored hackers targeted the U.S. company involved in developing the engine and companies providing parts for the engine
- At the time of the intrusions a Chinese state-owned was working to build a comparable engine

Takeaway: This is likely an example of the MSS conducting criminal activities to facilitate stealing intellectual property for China's commercial gain.

https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

Targeting by Geographic Region

Near East

Top 10 Targeted Technologies

Aeronautic Systems	8%
Electronics	8%
Armament & Survivability	8%
C4	4%
Radars	4%
Software	4%
Ground Systems	3%
Mfg Equip. & Mfg Processes	3%
Optics	3%
Energy Systems	2%

Top 5 Methods of Operation

Résumé Submission	33%
Exploitation of Business Activity	22%
RFI/Solicitation	15%
Attempted Acquisition of Technology	12%
Exploitation of Experts	7%

Top 5 Methods of Contact

Résumé - Academic	23%
Email	20%
Foreign Visit	18%
Résumé - Professional	10%
Conferences, Conventions, & Trade Shows	9%

Most Common MO + MC Combinations

Résumé Submission + Résumé - Academic	21%
Exploitation of Business Activity + Foreign Visit	15%

- DCSA identified entities from the Near East in 14% of cleared industry reporting in FY19
- Reporting associated to entities from the Near East increased by 28% in FY19
- Majority of reported incidents involved leveraging personal access to cleared personnel, via post-doctoral degrees, defense conferences, foreign visits
- Entities affiliated with region requested nearly every category of IBTL, with emphasis on aeronautic systems, electronics, and armament & survivability

Near East - Case Study

Export Company Executive Pleads Guilty to Violating U.S. Sanctions against Iran

- An executive at an export company pleaded guilty to conspiring to unlawfully export gas turbine parts from the United States to Iran
- Executive was President and Managing Director of an export company with an office in the United Arab Emirates and is a supplier of spare and replacement turbine parts for power generation companies in the Middle East, including Iran
- The executive worked with companies in Canada and Germany to violate and evade U.S. sanctions against Iran
- Executive had Canadian and German companies order parts from distributers in Florida and New York
- After the parts arrived in Canada and Germany, the executive worked with the companies to have the parts shipped to Iran

Takeaway: When purchasing sensitive technology, Illicit actors often hide eventual end user and end use of by identifying countries with favorable trade status as the destination. Often foreign entities will use brokers in the United States or other countries to disguise the actual end user or the requested technologies.

https://www.justice.gov/opa/pr/export-company-executive-pleads-guilty-violating-us-sanctions-against-iran

Targeting by Geographic Region

Europe & Eurasia

Top 10 Targeted Technologies

Aeronautic Systems	13%
Armament & Survivability	7%
Electronics	6%
C4	5%
Mfg Equip. & Mfg Processes	5%
Marine Systems	4%
Ground Systems	4%
Software	3%
Space Systems	3%
Optics	2%

Top 5 Methods of Operation

Exploitation of Business Activity	30%
RFI/Solicitation	21%
Attempted Acquisition of Technology	13%
Exploitation of Cyber Operations	11%
Exploitation of Experts	9%

Top 5 Methods of Contact

Foreign Visit	24%
Email	24%
Conferences, Conventions, & Trade Shows	12%
Cyber Operations	8%
Web Form Submission	8%

Most Common MO + MC Combinations

Exploitation of Business Activity + Foreign Visit	19%
RFI/Solicitation + Email	10%

- DCSA identified entities from the Europe & Eurasia region in 14% of cleared industry reporting in FY19
- Reporting associated to entities from Europe & Eurasia increased by 15% in FY19
- Leveraging commercial relationships and access to experts via foreign visits increased significantly over FY18
- Aeronautic systems remained most targeted technology from this region, increasing 57% from FY18

Targeting by Geographic Region

South & Central Asia

Top 10 Targeted Technologies

Aeronautic Systems	15%
Electronics	11%
C4	7%
Armament & Survivability	5%
Radars	3%
Software	3%
Mfg Equip. & Mfg Processes	3%
Energy Systems	2%
Optics	2%
Marine Systems	2%

Top 5 Methods of Operation

Exploitation of Business Activity	27%
Résumé Submission	27%
RFI/Solicitation	19%
Attempted Acquisition of Technology	16%
Exploitation of Experts	6%

Top 5 Methods of Contact

Foreign Visit	26%
Email	26%
Résumé - Academic	14%
Résumé - Professional	14%
Web Form Submission	10%

Most Common MO + MC Combinations

Exploitation of Business Activity + Foreign Visit	23%
Résumé Submission + Résumé - Professional	13%

- DCSA identified entities from South & Central Asia region in 11% of cleared industry reporting in FY19
- Reporting associated to entities from South & Central Asia increased by 4% in FY19
- Incidents occurring during foreign visits—exploitation of business activities and experts—increased significantly over FY18
- Regional South & Central Asia reporting was primarily associated with aeronautic systems technology

Targeting by Geographic Region

Western Hemisphere

Top 5 Targeted Technologies	
Aeronautic Systems	13%
Electronics	5%
Armament & Survivability	5%
C4	4%
Mfg Equip. & Mfg Processes	4%

- DCSA identified entities from the Western Hemisphere region in 10% of cleared industry reporting in FY19
- Reporting of entities from Western Hemisphere targeting technology increased 36% from FY18
- In FY19, regional Western Hemisphere reporting was primarily associated with aeronautic systems technology
- Collectors from this region used exploitation of business activity and RFI/Solicitation as the most common MOs

Africa

Top 5 Targeted Technologies	
Armament & Survivability	14%
Aeronautic Systems	8%
Biological	5%
C4	5%
Electronics / Space Systems	4%

- DCSA identified entities from the Africa region in a little over 1% of cleared industry reporting in FY19
- Reporting of entities from Africa targeting technology decreased by 13% over FY18
- Most often targeted armament and survivability technologies
- Exploitation of business activity was the most common MO used by collectors from this region
- Foreign Visit was the MC applied in 25% of the incidents from this region

Questions

Questions?