CDSE Center for Development of Security Excellence

Counterintelligence Webinar Series: Targeting U.S. Technologies 2019

LEARN.
PERFORM.
PROTECT.

TODAY'S SESSION

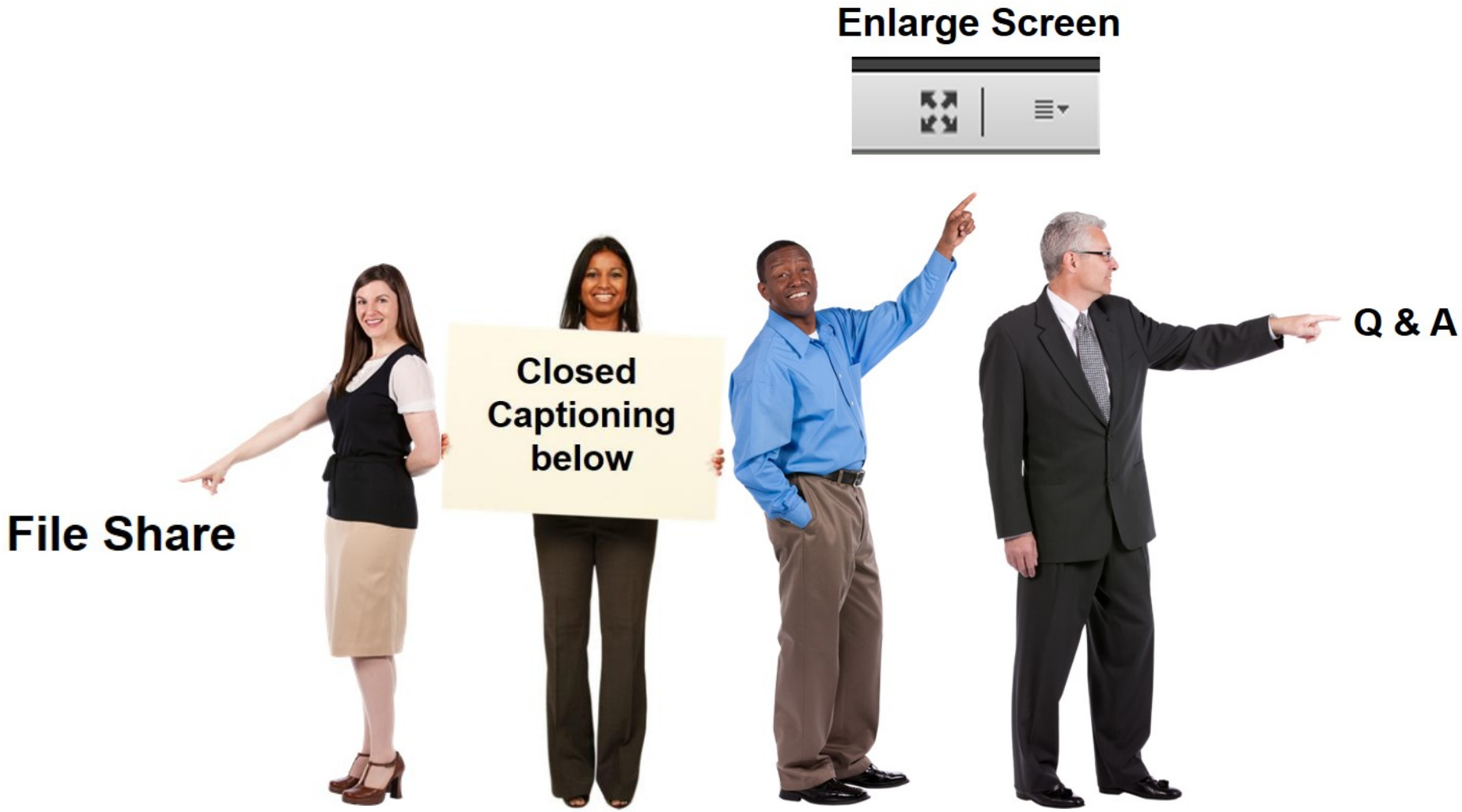
HOST:

Ed Kobeski, CDSE Counterintelligence

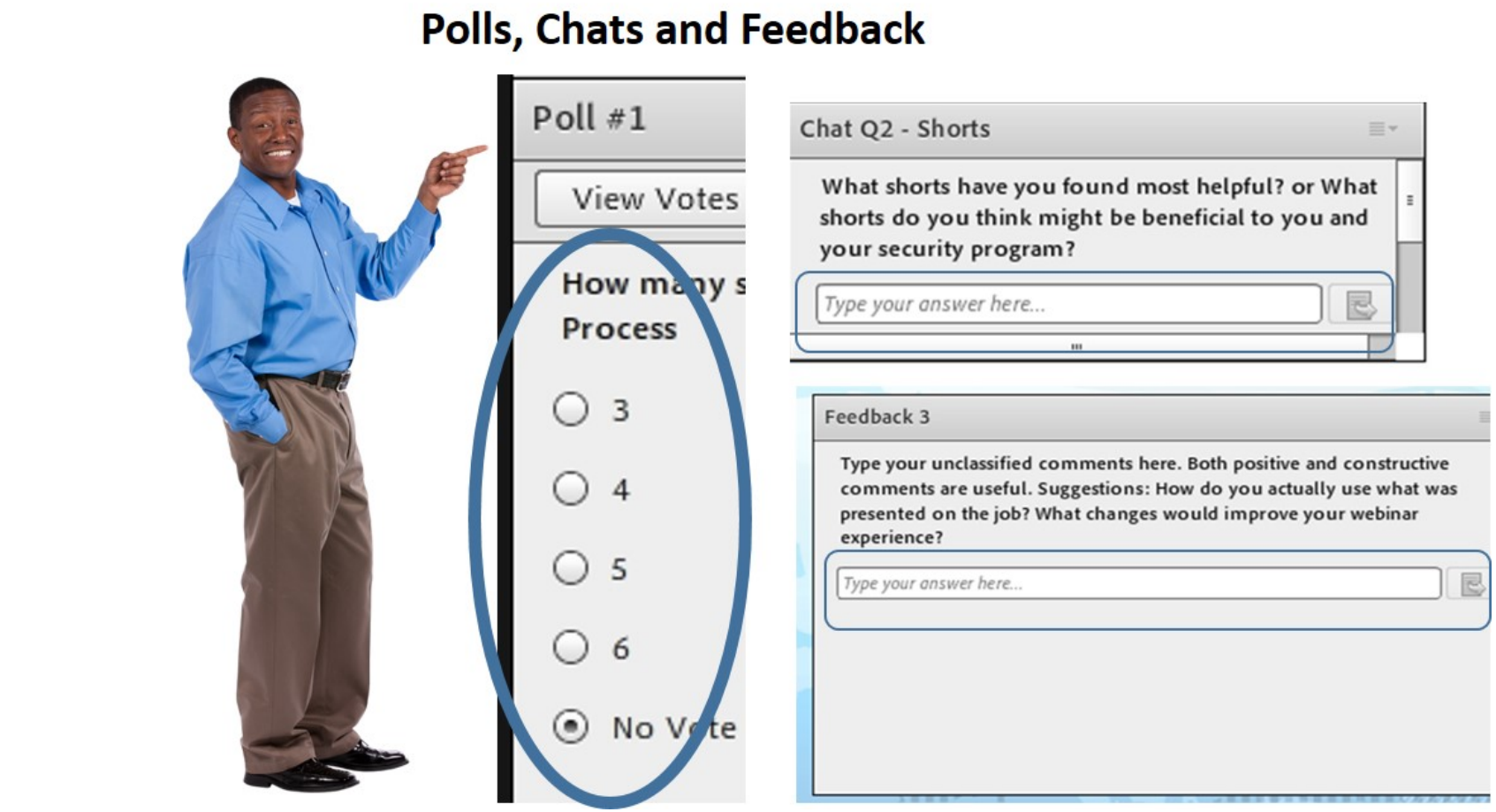
GUEST:

Mr. Brett Young, DCSA CI Production Branch Chief

Attendee Participation & Feedback



Attendee Participation & Feedback



Post Event Feedback

At the end of our event, please take a few minutes to share your opinions

Your feedback helps us improve the quality of our offerings.

Responding will only take a few minutes.

Responding is optional.

UNCLASSIFIED

Targeting U.S. Technologies

A Report of Foreign Targeting of Cleared Industry

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

2019

UNCLASSIFIED

Agenda

- Agenda
- Background
- Executive Summary
- Targeting of Technologies
- Targeting by Geographic Region
- Special Topics

(U) This product may contain information associated with United States Persons Information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided, in accordance with Executive Order 12333 and Department of Defense Manual 5240.01. It should be handled and protected in accordance with applicable Intelligence Oversight rules by persons and organizations subject to those rules. DCSA collects, retains, and disseminates United States Persons Information in accordance with applicable laws, directives, and policies. Should you require minimized United States Persons Information, contact DCSA Production Branch at (571) 305-6572.

Background

- FY18 cleared industry submitted 6,026 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
- Case studies and other U.S. Government (USG) assessments referenced in this presentation are from public press releases from the U.S. Department of Justice (DoJ) and the White House
- Counterintelligence awareness and training sources:
  - DCSA https://www.dcsa.mil/; and
  - The Center for Development of Security Excellence (CDSE) https://www.cdse.edu/.

Audience Poll Question #1

- In FY 18 Reporting, what was the most targeted Industrial Base Technology List (IBTL) technology according to Suspicious Contact Reporting (SCRs)?

- A. Nuclear
- B. Electronics
- C. Software
- D. Raw Materials
- E. Services and Other Products: Janitorial Services

Executive Summary

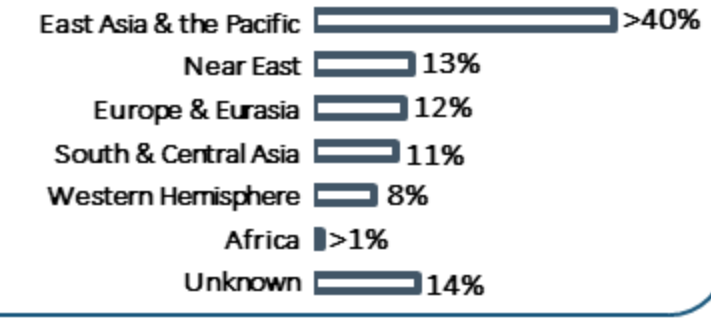
Most Targeted Technologies

- Electronics
- Aeronautic Systems
- Command, Control, Communication, & Computers (C4)
- Armament & Survivability
- Optics
- Radars
- Software
- Space Systems
- Marine Systems
- Energy Systems

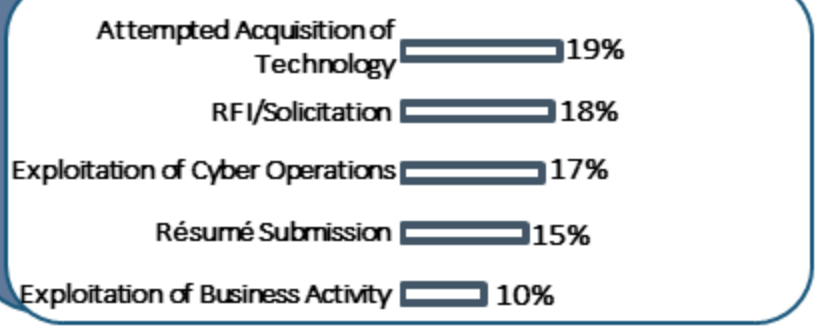
- The number of cleared industry reports that DCSA assessed to be suspicious contacts increased by 3% from FY17
- FY18 was the first year Optics was in the top five most targeted technology categories
- Electronics was the most commonly sought technology category:
  - Targeted electronics included – radiation hardened integrated circuits, monolithic microwave integrated circuits, programmable gate arrays (FPGA), circuit boards, digital signal processors, and wafers
- Foreign entities targeted unmanned or independent systems across Industrial Based Technology List categories:
  - Unmanned aerial vehicles (UAV), autonomous underwater vehicles, unmanned surface vessels, and unmanned ground systems; along with artificial intelligence software

Executive Summary

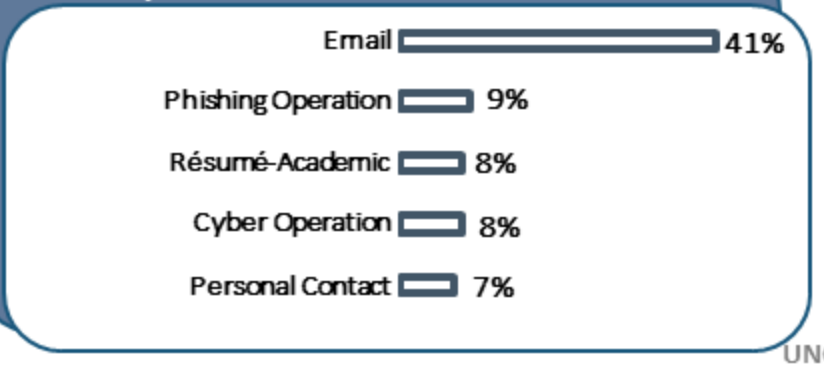
Targeting by Geographic Region FY18



Top Five Methods of Operation FY18



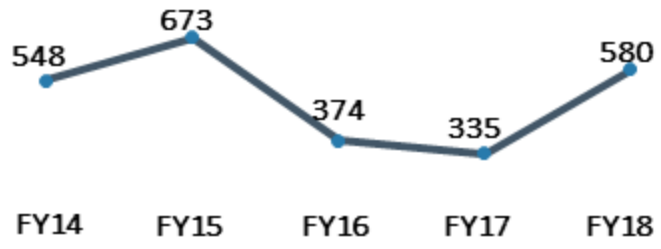
Top Five Methods of Contact FY18



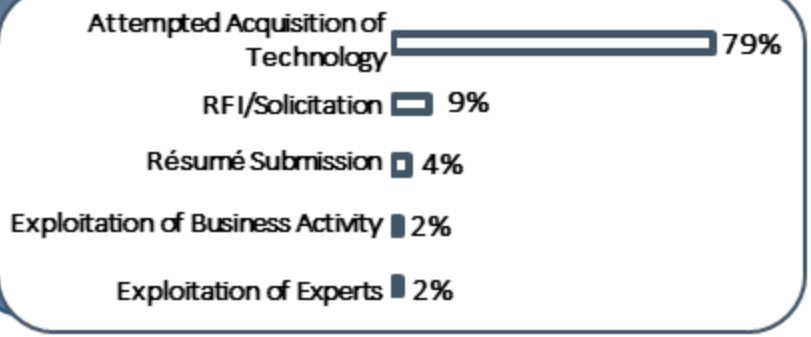
- East Asia & the Pacific accounted for 40% of industry reporting
  - Increase of 20% over FY17
  - China has been cited in multiple USG investigations and initiatives as having policies for technology transfer and intellectual property theft
- The top five most common methods of operation (MO) accounted for 79% of incidents
  - Exploitation of cyber operations increased by 55% over FY17
- Email was overwhelmingly the most common method of contact (MC) in FY18
  - Including incidents of phishing operations (an attempt to send malicious code via an email) cleared industry received half of all reported incidents via email

Targeting of Technologies - Electronics

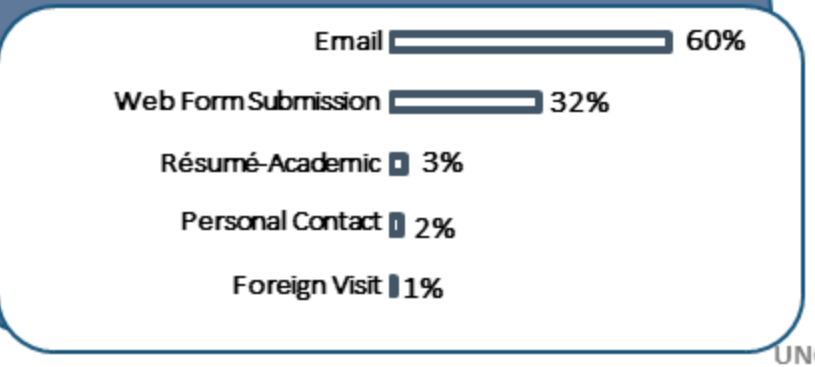
Targeting of Electronics FY14 – FY18



Top Five Methods of Operation FY18



Top Five Methods of Contact FY18



- Targeting of electronics in FY18
  - Most targeted technology in FY18
    - One of top three targeted technologies for past 7 years
  - 73% increase in reported targeting from FY17
  - East Asia & the Pacific accounted for 53% of the incidents
    - South & Central Asia 24%
    - Europe & Eurasia 13%
  - Commercial entities were the most common collectors, identified in 73% of reports
  - Attempted acquisition of technology identified as the MO in 79% of the incidents
  - Email was the MC in 60% of incidents

Top Targeted Electronics

Integrated Circuits
- Monolithic Microwave IC (MMIC)

Radiation Hardened IC
FPGA
Digital Signal Processors
Circuit Boards
Vacuum Tubes
Wafers

Targeting of Electronics- Case Study

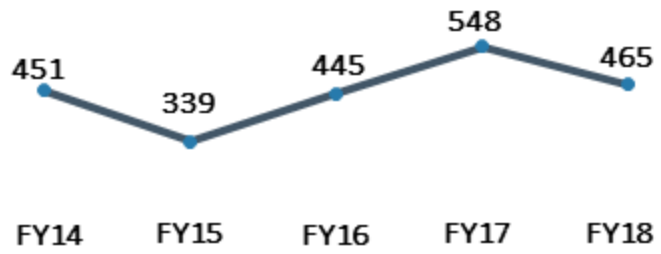
- Indicted in 2018, USPER1 was found guilty on June 26, 2019, of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), a Federal law that makes illegal, among other things, certain unauthorized exports
- USPER1 conspired with the co-defendant USPER2 to illegally export to China Monolithic Microwave Integrated Circuits (MMIC) with dual use applications
- USPER2 established access to a U.S. company's computer system by posing as a domestic customer seeking to purchase MMICs for use solely in the United States
- USPER2 illegally provided USPER1 unauthorized access to the company's protected computer system
- USPER1 used USPER2's account to hide intent to ship MMICs to China
- The MMICs USPER1 sent to China require an export license from the Commerce Department
- USPER1 never sought to obtain an export license
- According to DoJ, these MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures, and radars

Takeaway: Web form submission is a common MC. It allows a level of anonymity and for illicit actors to pose as legitimate domestic customers and obfuscate the ultimate destination of the parts.

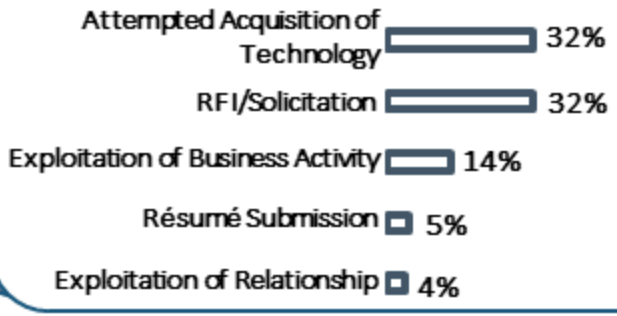
https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage

Targeting of Technologies – Aeronautic Systems

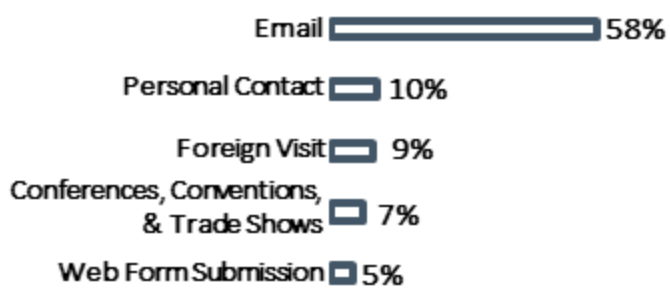
Targeting of Aeronautic Systems FY14 – FY18



Top Five Methods of Operation FY18



Top Five Methods of Contact FY18



- Targeting of aeronautic systems in FY18
  - Second most targeted technology in FY18
    - One of top three targeted technologies for past 6 years
  - 15% decrease in reported targeting from FY17
  - East Asia & the Pacific accounted for 34% of the incidents
    - Europe & Eurasia 17%
    - Near East; Western Hemisphere 13%
  - Commercial entities identified in 55% of reports
  - Attempted acquisition of technology sent via email was the most common MO + MC combination used in 29% of incidents in FY18

Top Targeted Aeronautic Systems

UAVs & Drones
- Counter-drone/Anti-drone

Fixed Wing Aircraft

Airframes and Structural Components

Flight Simulator Software

Rotary Wing Aircraft

Avionics

Targeting of Aeronautic Systems - Case Study

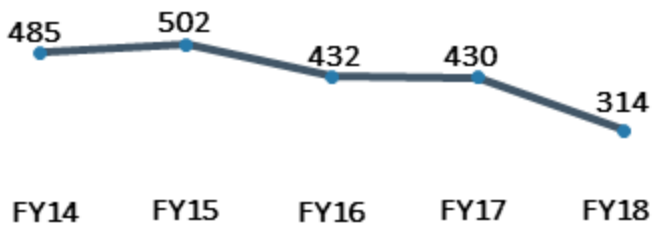
- U.S. District Court of Washington, DC, sentenced an Australian national to 24 months in prison and a forfeiture of $199,227 for shipping aircraft parts to an Iranian company in violation of U.S. embargo
- Australia extradited the defendant to the United States in 2018, and he pled guilty to the charges in February 2019
- According to the plea documents, the defendant solicited purchase orders from a representative of a trading company in Iran; the Iranian representative also operated companies in Malaysia that served as intermediaries for the Iranian company
- Defendant placed orders with U.S. companies for goods including aircraft parts that the Iranian company could not buy directly in the United States without approval of the U. S. Government
- Defendant placed orders through a broker in the United States and intentionally concealed the actual end user and end use for the parts
- Defendant attempted to or acquired precision pressure transducers, which have applications in avionics; emergency flotation systems kits designed for use on the Bell 206 helicopters, and shock mounted light assemblies used with helicopters and fixed wing aircraft

Takeaway: Foreign corporations and governments use brokers in the United States or in countries with favorable trade status to disguise the actual end user and end use of export-controlled technologies.

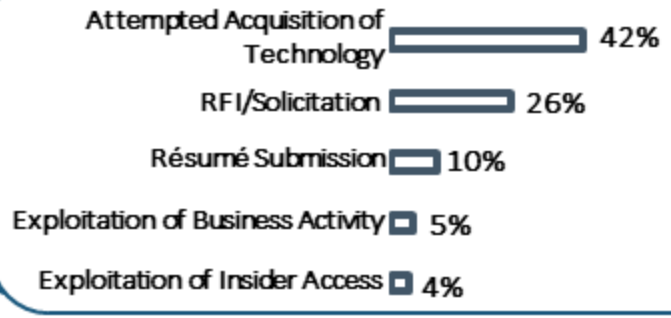
https://www.justice.gov/opa/pr/australian-national-sentenced-prison-term-exporting-electronics-iran

Targeting of Technologies – C4

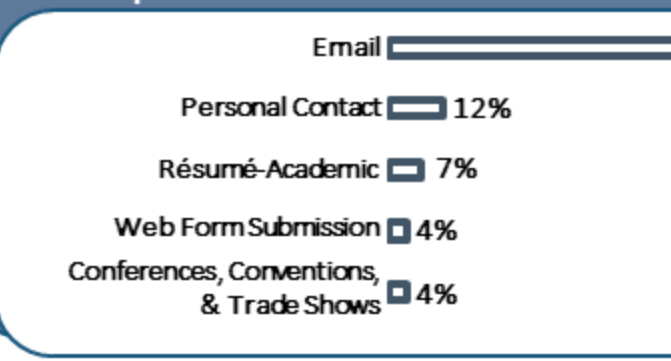
Targeting of C4 FY14 – FY18



Top Five Methods of Operation FY18



Top Five Methods of Contact FY18



- Targeting of C4 in FY18
  - Third most targeted technology in FY18
    - Since FY13 C4 has been one of the top three targeted technologies
  - 27% decrease in reported targeting from FY17
  - East Asia & the Pacific accounted for 32% of the incidents
    - Europe & Eurasia 18%
    - Near East 17%
  - Commercial entities were the most common affiliation - identified in 53% of reports
  - Attempted acquisition of technology sent via email was the most common MO + MC combination used in ~38% of incidents in FY18

Top Targeted C4

Antenna	Telecommunications Devices
Wide Area Surveillance Systems	Wireless Networks
Computers & CPUs	Common Data Links
Air & Missile Defense C2	Waveguide Components

Targeting of C4 - Case Study

- In early 2019, the U.S. District Court for the Southern District of Texas sentenced a Chinese national for selling counterfeit computer parts to companies in the Southern District
- From at least 2007 until late 2017, the Chinese national directed shipments of counterfeit computer-networking equipment to a retailer in Texas
- Defendant sold counterfeit networking products through several business entities and used corporate and personal aliases to evade detection
- The defendant also attempted to conceal the activity by sending and receiving payments using accounts that were not publicly connected to the business entities
- He and his customers agreed to mislabel packages, break up shipments into separate components, alter destination addresses, and use multiple forwarding companies based in the United States

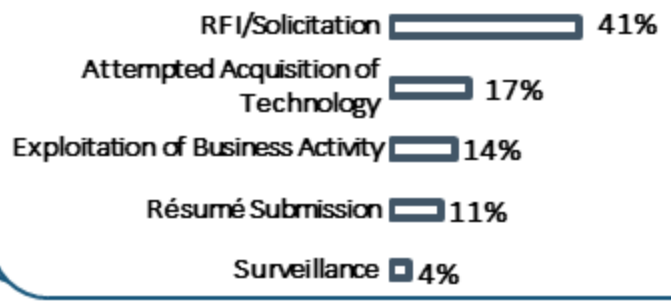
Takeaway: Counterfeit parts are often substandard and may fail under stress. In addition, counterfeit computer parts could include malicious coding that may allow foreign adversaries the ability to collect DoD data or cause systems to fail.

https://www.justice.gov/opa/pr/Chinese-national-sentenced-prison-selling-counterfeit-computer-parts

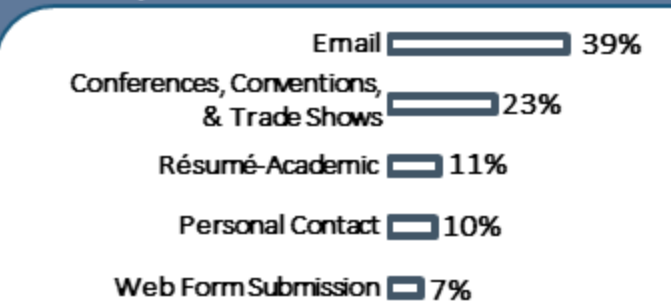
Targeting of Technologies – Armament & Survivability

Targeting of Armament & Survivability FY14 – FY18

Top Five Methods of Operation FY18



Top Five Methods of Contact FY18



- Targeting of Armament & Survivability in FY18
  - Fourth most targeted technology in FY18
  - 3% increase in reported targeting from FY17
  - East Asia & the Pacific accounted for 31% of the incidents
    - Near East 23%
    - South & Central Asia 13%
  - Commercial entities were the most common affiliation - identified in 42% of reports
  - RFI/solicitation using an email to contact the target was the most common MO + MC combination used in 22% of incidents in FY18

Top Targeted Armament & Survivability Systems

Missiles
- Terminal High Altitude Area Defense

X-Ray Detection

Launchers (Missile, Torpedo, Rocket)

Automatic & Semi-Automatic Weapons

Electronic Warfare

Mine/Explosive Detection

Gun Rounds

Targeting of Armament & Survivability - Case Study

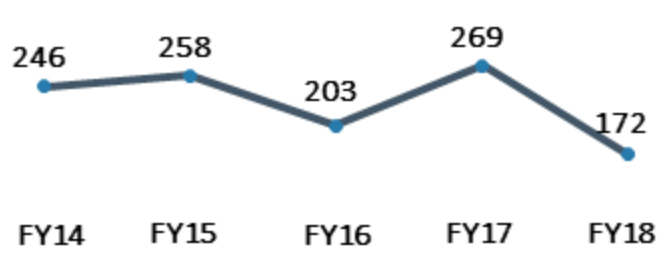
- According to DoJ, in December 2017, an Italian national and member of the Italian armed services pled guilty to exporting and attempting to export military technology
- According to court filings, between June 2013 and May 2017, the defendant illegally exported and attempted to export night vision goggles and assault rifle components designated as defense articles on the U.S. Munitions list
- Records show along with the night vision equipment and assault rifle components, the defendant also purchased pieces of body armor
- Defendant purchased export control devices from U.S.-based manufacturers or distributors via Internet-based marketplaces
- Defendant directed sellers to ship products to freight forwarders in the United States.
- Defendant made false statements to the freight forwarders about the contents in order to export the packages to Italy without required licenses

Takeaway: Shipping to freight companies can be used to obfuscate the actual location and identity of the end user.

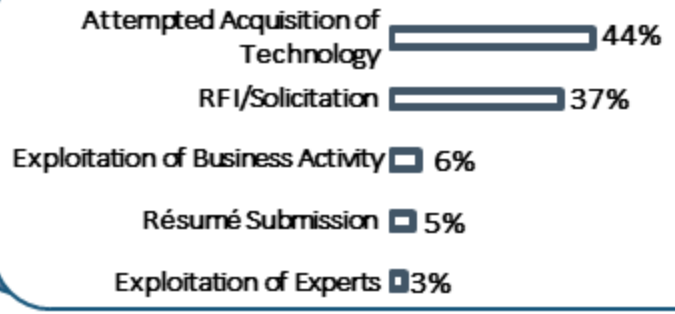
https://www.justice.gov/usao-edny/pr/italian-national-sentenced-11-months-prison-illegally-exporting-and-attempting-export

Targeting of Technologies – Optics

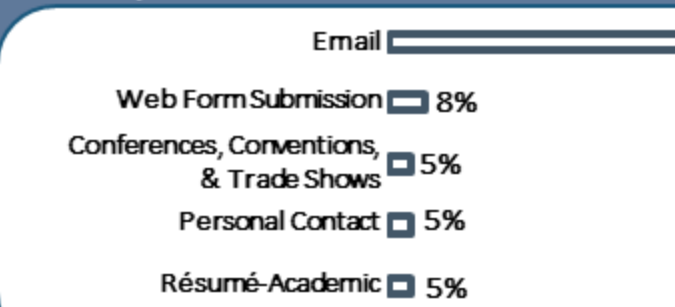
Targeting of Optics FY14 – FY18



Top Five Methods of Operation FY18



Top Five Methods of Contact FY18



- Targeting of Optics in FY18
  - Fifth most targeted technology in FY18
    - First year in top five since FY12 when optics was part of the lasers, optics, & sensors category
  - 36% decrease in reported targeting from FY17
  - East Asia & the Pacific accounted for 37% of the incidents
    - South & Central Asia 27%
    - Europe & Eurasia 13%
  - Commercial entities were the most common affiliation - identified in 61% of reports
  - Attempted acquisition of technology sent via email was the most common MO + MC combination used in 41% of incidents in FY18

Top Targeted Armament & Survivability Systems

Night Vision
- Panoramic Night Vision Goggles

Cameras

Mirrors

Wave Optics Modeling & Analysis

Lenses

Reflective Coatings

Holograms & Holographic Technology

Targeting of Optics - Case Study

- In August 2018, the District Court of Seattle sentenced a Canadian national for conspiracy to export restricted goods and technology to Iran
- According to records filed with the court, between 2011 and 2017 the defendant and co-conspirators attempted and exported dual use technology to Iran
- Specific items included two types of thermal imaging cameras: a thin film measurement system and inertial guidance systems testing equipment
  - The thermal imaging cameras can be used in commercial security systems and on UAVs and military drones
  - The thin film measurement system measures liquid coatings and parts used in cell phones and missiles
- Conspirators falsified shipping documents and deceived manufacturers by claiming goods were being shipped to Turkey and Portugal, while knowing the true destination was Iran

Takeaway: Claiming equipment is bound for a country with positive trade relations is a common method to obtain export-controlled technologies for entities in countries under export restrictions.

https://www.justice.gov/usao-wdwa/pr/canadian-sentenced-3-years-prison-conspiracy-export-restricted-goods-and-technology

Targeting of Technologies – 6 through 10 Most Targeted

Radars

- Targeted Systems: Ground penetrating radar; through-the-wall radar; target acquisition; electronically steered

Software

- Targeted Software: Modeling and simulation; artificial intelligence; information & cyber security; software & algorithms; system development kits

Space Systems

- Targeted Systems: Satellites & satellite buses; space broadcast systems; space launch vehicle/systems; space mission control systems

Marine Systems

- Targeted Systems: Autonomous underwater vehicles; submarines & designs; combat ships & landing vessels; unmanned surface vessels; deep seas submersibles

Energy Systems

- Targeted Systems: Gas turbine engines; propellants; rocket engines; turbo fan engines; ocean power technologies; energy systems components; generators

Audience Poll Question #2

- In FY 18 Reporting, which region accounted for the highest volume of targeting according to Suspicious Contact Reporting (SCRs)?

- A. Near East
- B. Europe and Eurasia
- C. Africa
- D. South And Central Asia
- E. East Asia and the Pacific

Targeting by Geographic Region

East Asia & the Pacific

Top 10 Targeted Technologies

Electronics	12%
Aeronautic Systems	6%
C4	4%
Armament & Survivability	4%
Optics	2%
Radars	2%
Energy Systems	2%
Sensors (Acoustic)	2%
Marine Systems	2%
Software	2%

Top 5 Methods of Operation

Attempted Acquisition of Technology	21%
Résumé Submission	18%
RFI/Solicitation	13%
Exploitation of Business Activity	13%
Exploitation of Supply Chain	11%

Top 5 Methods of Contact

Email	49%
Résumé - Academic	12%
Foreign Visit	9%
Web Form Submission	7%
Conferences, Conventions, & Trade Shows	6%

Most Common MO + MC Combinations

Attempted Acquisition of Technology + Email	14%
Résumé Submission + Résumé - Academic	12%

- East Asia and the Pacific collectors remained the most active in FY18, accounting for 40% of reporting from cleared industry
- Volume of incidents related to this region increased by 20% over FY17
- Most frequently reported as targeting electronics, specifically – integrated circuits, radiation hardened integrated circuit, and digital signal processors
- Targeting of aeronautic systems included – UAV, fixed wing aircraft, and rotary wing aircraft

East Asia & the Pacific - Case Study

- In September 2018, DoJ indicted Fujian Jinhua Integrated Circuits, Co., Ltd (Jinhua), a state-owned Chinese company; United Microelectronics Corporation (UMC), a Taiwanese company; and three Taiwan individuals for alleged economic espionage. The USG alleged the defendants schemed to steal dynamic random access memory (DRAM) trade secrets from a U.S. company. According to DoJ, prior to the events detailed in the indictment China did not possess DRAM technology
- The indictment alleged the president of a Taiwan subsidiary of the U.S. company responsible for manufacturing one of the company's DRAM chips resigned from the company and began working at UMC
- At UMC he developed a cooperation agreement with Jinhua. The agreement included UMC transferring DRAM technology to Jinhua to mass produce DRAM chips
- He then recruited employees at the U.S. company's Taiwan subsidiary. These employees stole and provided to UMC trade secrets relating to DRAM design and manufacture

Takeaway: This case study is an example of exploitation of insider access. The two employees took advantage of their trusted access to information to steal it and provide it to their new company. It also emphasizes the need for robust network security protocols and limitation of removable/external storage devices being allowed on networks. Moreover, this case highlights the risk involved in joint ventures, business relationships, and overseas production.

https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage

Targeting by Geographic Region

Near East

Top 10 Targeted Technologies

Aeronautic Systems	9%
Armament & Survivability	9%
C4	7%
Radars	4%
Electronics	3%
Energy Systems	3%
Software	3%
Ground Systems	3%
Optics	3%
Space Systems	2%

Top 5 Methods of Operation

Résumé Submission	33%
RFI/Solicitation	25%
Attempted Acquisition of Technology	17%
Exploitation of Business Activity	15%
Exploitation of Relationship	3%

Top 5 Methods of Contact

Email	36%
Résumé - Academic	20%
Résumé - Professional	12%
Conferences, Conventions, & Trade Shows	8%
Foreign Visit	8%

Most Common MO + MC Combinations

Résumé Submission + Résumé - Academic	20%
Attempted Acquisition of Technology + Email	16%

- DCSA identified entities from the Near East in 13% of cleared industry reporting in FY18
- Reporting associated to entities from the Near East dropped by 37% in FY18
- Commercial collectors are becoming more prominent in incidents originating from this region
- Targeted aeronautic systems included: UAV detection and counter UAV systems, flight simulator software and training, and rotary wing aircraft
- Targeted armament and survivability systems included: automatic and semi-automatic weapons, X-ray detection systems, electronic warfare, and missiles

Near East - Case Study

- In March 2018, DoJ, U.S. Attorney for Central District of California, filed charges against USPER3 relating to a plan to send export-controlled computer servers to Iran, a Near East region country. The indictment accused the USPER3 and a company USPER3 owned and operated with violating the International Emergency Economic Powers Act (IEEPA)
- The USPER3 is accused of purchasing computer servers and sending them to Iran without obtaining licenses from the USG as required by IEEPA. These servers are dual use, with commercial and military applications
- The USPER3 allegedly listed false destinations when dealing with the manufacturer. The USPER3 identified Kosovo and Slovenia as the destinations for the servers. However, the U.S. Attorney asserts USPER3 knew the servers were actually destined for Bank Mellot, a financial institution in Iran

Takeaway: Falsified end user or destination is a common tactic used to obtain export-controlled technology. Using U.S. persons or U.S. companies as a broker to purchase the items also helps obfuscate the destination and the end user, and lends an appearance of legitimacy. In addition, when acquiring dual use technologies, the collector might also misrepresent the end use of the targeted items.

https://www.justice.gov/usao-cdca/pr/dana-point-man-charged-scheme-send-export-controlled-computer-servers-iran

Targeting by Geographic Region

Europe & Eurasia

Top 10 Targeted Technologies

Aeronautic Systems	10%
Electronics	10%
C4	7%
Armament & Survivability	5%
Software	5%
Space Systems	3%
Optics	3%
Positioning, Navigation, & Time	3%
Radars	2%
Marine Systems	2%

Top 5 Methods of Operation

RFI/Solicitation	27%
Attempted Acquisition of Technology	25%
Exploitation of Business Activity	13%
Résumé Submission	11%
Exploitation of Cyber Operations	9%

Top 5 Methods of Contact

Email	48%
Résumé - Professional	10%
Conferences, Conventions, & Trade Shows	9%
Cyber Operations	6%
Personal Contact	6%

Most Common MO + MC Combinations

Attempted Acquisition of Technology + Email	19%
RFI/Solicitation + Email	16%

- DCSA identified entities from the Europe & Eurasia region in 12% of cleared industry reporting in FY18
- Reporting associated to entities from Europe & Eurasia decreased by 8% in FY18
- Targeted aeronautic systems included: UAV detection and counter UAV systems, flight simulator software and training
- Targeted electronics included: integrated circuits, radiation hardened integrated circuits, wafers

Targeting by Geographic Region

South & Central Asia

Top 10 Targeted Technologies

Electronics	20%
Aeronautic Systems	10%
Optics	7%
C4	7%
Armament & Survivability	6%
Radars	4%
Energy Systems	2%
Lasers	2%
Software	2%
Marine Systems	1%

Top 5 Methods of Operation

Attempted Acquisition of Technology	42%
RFI/Solicitation	28%
Résumé Submission	17%
Exploitation of Business Activity	4%
Exploitation of Cyber Operations	4%

Top 5 Methods of Contact

Email	66%
Résumé - Professional	9%
Résumé - Academic	7%
Web Form Submission	5%
Social Networking Services	3%

Most Common MO + MC Combinations

Attempted Acquisition of Technology + Email	37%
RFI/Solicitation + Email	24%

- DCSA identified entities from South & Central Asia region in 11% of cleared industry reporting in FY18
- Reporting associated to entities from South & Central Asia decreased by 13% in FY18
- DCSA identified electronics as the targeted technology in 20% of the incidents; 39% of these incidents targeted integrated circuits
- Targeted electronics included: integrated circuits, radiation hardened integrated circuits, field-programmable gate arrays

Targeting by Geographic Region

Western Hemisphere

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

- DCSA identified entities from the Western Hemisphere region in 8% of cleared industry reporting in FY18
- Reporting of entities from Western Hemisphere targeting technology decreased 8% from FY17
- Targeted aeronautic systems included: UAVs, flight simulator software and training, and airframes and structural components
- Collectors from this region used RFI/solicitation and exploitation of insider access as the most common MO

Africa

Top 5 Targeted Technologies	
Aeronautic Systems	15%
C4	13%
Electronics	8%
Armament & Survivability	7%
Ground Systems	4%

- DCSA identified entities from the Africa region in a little over 1% of cleared industry reporting in FY18
- Reporting of entities from Africa targeting technology increased by 32% over FY17
- Targeted aeronautic systems included: UAVs and fixed wing aircraft
- Targeted C4 components included: wide area surveillance systems, telecommunications devices, and identification friend/foe

Audience Poll Question #3

- What should you do with a suspicious email with an attachment or embedded link?

- A. Open it
- B. Ask a coworker to open it while you hide under the desk
- C. Throw away your computer- it's already too late
- D. Delete it immediately and slowly back away
- E. Report it!

Special Topics

Cyber Activity Targeting Cleared Industry

- Exploitation of cyber operations was the MO identified in 17% of FY18 reporting, the third most common MO
- Increased by 55% over FY17
- The specific actor was unidentified in 75% of incidents of exploitation of cyber operations
- The targeted technology is unknown in 91% of the incidents in FY18
- Most common MC associated with exploitation of cyber operations:
  - Phishing

    Phishing
    Spearphishing
    Whaling
  - Cyber Operation

    Network scanning and probing
    Web site exploitation
    Compromised credentials
    Brute force

Special Topics

China Technology Transfer

- On March 22, 2018, the White House released a Presidential Memorandum citing a U.S. Trade Representative's investigation, which supported four findings, including three related to technology and data theft:
  - *"China uses foreign ownership restriction, including joint ventures requirements … and other investment restriction to require or pressure technology transfer from U.S. companies to Chinese Entities …*
  - *"China directs and facilitates the systemic investment in, and acquisition of U.S. companies and assets by Chinese companies to obtain cutting-edge technologies … to generate large scale technology transfer in industries deemed important by Chinese government industrial plans …*
  - *"China conducts and supports unauthorized intrusions into, and theft from, the computer networks of U.S. companies."*

"No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China,"
Christopher Wray, Director, FBI

Takeaway: Chinese targeting of cleared industry spans a wide array of methods and tactics, many of them cloaked in the legitimacy of conventional business activity. Technology transfer and intellectual property lost to Chinese entities impacts U.S. national and economic security.

https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/
https://www.justice.gov/opa/speech/file/1107256/download

Questions

Questions?

CDSE WANTS TO HEAR FROM YOU!

CDSE Counterintelligence POC:

Ed Kobeski

410-689-7842

EMAIL: Edwin.f.Kobeski.civ@mail.mil