Targeting U.S. Technologies

A Report of Foreign Targeting of Cleared Industry

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

2019

DCSA Counterintelligence Directorate, Production Branch prepared this product. For questions, or to provide feedback please email us at: DCSA.CI.Production@mail.mil

Table of Contents

PREFACE

The transition of the Defense Security Service into the Defense Counterintelligence and Security Agency (DCSA) has involved integration of new missions, including background investigations, and expansion of our security training enterprise. Even as we transition, we remain dedicated to securing the National Industrial Base (NIB) as part of our mission to strengthen national security and provide risk management services. As such, DCSA continues to work with cleared industry to detect and deter foreign entities' attempts to illicitly acquire classified and sensitive information and technology.

Securing the NIB is more relevant and more challenging than ever as our nation faces the most significant, diverse, and resourceful foreign intelligence threat it has ever experienced. The DCSA transition goes beyond new missions to include the development and implementation of new methodologies to secure the NIB. DCSA's new methodology is data-driven, risk informed, and partner-enabled. DCSA continues to move toward National Industrial Security Program compliance coupled with an asset-focused and threat-driven oversight methodology.

In protecting assets — such as the technologies, information, and personnel at cleared facilities — it is important to identify the threats, determine vulnerabilities, and implement appropriate countermeasures. These factors are essential in developing and successfully applying tailored security plans to protect assets at cleared facilities.

DCSA's annual report, ***Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry,*** is a key resource that identifies and describes the threat foreign entities pose to critical technologies and classified information in the hands of cleared industry. I encourage you to use this report as one tool in your risk management toolbox in determining strategies to mitigate risks to critical assets.

Charles S. Phalen, Jr.

Acting Director

Defense Counterintelligence and Security Agency

SECTION 1: BACKGROUND

Scope

During fiscal year 2018 (FY18), the approximately 13,000 cleared contractor facilities reported 6,026 incidents that the Defense Counterintelligence and Security Agency (DCSA) considered a suspicious contact report (SCR). An SCR is a report DCSA receives from cleared industry that contains indicators that are either likely, almost certain, or for which there is an even chance that an individual, regardless of nationality, attempted to obtain unauthorized access to sensitive or classified information and technology or compromise a cleared employee. These 6,026 reports are the basis for the numeric listing of foreign intelligence entities (FIE)[i] targeting of cleared industry. In addition, we include case studies and assessments of foreign entities targeting U.S. technologies based on publicly available sources to augment the data and provide examples of foreign collection targeting cleared industry. The primary source of these case studies is the Department of Justice press releases published following the unsealing of indictments or following adjudication of cases. In case studies based on indictments, these contain allegations that a defendant has committed a crime. These defendants are presumed to be innocent until and unless proven guilty in court. Although some of the actual incidents used in the case studies did not occur in FY18, the tactics described in the case studies remain relevant.

Assessing Foreign Intelligence Entity Threat to Cleared Industry

This product details and enumerates cleared industry's reporting of SCRs that represent potential FIE attempts to illicitly acquire U.S. technologies resident in cleared industry. As an unclassified product, this report does not provide a holistic view of the FIE threat to cleared industry. An SCR from cleared industry represents an incident where a cleared facility's security protocols identified a potential FIE attempt to collect on U.S. technology. Therefore, an SCR, along with demonstrating FIE targeting to some extent also represents a success for a facility's security posture and its Counterintelligence (CI) awareness and reporting regimen. DCSA cannot estimate in this forum the volume or targets of FIE activity that go unnoticed or unreported by cleared industry. DCSA annually produces a companion report at the classified level — *Targeting U.S. Technologies: An Assessment of Threats to Cleared Industry*.

Counterintelligence Awareness and Training

DCSA Counterintelligence Directorate has unclassified outreach products that provide information on CI topics. They are available on the DCSA homepage: https://www.dcsa.mil/

The Center for Development of Security Excellence (CDSE) provides diverse security courses and products to Department of Defense (DoD) personnel, DoD contractors, employees of other federal agencies, and selected foreign governments. CDSE content and course information is available at their web site: https://www.cdse.edu/

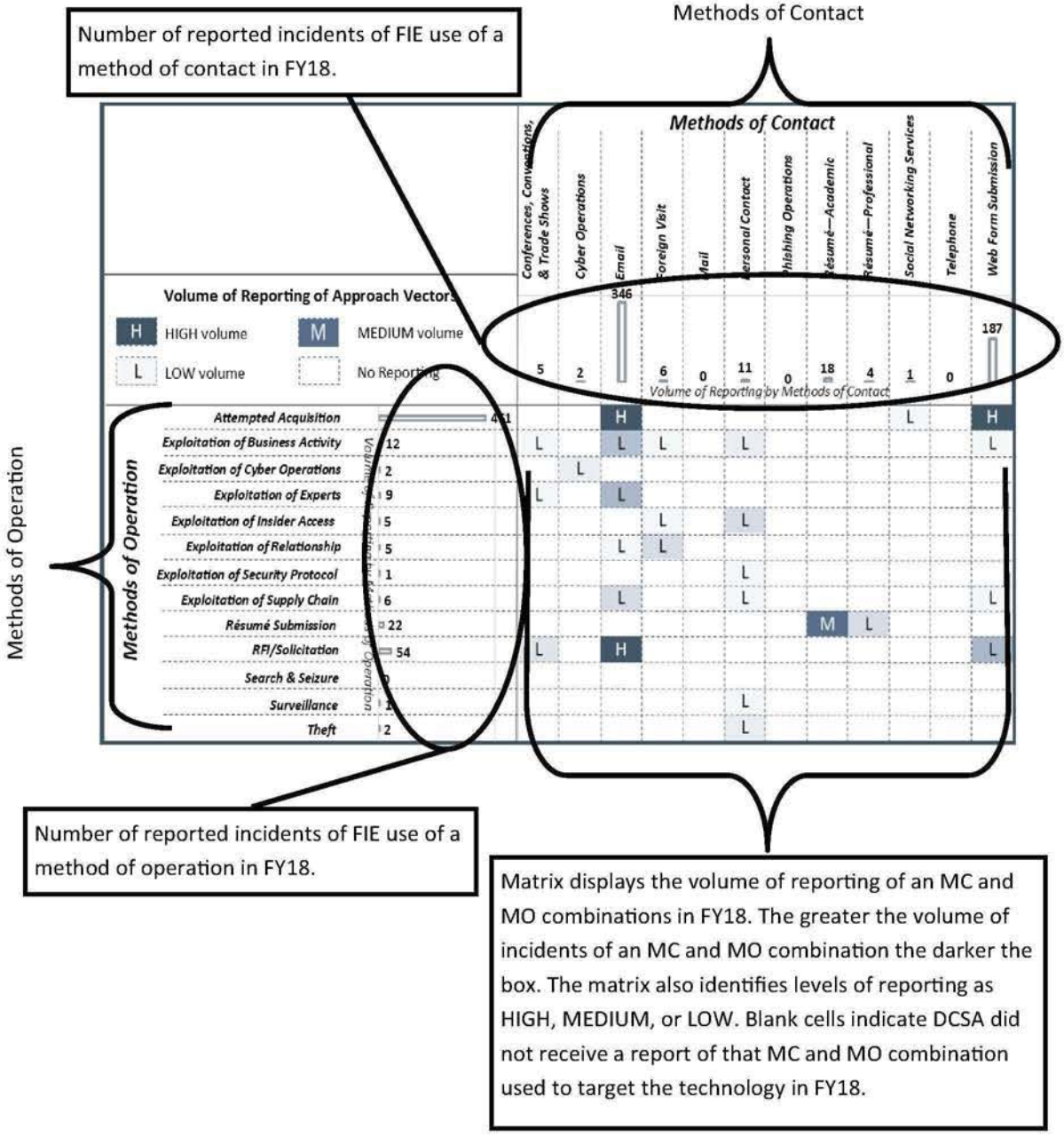
i. Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

Displaying FIE Methods of Targeting Technology in Cleared Industry

Foreign entities use approach vectors that include a method of operation (MO) paired with a method of contact (MC) to attempt to illicitly obtain access to information and technology. The graphic below is an example of a matrix of FIE approaches, commonly referred to as the MCMO or 12x13 matrix (12 MCs x 13 MOs). This matrix depicts the volume of reported incidents of targeting of a specific technology in FY18. It displays the MCs and MOs used in incidents reported by cleared industry in FY18, which were likely attempts to illicitly gain access to technology, information, or cleared employees at the facility.

As previously stated in the Assessing Foreign Intelligence Entity Threat to Cleared Industry section above, the data used in this report to create these matrices does not display the full nature of the FIE threat to the information and technologies resident in cleared industry. We base this matrix on incidents when a facility's security protocols and employee CI awareness identified and reported a suspicious incident. The volume of incidents that go unnoticed or unreported by cleared industry is unknown.

In this report we use an enhanced MCMO or 12x13 matrix (see below) to characterize the reporting of foreign targeting of the five most targeted technologies.



SECTION 2: EXECUTIVE SUMMARY

In FY18, DCSA received nearly 50,000 reports of suspicious activities from cleared facilities operating as part of the National Industrial Security Program (NISP). Of these, DCSA CI Special Agents and Intelligence Analysts reviewed and identified 6,026 as incidents of CI concern (considered SCRs) that are likely incidents of a foreign entity attempting to illicitly obtain information or technology resident in cleared industry, or an attempt to compromise a cleared employee. These reports are the basis for ranking FIE targeting of U.S. technologies resident in cleared industry.

Top targeted technologies based on cleared industry reporting in FY18 and the percentage of reports by Industrial Base Technology List (IBTL) category.

1.	Electronics	9%
2.	Aeronautic Systems	7%
3.	Command, Control, Communications, and Computers (C4)	5%
4.	Armament & Survivability	5%
5.	Optics	3%
6.	Radars	2%
7.	Software	2%
8.	Space Systems	2%
9.	Marine Systems	2%
10.	Energy Systems	2%
11.	Positioning, Navigation, & Time	1%
12.	Sensors (Acoustic)	1%
13.	Materials: Raw & Processed	1%
14.	Ground Systems	1%
15.	Lasers	1%
16.	Biological	1%
17.	Directed Energy	1%
18.	Agriculture	1%

Other technologies targeted in less than 1 percent of cleared industry reporting each: Manufacturing Equipment & Manufacturing Process; Nuclear; Chemical; Medical; Quantum Systems; Nanotechnology; Energetic Materials; Cognitive Neuroscience; Signature Control.

Technologies with no reported targeting in FY18: Computational Modeling of Human Behavior, and Synthetic Biology.

Key Findings from FY18 Cleared Industry Reporting

- The number of reports assessed to be a suspicious contact increased by 3 percent over FY17
- The top four most targeted technologies in FY18 were in the top five most targeted technologies in FY17
- Optics was the fifth most targeted technology; previously it had not been one of the top five
- East Asia and the Pacific was the most commonly identified origin of incidents reported by cleared industry
- Attempted acquisition of technology was the most common MO
- Exploitation of cyber operations increased by 55 percent in FY18
- Email was the most common MC used in 41 percent of the reported incidents
- Phishing operation was the second most common MC used in 9 percent of the incidents
- Cleared industry reporting also noted foreign collection targeting services provided by cleared industry

Overview

Overall reporting that DCSA categorized as a suspicious contact report increased by 3 percent in FY18. Reports where the specific technology or Industrial Base Technology List (IBTL) could not be identified amounted to 49 percent of the reporting. This is up from 40 percent in FY17. Electronics was the IBTL category that experienced the greatest increase in volume of reported targeting. Reported targeting of electronics increased by 73 percent in FY18.

Electronics was the most targeted technology in FY18. Integrated circuits was the most targeted category of electronics.

Aeronautics systems dropped from being the most targeted in FY17 to second most targeted in FY18. Aeronautics systems experienced a 15 percent decrease in targeting in FY18. Actors targeting aeronautic systems most commonly sought Unmanned Aerial Vehicles (UAV) technology and information.

Along with UAVs and drones, unmanned or independent systems were commonly targeted across technology sectors. Artificial intelligence was a highly targeted software. In marine systems, FIE targeted autonomous underwater vehicles and unmanned surface vessels technology. Similarly, unmanned ground systems technology was also targeted.

In FY18, cleared industry identified entities from East Asia and the Pacific region in more than 40 percent of reporting. The volume of reporting DCSA associated to entities in East Asia and the Pacific increased by 20 percent in FY18. Entities from this region were identified in over half of the incidents targeting electronics and a third of the incidents targeting aeronautic systems.

China, an East Asia and the Pacific region country, has been cited in multiple U.S. Government investigations and initiatives as having policies for technology transfer and intellectual property theft that pose a threat to U.S. economic security.

The Near East remained the second most active collector in FY18; even with a 37 percent decrease in the number or reports associated to entities from this region. Entities from this region most commonly targeted aeronautic systems and armament and survivability technologies.

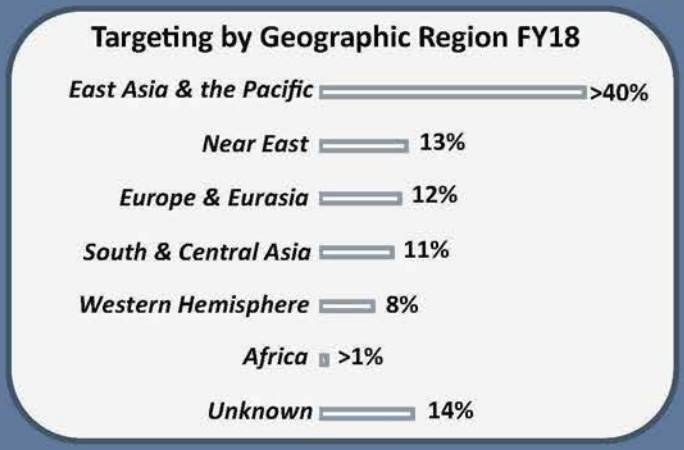
Cleared industry reporting in FY18 identified commercial entities as the collector in 42 percent of all reports. These entities used attempted acquisition of technology MO in approximately 35 percent of reported collection attempts. In addition, these entities relied heavily on email as the MC, using email in nearly 72 percent of these attempts.

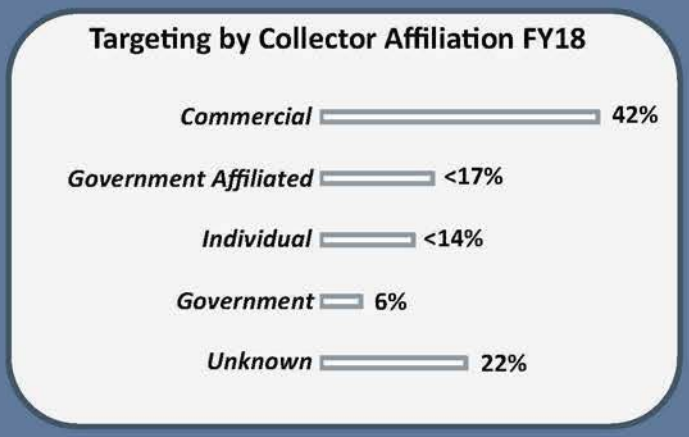
FIE applied attempted acquisition of technology, request for information (RFI)/solicitation, or exploitation of cyber operations in 54 percent of incidents in FY18. Most of these attempts were accomplished remotely via email and web form submission, not requiring the collector to have direct contact with the target or even be in the United States.

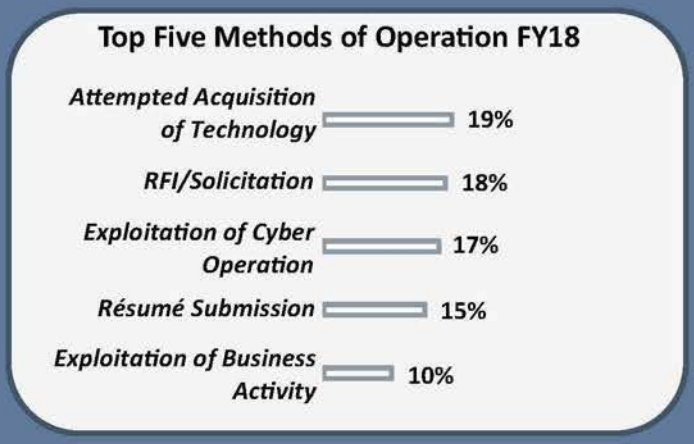
Exploitation of cyber activity increased by 55 percent in FY18. Although in overall data it was one of the top MOs the origin of the incident and the specific targeted technology are often unknown.

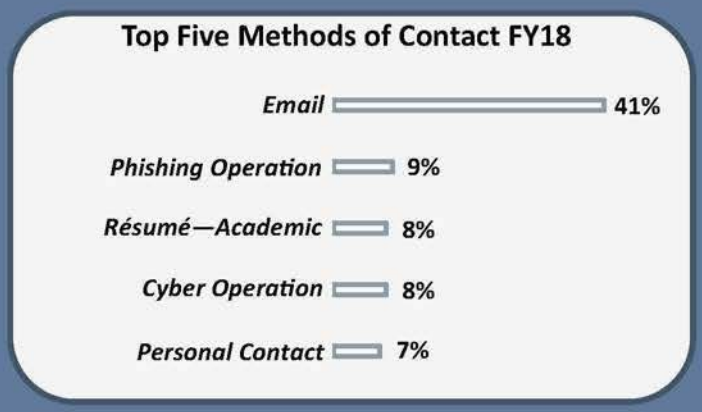
Email was overwhelmingly the most common MC used in FY18 by FIE targeting cleared industry. Cleared industry cited email in 41 percent of the reports. This does not include the 9 percent of FY18 reporting which listed the MC as phishing operation, which is an attempt to send malicious code via an email. Combining email and phishing operation, cleared industry received half of all incidents via email.

FIE use approach vectors in their collection attempts. An approach vector includes an MO, the method the actor uses to obtain the information, with an MC, the method the actor uses to contact the target. The most common approach vector in FY18 was attempted acquisition of technology sent via email.







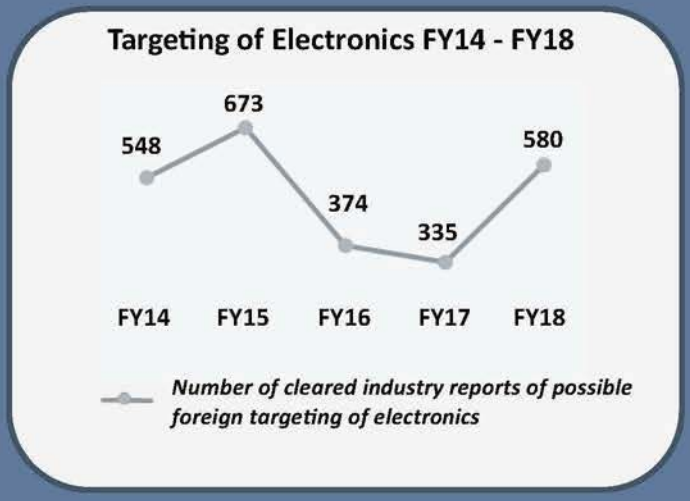


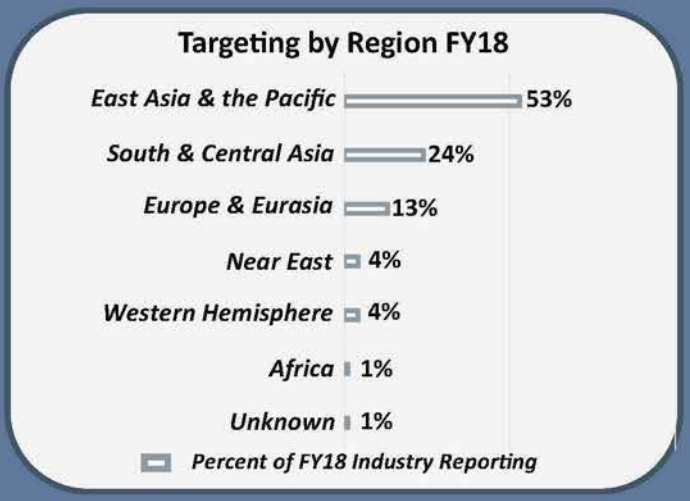
Percent of FY18 Industry Reporting

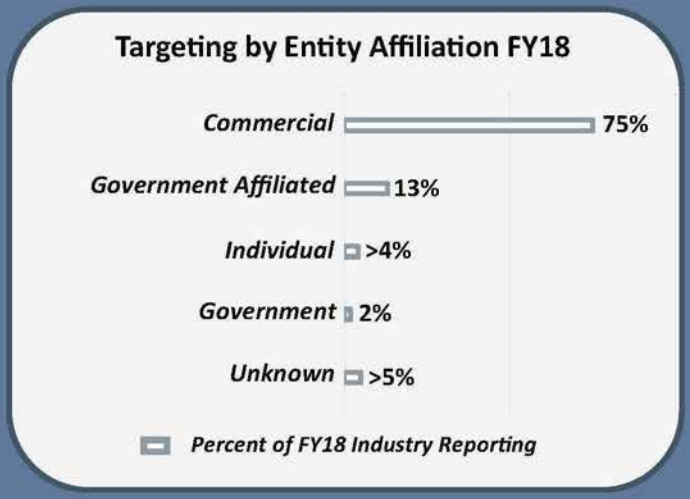
SECTION 3: TARGETING OF TECHNOLOGIES

REPORTED FOREIGN TARGETING OF 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. Electronics includes, but is not limited to, integrated circuits, programmable memory, and wafers.







Key Findings from FY18 Cleared Industry Reporting

- Electronics was the most targeted technology category in FY18
- Reported targeting of electronics increased by 73 percent over FY17
- East Asia and the Pacific region was the origin of most reported targeting of electronics
- Attempted acquisition of technology was the most common MO and email was the most common MC used to contact industry in attempts to target electronics

Overview

For each of the past 7 years, electronics has been one of the top three targeted technologies based on cleared industry reporting of suspicious contacts by foreign entities. Integrated circuits, primarily monolithic microwave integrated circuits, were the most targeted subcomponents in FY18.

In FY18, cleared industry reporting identified entities from East Asia and the Pacific region in over half of the incidents involving electronics. Reported incidents of targeting of electronics by entities from the East Asia and the Pacific region increased by 192 percent in FY18 compared to FY17. Electronics has been the top targeted technology by this region in 4 of the past 5 years. In FY18, their targeting included integrated circuits, radiation hardened (RADHARD) integrated circuits, digital signal processors, and circuit boards.

South and Central Asia entities were the second most active collectors targeting electronics. Entities from this region targeted integrated circuits, RADHARD, and field programmable gate arrays (FPGA). Entities from Europe and Eurasia were the third most active and targeted integrated circuits, FPGAs, and wafers.

Cleared industry identified commercial entities in three quarters of the incidents involving electronics. Commercial was the most common affiliation targeting electronics from all six of the geographic regions.

In FY18, entities targeting electronics used the attempted acquisition of technology MO in 79 percent of the reported incidents. Email was the most common MC, used in 60 percent of the incidents.

Takeaway: Cleared facilities developing or applying leading edge and legacy electronics technologies are reporting incidents of foreign entities targeting electronics in a greater volume than any other technology category. Integrated circuits, especially with special use properties such as radiation hardening, are highly sought after. The electronics sector is also vulnerable to counterfeit and substandard parts entering the supply chain.

Foreign Collection Methodology Targeting Electronics

Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting electronics in FY18.

The most commonly reported approach vector associated to electronics in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 283 times in FY18. The next most commonly reported approach was **attempted acquisition** via **web form submission.**

Volume of Reporting of Approach Vectors

H HIGH volume | M MEDIUM volume | L LOW volume | No Reporting

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions,	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
	Volume of Reporting by Methods of Contact	5	2	346	6	0	11	0	18	4	1	0	187
Attempted Acquisition	461			H							L		H
Exploitation of Business Activity	12	L		L	L		L						L
Exploitation of Cyber Operations	2		L										
Exploitation of Experts	9	L		L									
Exploitation of Insider Access	5				L		L						
Exploitation of Relationship	5			L	L								
Exploitation of Security Protocol	1						L						
Exploitation of Supply Chain	6			L			L						L
Résumé Submission	22								M	L			
RFI/Solicitation	54	L		H									L
Search & Seizure	0												
Surveillance	1						L						
Theft	2						L						

Top Targeted Electronics Subcomponents

Integrated Circuits
- Monolithic Microwave Integrated Circuits (MMIC)

Radiation Hardened Integrated Circuits

Field Programmable Gate Arrays

Digital Signal Processors

Circuit Boards

Vacuum Tubes

Wafers

Targeting Electronics Case Study

Indicted in 2018, an electrical engineer was convicted in 2019 of conspiring to illegally export MMICs with commercial and military applications to China

- U.S. Person (USPER1) conspired with USPER2 to gain illegal access to a protected computer at a U.S. Company
- USPER1 was the president of a Chinese company placed on the Commerce Department's Entity List in 2014
- USPER2 created an account on the targeted U.S. company's web portal posing as a domestic customer seeking to obtain MMICs for use in the United States
- USPER1 gained access to the company's web portal using USPER2's account

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.

Source: U.S. Department of Justice, U.S. Attorney's Office, Central District of California, https://www.justice.gov/usao-cdca/pr/electrical-engineer-convicted-conspiring-illegally-export-china-semiconductor-chips

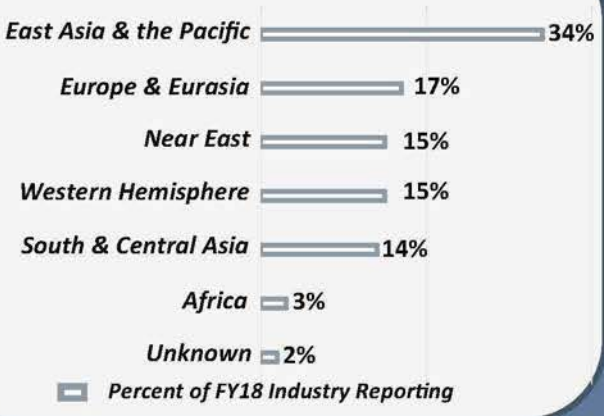
REPORTED FOREIGN TARGETING OF AERONAUTIC SYSTEMS

Aeronautic systems include combat and non-combat air vehicle design and capabilities. This category does not include armament and survivability, C4, and intelligence, reconnaissance, and surveillance (ISR) technologies that may be added to aeronautic systems for a specific combat or non-combat role. Aeronautic systems includes, but is not limited to, fixed and rotary wing aircraft and design, UAV, and airframes.

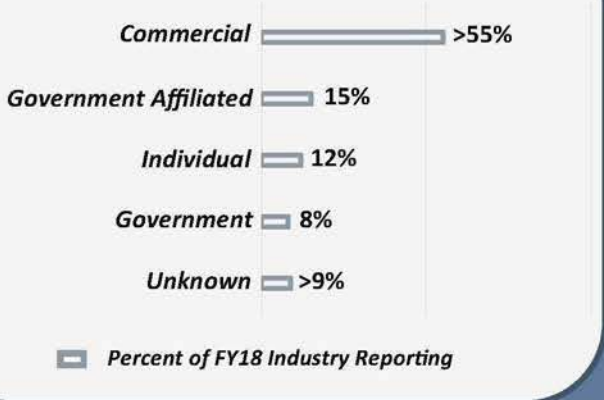
Targeting of Aeronautic Systems FY14 - FY18

Number of cleared industry reports of possible foreign targeting of aeronautic systems

Targeting by Region FY18



Targeting by Entity Affiliation FY18



Key Findings from FY18 Cleared Industry Reporting

- Aeronautic systems was the second most targeted technology category in FY18
- Reported targeting of aeronautic systems decreased by 15% from FY17
- East Asia and the Pacific region was the origin of most reported targeting of aeronautic systems
- Attempted acquisition of technology was the most common MO and email was the most common MC used to contact industry in attempts to target aeronautic systems

Overview

For each of the past 6 years, aeronautic systems has been one of the top three targeted technologies based on cleared industry reporting of suspicious contacts by foreign entities. Unmanned aerial vehicles and drones, notably counter-drone/ anti-drone products, were the most targeted aeronautic systems technologies in FY18.

In FY18, cleared industry reporting identified entities from East Asia and the Pacific region in over a third of the incidents involving aeronautic systems. Reported incidents of targeting of aeronautic systems by entities from the East Asia and the Pacific region decreased by 8 percent in FY18 compared to FY17. Entities from this region targeted UAV and drone technologies commonly seeking UAV transponder or counter-UAV technologies.

Europe and Eurasia entities were the second most active collectors targeting aeronautic systems. Entities from this region also targeted UAVs and drones, as well as fixed wing aircraft technologies. Entities from the Near East and Western Hemisphere regions were equally active collectors of aeronautic systems technologies in FY18.

Cleared industry identified commercial entities in over half of the incidents involving aeronautic systems. Commercial was the most common affiliation targeting aeronautic systems from all six of the geographic regions.

In FY18, entities targeting aeronautic systems used the attempted acquisition of technology and the RFI/solicitation MO each in 32 percent of the reported incidents. Email was the most common MC, used in 58 percent of the incidents.

Takeaway: The United States is a leader in this technology field and will remain a target as other countries plan to develop peer capabilities. In addition, aeronautic systems technology is vital in developing force projection, reconnaissance and surveillance, and air dominance capabilities.

Foreign Collection Methodology Targeting Aeronautic Systems

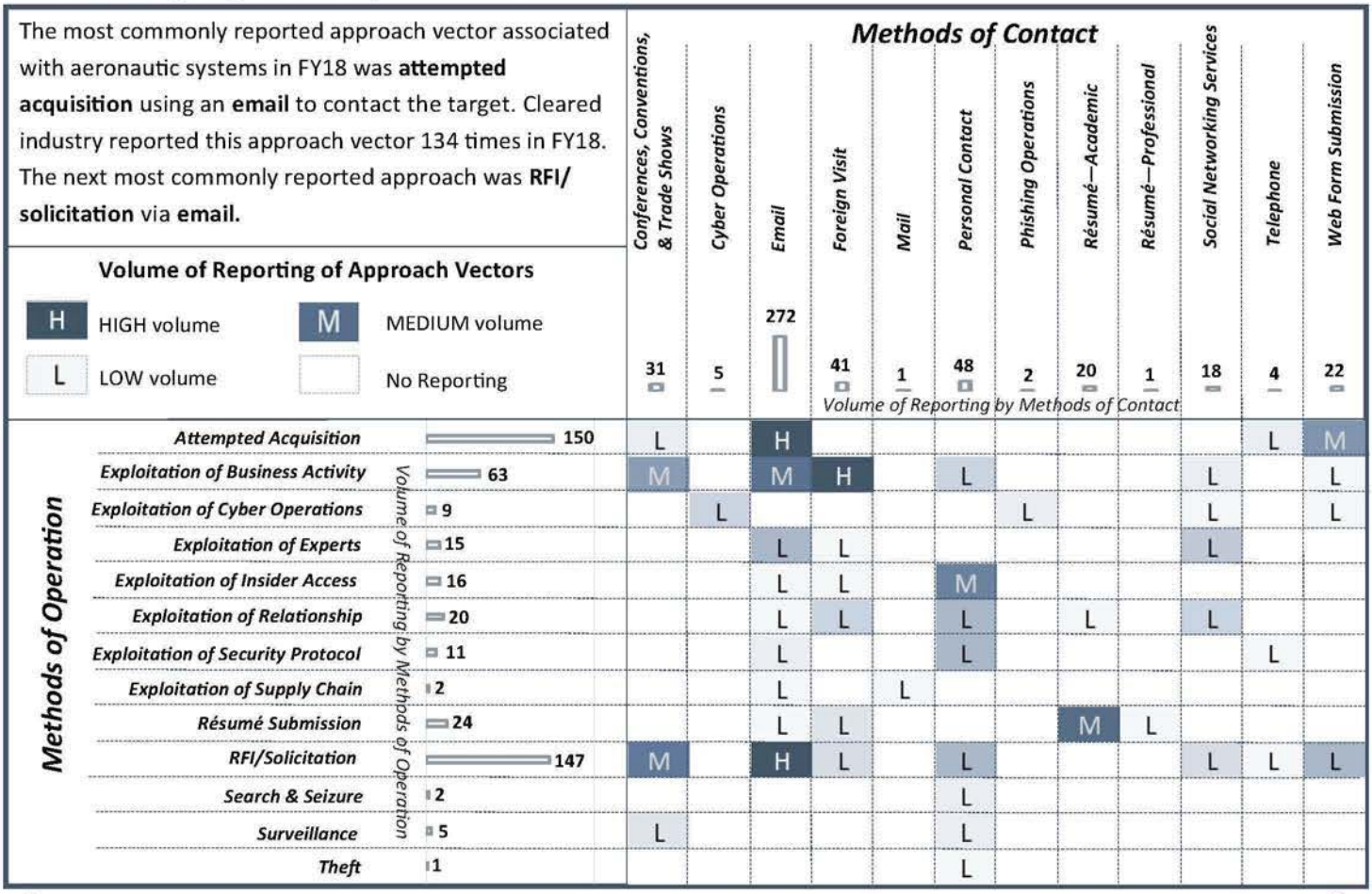
Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting aeronautic systems in FY18.

The most commonly reported approach vector associated with aeronautic systems in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 134 times in FY18. The next most commonly reported approach was **RFI/ solicitation** via **email.**

Volume of Reporting of Approach Vectors

H HIGH volume M MEDIUM volume

L LOW volume No Reporting



Top Targeted Aeronautic Systems Subcomponents

UAVs & Drones
- Counter-drone/Anti-drone Products

Fixed Wing Aircraft

Airframes & Structural Components

Flight Simulator Software & Training

Rotary Wing Aircraft

Other Fixed Wing Aircraft (Cargo & Transport)

Avionics

Targeting Aeronautic Systems Case Study

In March 2019, the U.S. District Court for the District of Columbia sentenced an Australian national for shipping aircraft parts to an Iranian company in violation of U.S. Embargo

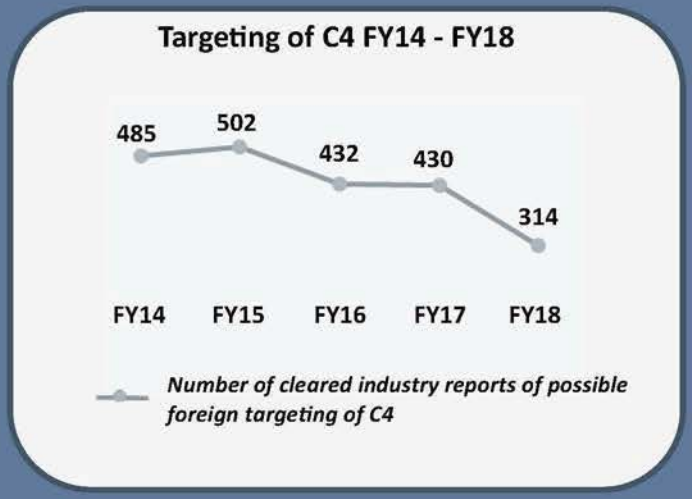
- Australia extradited the defendant to the United States in 2018
- The defendant solicited purchase orders and business for the goods from a trading company in Iran
- The Iranian trading company also operated companies in Malaysia that acted as intermediaries
- The defendant placed orders for aircraft parts and other items that the Iranian company could not buy directly
- To further conceal the end user, when necessary the defendant used a U.S.-based broker to order the parts

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.

Source: U.S. Department of Justice, Office of Public Affairs, https://www.justice.gov/opa/pr/australian-national-sentenced-prison-term-exporting-electronics-iran

REPORTED FOREIGN TARGETING OF COMMAND, CONTROL, COMMUNICATION, AND COMPUTERS

C4 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. C4 includes, but is not limited to, computers and central processing units (CPU), common data links, telecommunication devices, and antenna.



Key Findings from FY18 Cleared Industry Reporting

- Each year since FY13, C4 has been one of the top three targeted technology categories
- Reported foreign targeting of C4 technologies decreased by 27 percent in FY18 when compared to FY17
- Entities from East Asia and the Pacific region were the most active collectors of C4 technologies identified in cleared industry reporting in FY18
- These collectors contacted cleared industry via email in 63 percent of reported incidents

Overview

With the decrease of 27 percent in targeting in FY18, C4 dropped from the second to the third most commonly targeted technology as identified in cleared industry reporting. Industry reported fewer attempts to target highly sought after C4 components such as antennas, telecommunication devices, computers and CPUs, and common data links. Conversely, reporting identified an increase of incidents relating to wide area surveillance systems and wireless networks and technologies.

In FY18, cleared industry reporting identified entities from East Asia and the Pacific region in 32 percent of the incidents involving C4. Reported incidents of targeting of C4 by entities from the East Asia and the Pacific region increased by 1 percent in FY18 compared to FY17. Entities from this region targeted C4 components such as antennas, wireless networks and technologies, and wide area surveillance systems. In FY17, this region was the second most active region after the Near East region.

Europe and Eurasia entities were the second most active collectors targeting C4 in FY18. Entities from this region targeted telecommunication devices, wide area networks and technologies, computers, and CPUs.

In FY18, commercial entities were identified in over half of the reported incidents of targeting of C4 technologies. This was the most common affiliation targeting C4 from all geographic regions except the Western Hemisphere, in which individual was the most common collector affiliation.

In FY18, entities targeting C4 most frequently used the attempted acquisition of technology MO and email was the most frequently used MC.

Takeaway: C4 technologies are highly sought after by foreign collectors. Beyond targeting industry for sensitive technologies, foreign entities also attempt to provide counterfeit computer parts to U.S. companies that could subsequently enter DoD supply chains. Counterfeit parts could fail due to substandard quality or by design; either could negatively impact the warfighter.

Foreign Collection Methodology Targeting C4

Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting C4 in FY18.

The most commonly reported approach vector associated to C4 technologies in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 118 times in FY18. The next most commonly reported approach was **RFI/solicitation** via **email.**

Volume of Reporting of Approach Vectors

- H — HIGH volume
- M — MEDIUM volume
- L — LOW volume
- No Reporting

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions, & Trade Shows	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
	Volume of Reporting by Methods of Contact	13	4	198	7	0	39	1	21	11	4	2	14
Attempted Acquisition	131	L		H			L					L	L
Exploitation of Business Activity	17	L		L	L		L						
Exploitation of Cyber Operations	5		L					L					
Exploitation of Experts	10			L			L				L		
Exploitation of Insider Access	13				L		M						
Exploitation of Relationship	12	L		L			L				L		
Exploitation of Security Protocol	6				L		L						
Exploitation of Supply Chain	3			L									
Résumé Submission	32								M	M			
RFI/Solicitation	82	L		H			L				L		L
Search & Seizure	1						L						
Surveillance	2	L											
Theft	0												

Top Targeted C4 Subcomponents

- Antenna
- Wide Area Surveillance System
- Computers & CPUs
- Air & Missile Defense C2
- Telecommunication Devices
- Wireless Networks & Technologies
- Common Data Links
- Waveguide Components

Targeting 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

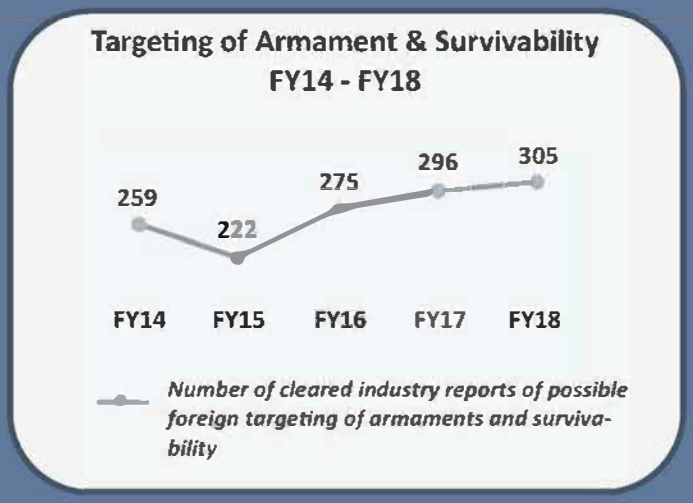
- From at least 2007 until late 2017, the Chinese national directed shipments of counterfeit computer-networking equipment to a retailer in Texas
- He sold counterfeit networking products through several business entities and used corporate and personal aliases to evade detection
- He and his customers agreed to mislabel packages, break up shipments into separate components, alter destination addresses, and use multiple forwarding companies based in the United States

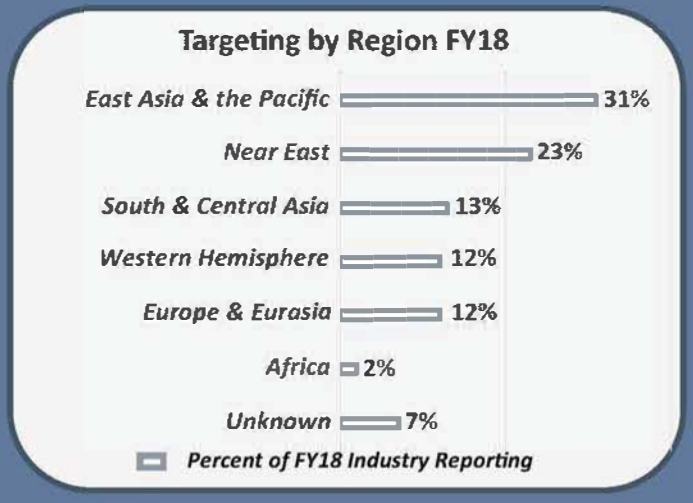
Takeaway: Counterfeit parts are often substandard and may fail under stress. In addition, computer parts could include malicious coding that may allow foreign adversaries the ability to collect DoD data or cause systems to fail.

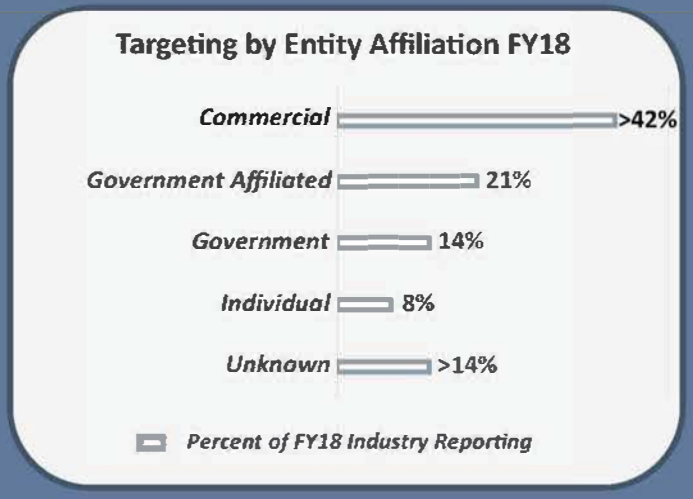
Source: U.S. Department of Justice, Office of Public Affairs, Press Release 19-130, https://www.justice.gov/opa/pr/Chinese-national-sentenced-prison-selling-counterfeit-computer-parts

REPORTED FOREIGN TARGETING OF ARMAMENT AND SURVIVABILITY

Armament and survivability: Armaments are the conventional munitions technologies designed to increase the lethality of ground, aeronautic, marine, and space systems. Conversely, survivability technologies provide various levels of protection for ground, aeronautic, marine, and space systems from armaments. Armament and survivability includes, but is not limited to, missiles, rockets, automatic and semi-automatic weapons, electromagnetic rail guns, artillery and mortar rounds, and body armor.







Key Findings from FY18 Cleared Industry Reporting

- Armament and survivability was the fourth most targeted technology category in FY18
- Reported targeting of armaments and survivability technology increased by 3 percent from FY17
- East Asia and the Pacific region was the origin of most reported targeting of armament and survivability
- RFI/solicitation was the most common MO and email was the most common MC used to contact industry in attempts to target armaments and survivability technologies

Overview

Every year since FY12, except for FY15, the number of incidents of targeting armaments and survivability has increased. FY18 is only the second year that armament and survivability has been one of the top five targeted technologies as reported by cleared industry. The most targeted technologies in this category included missiles, automatic and semi-automatic weapons, and electronic warfare.

Cleared industry reporting in FY18 identified entities from East Asia and the Pacific region in 31 percent of the incidents. The volume of reporting of East Asia and the Pacific entities targeting this technology increased by 8 percent in FY18. Entities from this region targeted missiles, automatic and semi-automatic weapons, and electronic warfare.

Entities from the Near East were the next most active and were identified in 23 percent of the reporting. Entities from this region most often targeted missiles, automatic and semi-automatic weapons, and missile warning systems.

Commercial entities were involved in over 42 percent of the incidents targeting this technology. In 55 percent of the incidents associated with commercial entities they used RFI/solicitation as the MO.

In FY18, 41 percent of suspicious contacts listed RFI/solicitation as the MO, the second most common MO was attempted acquisition of technology noted in 17 percent of reports. Email was noted as the MC in 39 percent of the incidents targeting this technology, followed by conferences, conventions, and trade shows, reported in 23 percent of the reports.

Takeaway: The United States is a leader in developing and applying armament and survivability technologies, which include weapon systems and protective technologies. Foreign adversaries that obtain sensitive information relating to these technologies can benefit from replicating U.S. capabilities and developing countermeasures to U.S. systems.

Foreign Collection Methodology Targeting Armament and Survivability

Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting armament and survivability in FY18.

The most commonly reported approach vector associated with armament and survivability technologies in FY18 was **RFI/solicitation** using an **email** to contact the target. Cleared industry reported this approach vector 68 times in FY18. The next most commonly reported approach was **attempted acquisition** via **email.**

Volume of Reporting of Approach Vectors

H HIGH volume | M MEDIUM volume | L LOW volume | No Reporting

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions, & Trade Shows	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
	Volume of Reporting by Methods of Contact	69	7	120	14	2	30	1	34	0	7	0	20
Attempted Acquisition	53	L		H									L
Exploitation of Business Activity	43	M		L	L		L						
Exploitation of Cyber Operations	8		L					L					
Exploitation of Experts	6			L							L		
Exploitation of Insider Access	9				L		L						
Exploitation of Relationship	7				L		L						
Exploitation of Security Protocol	5	L				L	L						
Exploitation of Supply Chain	2			L		L							
Résumé Submission	34								H				
RFI/Solicitation	124	H		H	L		L				L		M
Search & Seizure	1						L						
Surveillance	11	L					L						
Theft	2						L						

Top Targeted Armament & Survivability Subcomponents

Missiles
- Terminal High Altitude Area Defense (THAAD)

X-Ray Detection

Launchers (Missile, Torpedo, Rocket, etc.)

Automatic & Semi-Automatic Weapons

Electronic Warfare

Mine/Explosive Detection

Gun Rounds (anti-Armor, Armor Piercing, etc.)

Targeting Armament & Survivability Case Study

In December 2017, an Italian National pled guilty to exporting and attempting to export military technology

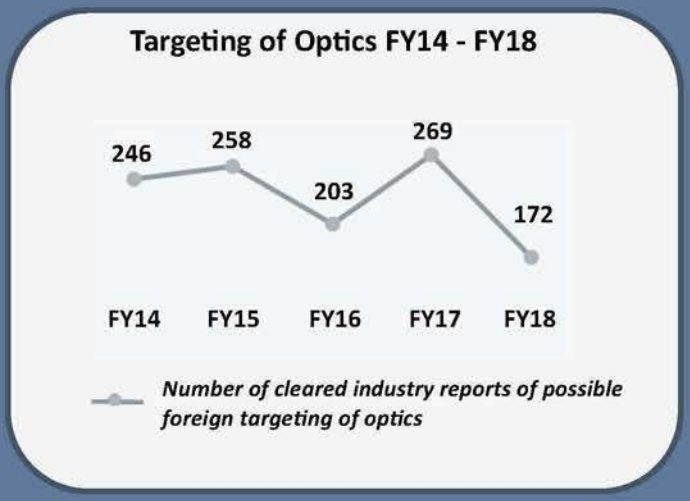
- According to court filings, between June 2013 and May 2017, the defendant illegally exported and attempted to export night vision goggles and assault rifle components
- Defendant purchased export control devices from U.S.-based manufacturers and distributers via internet-based marketplaces
- Defendant 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

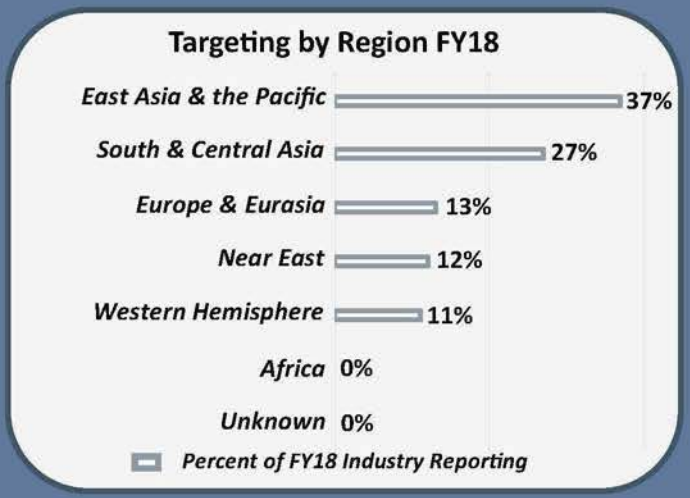
Takeaway: Shipping to freight companies can be used to obfuscate the actual location and identity of the end user.

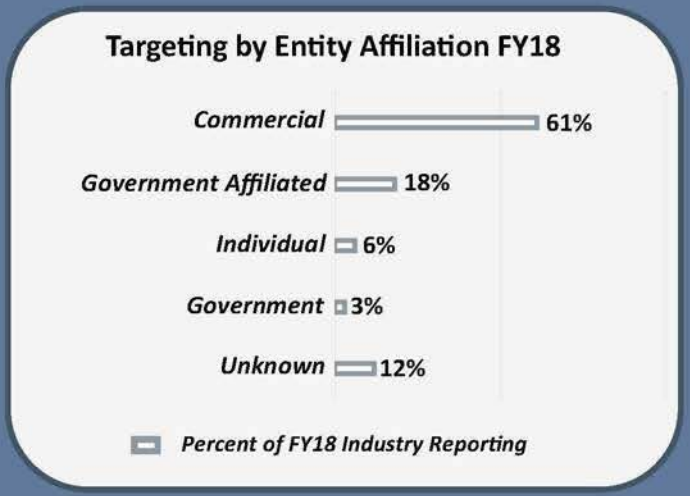
Source: U.S. Department of Justice, U.S. Attorney's Office, Eastern District of New York, https://www.justice.gov/usao-edny/pr/italian-national-sentenced-11-months-prison-illegally-exporting-and-attempting-export

REPORTED FOREIGN TARGETING OF 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 properties of light, the optics category refers to the study and detection of light in the visible, ultraviolet, and infrared portions of the electromagnetic spectrum. Optics includes, but is not limited to, cameras, fiber optics, lenses, mirrors, night vision, polarization, reflective coatings, and refractive coatings.







Key Findings from FY18 Cleared Industry Reporting

- FIE targeting of optics technologies decreased in FY18; however, it was the fifth most targeted technology
- The majority of foreign collectors targeting optics were commercial entities
- Attempts to purchase optics related technology was the most common approach, often via email

Overview

FY18 was the first year that optics was one of the five top targeted technologies since FY12 when it was a component of the laser, optics, and sensor category, despite experiencing a 36 percent decrease in reported targeting from FY17. The most targeted optics technologies were night vision, cameras, mirrors, and lenses.

East Asia and the Pacific region was the origin for 37 percent of the incidents reported by cleared industry relating to optics. The volume of targeting from this region decreased by 41 percent from FY17. Entities from East Asia and the Pacific targeted cameras and mirrors more than any other optic technology.

South and Central Asia entities were the next most prolific collectors of optics technology in FY18. Noted in over a quarter of the reports relating to optics, entities from South and Central Asia targeted night vision technology more than any other optic technology.

Commercial entities were by far the most common collectors identified in cleared industry reporting of targeting optics. These entities applied the attempted acquisition of technology and RFI/solicitation MO in nearly 90 percent of the incidents.

In FY18, the MOs attempted acquisition of technology and RFI/solicitation were the most used by FIE targeting optics. One of these MOs was identified in 81 percent of the incidents reported in FY18. Exploitation of business activity was the third most reported MO, accounting for just 6 percent of the incidents. By far, email was the most common MC used targeting optics. Cleared industry reporting listed email as the MC in 71 percent of the incidents.

Takeaway: Optics remains a highly sought after technology, even with the reduction of reported FIE targeting in FY18. High quality night vision provides an advantage to U.S. warfighters. FIE will continue to target U.S. optics technology for military and commercial uses. Once obtained, foreign entities can apply the technology and further proliferate it to other countries for commercial gain.

Foreign Collection Methodology Targeting Optics

Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting optics in FY18.

The most commonly reported approach vector associated to optics in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 70 times in FY18. The next most commonly reported approach was **RFI/solicitation** via **email.**

Volume of Reporting of Approach Vectors

H	HIGH volume	M	MEDIUM volume
L	LOW volume		No Reporting

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions, & Trade Shows	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
Methods of Contact		9	0	122	2	0	8	1	9	1	6	0	14
	Volume of Reporting by Methods of Contact												
Attempted Acquisition	75			H				L					L
Exploitation of Business Activity	11	L		L	L		L						
Exploitation of Cyber Operations	0												
Exploitation of Experts	6			L			L				L		
Exploitation of Insider Access	5				L		L						
Exploitation of Relationship	2						L				L		
Exploitation of Security Protocol	1						L						
Exploitation of Supply Chain	0												
Résumé Submission	9								L	L			
RFI/Solicitation	63	L		H					L		L		L
Search & Seizure	0												
Surveillance	0												
Theft	0												

Top Targeted Optics Subcomponents

Night Vision
- Panoramic Night Vision Goggles

Cameras

Mirrors

Lenses

Reflective Coatings

Holograms & Holographic Technology

Wave-optics Modeling & Analysis

Targeting 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

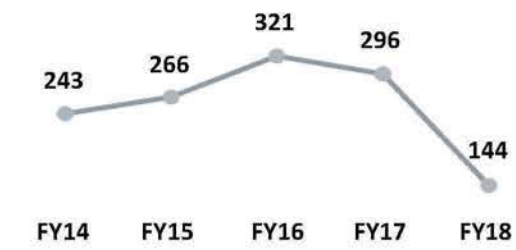
- Defendant and co-conspirators illegally exported and attempted to export dual-use technologies to Iran
- Specific items included two types of thermal imaging cameras; other items included inertial guidance systems testing equipment
- The thermal imaging cameras can be used in commercial security systems and on UAVs and military drones
- 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. *Source: U.S. Department of Justice, U.S. Attorney's Office, Western District of Washington, https://www.justice.gov/usao-wdwa/pr/canadian-sentenced-3-years-prison-conspiracy-export-restricted-goods-and-technology*

FOREIGN TARGETING OF OTHER TECHNOLOGIES

Radars

Targeting of Radars FY14 - FY18



Number of cleared industry reports of possible foreign targeting of radars

In FY18, 2 percent of the reports from cleared industry identified radars as the targeted technology. The reported targeting of radars has decreased over the past 2 years, dropping by 51 percent from FY17. The most frequently targeted radars in FY18 have ground forces applications with ground penetrating radar and through-the-wall radar accounting for 24 percent of targeted radar systems. Radars commonly associated with anti-access area denial (A2/AD) such as target acquisition, air defense, and early warning were noted in fewer incidents.

In FY18, entities from the East Asia and the Pacific region were the most active collectors targeting radar. They accounted for 39 percent of the incidents, followed by the Near East and South and Central Asia regions. Commercial entities were noted in 49 percent of the incidents targeting radars.

Targeted Radar Types

- Ground Penetrating radar
- Through-the-wall radar
- Target Acquisition
- Electronically Steered

Top Methods of Operation

- Attempted Acquisition of Technology
- RFI/Solicitation
- Exploitation of Business Activity

Top Methods of Contact

- Email
- Conferences, Conventions, & Trade Shows
- Personal Contact

Software

Targeting of Software FY14 - FY18

Number of cleared industry reports of possible foreign targeting of software

Reporting from cleared industry of incidents relating to software accounted for 2 percent of all reports in FY18. The reports relating to targeting of software dropped by 46 percent in FY18. Cleared industry identified modeling and simulation software in 28 percent of the reporting. The next most reported software was artificial intelligence software, noted in 11 percent of the reporting. All other types of software were noted in less than 10 percent of the reports related to this category.

Not surprisingly, East Asia and the Pacific region entities were the most active collectors targeting software, accounting for 35 percent of the reporting in FY18. Europe and Eurasia entities were the second most active, identified in 25 percent of the reports. Commercial was the most active entity affiliation identified in 43 percent of the reports relating to software.

Targeted Software

- Modeling & Simulation
- Artificial Intelligence
- Information & Cyber Security Technology
- Software & Algorithms
- System Development Kits

Top Methods of Operation

- RFI/Solicitation
- Attempted Acquisition of Technology
- Exploitation of Business Activity

Top Methods of Contact

- Email
- Personal Contact
- Conferences, Conventions, & Trade Shows

Space Systems

Targeting of Space Systems FY14 - FY18

Number of cleared industry reports of possible foreign targeting of space systems

Cleared industry reporting of suspicious contacts identified space systems as the targeted technology in 2 percent of the reports in FY18. The volume of reporting related to space systems decreased by 22 percent from FY17. In FY18, one-third of the reports of targeting space systems involved satellite buses. A satellite bus is a general satellite model on which multiple satellites can be produced with different payloads.

DCSA identified East Asia and the Pacific region entities in 31 percent of the reporting associated with targeting of space systems. Entities from Europe and Eurasia were identified in 24 percent of the reporting in FY18, and entities from the Western Hemisphere were identified in 20 percent. Cleared industry reported commercial entities in 35 percent of the reporting and government affiliated entities in 34 percent.

Targeted Space Systems

- Satellites & Satellite Buses
- Space Broadcast Systems
- Space Launch Vehicle/Systems
- Space Mission Control Systems
- Space Survivability Systems & Equip.

Top Methods of Operation

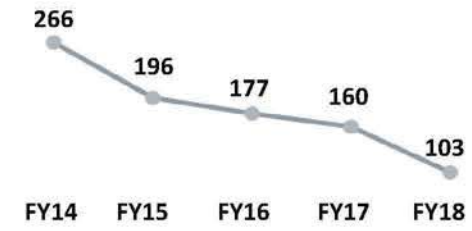
- Attempted Acquisition of Technology
- RFI/Solicitation
- Exploitation of Business Activity

Top Methods of Contact

- Email
- Personal Contact
- Foreign Visit

Marine Systems

Targeting of Marine Systems FY14 - FY18



Number of cleared industry reports of possible foreign targeting of marine systems

Since FY13, the targeting of marine systems has decreased each year. In FY18, marine systems were identified in under 2 percent of cleared industry reporting. The volume of incidents targeting marine systems dropped 36 percent from FY17. Of specific marine systems technologies, reports of targeting of combat ships and landing vessels decreased by 63 percent, and that of submarines and designs fell by 25 percent.

According to FY18 reporting, entities from East Asia and the Pacific region were involved in 48 percent of the incidents and Western Hemisphere entities were the second most active, noted in 17 percent of the reports. Commercial and government affiliated were the two most active entities targeting marine systems in FY18, accounting for 39 and 23 percent of the reporting, respectively.

Targeted Marine Systems

- Autonomous Underwater Vehicles
- Submarines & Designs
- Combat Ships & Landing Vessels
- Unmanned Surface Vessels
- Deep Seas Submersibles

Top Methods of Operation

- RFI/Solicitation
- Attempted Acquisition of Technology
- Exploitation of Business Activity

Top Methods of Contact

- Email
- Personal Contact
- Conferences, Conventions, & Trade Shows

Energy Systems

Energy systems was the tenth most targeted technology as reported by cleared industry in FY18. These technologies were targeted in just under 2 percent of cleared industry reporting. The East Asia and the Pacific region was the origin of over half of the reported attempts to collect on energy systems.

Targeted Energy Systems

Gas Turbine Engines	Batteries
Propellants	Rocket Engines
Turbo Fan Engines	Ocean Power Technologies
Energy Systems Components	Generators

Top Methods of Operation

- Résumé Submission
- Attempted Acquisition of Technology
- RFI/Solicitation

Top Methods of Contact

- Email
- Résumé—Academic
- Foreign Visit

Positioning, Navigation, and Time

Positioning, navigation, and time (PNT) accounted for the targeted technology in just over 1 percent of reporting in FY18. DCSA identified entities from East Asia and the Pacific region in 39 percent of the reports of targeting of PNT.

Targeted Positioning, Navigation, and Time

Inertial Measuring Units	Gyroscopes
Global Positioning System (GPS)	Accelerometers
Navigational Aids	GPS Alternative Systems
Radio Frequency & other Beacon-Based Navigation Technology	

Top Methods of Operation

- Attempted Acquisition of Technology
- RFI/Solicitation
- Exploitation of Business Activity

Top Methods of Contact

- Email
- Personal Contact
- Conferences, Conventions, & Trade Shows

Sensors (Acoustic)

Reported targeting of sensors (acoustic) technology increased by 122 percent in FY18 over FY17. Entities from East Asia and the Pacific accounted for 63 percent of reporting relating to sensors.

Targeted Sensor (Acoustic)

Acoustic Sensor Products	Active Sonar
Sonobouys	Seismic Ground
Acoustic, Sensors, and Displays	

Top Methods of Operation

- Attempted Acquisition of Technology
- RFI/Solicitation
- Résumé Submission

Top Methods of Contact

- Email
- Web Form Submission
- Résumé—Academic

Materials: Raw and Processed

In FY18 reporting, the number of incidents of targeting of materials: raw and processed, dropped by 40 percent from FY17. Entities from East Asia and the Pacific accounted for 58 percent of the reports.

Targeted Materials: Raw and Processed

Fiber-based Materials	Alloys
Plastic—Unique or Advanced	Structural Foam
Chemicals	

Top Methods of Operation

- Attempted Acquisition of Technology
- RFI/Solicitation
- Résumé Submission

Top Methods of Contact

- Email
- Résumé—Academic
- Social Networking Services

Ground Systems

Reported targeting of ground systems was up 7 percent from FY17. Entities from the Near East were the most active collectors identified in 28 percent of the SCRs.

Targeted Ground Systems

Light Armored Vehicles & Designs

Medium Tactical Vehicles & Designs

Unmanned Ground Systems

Cargo Systems

Transport Vehicles & Designs

M1 Abrams Variations of Heavy Tanks & Designs

Top Methods of Operation

- RFI/Solicitation
- Exploitation of Business Activity
- Attempted Acquisition of Technology

Top Methods of Contact

- Conferences, Conventions, & Trade Shows
- Email
- Foreign Visit

Lasers

In FY18 the reported targeting of lasers decreased 27 percent from FY17. East Asia and the Pacific region entities were identified in 47 percent of the reports of targeting technologies and information relating to lasers.

Targeted Lasers

Solid State Lasers

Gas Lasers

High Energy Laser Weapons

Fiber Lasers

Top Methods of Operation

- Attempted Acquisition of Technology
- RFI/Solicitation
- Exploitation of Relationship

Top Methods of Contact

- Email
- Personal Contact
- Conferences, Conventions, & Trade Shows

Biological

Targeted Biological

Biological Agent Detection Equipment

Biological or Physiological Research

DNA Research

Top Methods of Operation

- Résumé Submission
- Exploitation of Relationship
- Exploitation of Insider Access

Top Methods of Contact

- Résumé—Academic
- Email
- Foreign Visit

Directed Energy

Targeted Directed Energy

Directed Electromagnetic Radiation (not lasers)

High-Power Microwave Systems

Directed Particles with Mass

Top Methods of Operation

- Attempted Acquisition of Technology
- RFI/Solicitation
- Exploitation of Cyber Operations

Top Methods of Contact

- Email
- Cyber Operations
- Résumé—Academic

Agriculture

Targeted Agriculture

Reporting did not list specific agricultural products or services

Top Methods of Operation

- Résumé Submission
- Exploitation of Insider Access
- Exploitation of Relationship

Top Methods of Contact

- Résumé—Academic
- Personal Contact
- Foreign Visit

SECTION 4: TARGETING BY GEOGRAPHIC REGION

EAST ASIA AND THE PACIFIC REGION

Top 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 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 Methods of Contact

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

Entities from East Asia and the Pacific region remained the most active collectors identified in cleared industry reporting in FY18. They were identified in 40 percent of the incidents reported by cleared industry in FY18. The number of incidents associated with this region increased by 20 percent over FY17. DCSA identified commercial entities in over half of the incidents from this region.

Electronics was the top targeted technology in incidents originating from this region, noted in nearly twice as many reports as the second most frequently reported technology — aeronautic systems. Integrated circuits, RADHARD integrated circuits, and digital signal processers were the most targeted electronics. The most targeted aeronautic systems subcomponents by entities from this region were UAV, fixed wing aircraft, and rotary wing aircraft.

Entities from this region used the attempted acquisition of technology and résumé submission MOs in 21 and 18 percent of the reported incidents respectively, while RFI/solicitation and exploitation of business activity both were identified in 13 percent of the incidents. This region was the only region where FIE significantly use the exploitation of supply chain MO. This MO was used in 11 percent of the incidents from this region. The email MC was used in nearly half of the incidents associated with this region.

East Asia and the Pacific Region Case Study

In September 2018, the Justice Department 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 U.S. Government alleged the defendants schemed to steal dynamic random access memory (DRAM) trade secrets from a U.S. company. According to the Justice Department, prior to the events detailed in the indictment China did not possess DRAM technology.

The indictment alleged Taiwan national Stephen Chen became the president of a Taiwan subsidiary of the U.S. company responsible for manufacturing one of the company's DRAM chips. Subsequently, Chen 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.

Chen then recruited employees at the U.S. company's Taiwan subsidiary. Two of these employees stole and provided to UMC trade secrets relating to DRAM design and manufacture. One employee downloaded over 900 confidential files and stored them on a USB external drive and to personal cloud storage, where he could access them while working for UMC.

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.

Source: U.S. Department of Justice, Office of Public Affairs, https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage

NEAR EAST REGION

Top 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 Methods of Operation

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

Top Methods of Contact

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

Each year for the past decade the Near East has been the second most commonly identified region in suspicious contact reports submitted by cleared industry. FY18 was a continuation of this pattern with entities from this region being the second most active. DCSA identified Near East entities in 13 percent of the reports in FY18; this is down from 21 percent of reports in FY17. A trend in incidents involving entities from this region has been that commercial entities from this region are becoming more prevalent. In FY17, 33 percent of the reports from industry associated to this region involved commercial entities. In FY18, it was 41 percent of the incidents. From FY11 to FY16, the most common affiliation for Near East entities was government affiliated.

In FY18, entities from this region were noted targeting aeronautic systems and armament and survivability technologies equally. Each of these technologies was identified as the targeted technology in 9 percent of the reporting associated to this region. The most commonly targeted aeronautic systems included UAV technologies such as UAV detection and counter UAV systems; flight simulator software and training; and rotary wing aircraft. The most targeted armament and survivability technologies were automatic and semi-automatic weapons; X-ray detection systems; electronic warfare; and missiles.

Entities from this region used the résumé submission MO in 33 percent of the incidents and RFI/solicitation MO in 25 percent. Email and résumé – academic were the two most common MCs, used in 36 and 20 percent, respectively, in incidents DCSA attributed to this region.

Near East Region Case Study

In March 2018, the U.S. Department of Justice, U.S. Attorney for Central District of California filed charges against a USPER relating to a plan to send export controlled computer servers to Iran, a Near East region country. The indictment accused the USPER and a company the USPER owned and operated with violating the International Emergency Economic Powers Act (IEEPA). This act restricts the export of certain goods from the United States to foreign nations.

The USPER is accused of purchasing computer servers and sending them to Iran without obtaining licenses from the U.S. Government as required by IEEPA. These servers are dual use, with commercial and military applications.

The USPER allegedly listed false destinations when dealing with the manufacturer. The USPER identified Kosovo and Slovenia as the destinations for the servers. However, the U.S. Attorney asserts the USPER knew the servers were actually destined for Bank Mellot, a financial institution in Iran.

Takeaway: As noted in this case study and several earlier case studies, 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.

Source: U.S. Department of Justice, U.S. Attorney's Office, Central District of California, https://www.justice.gov/usao-cdca/pr/dana-point-man-charged-scheme-send-export-controlled-computer-servers-iran

EUROPE AND EURASIA REGION

Top 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 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 Methods of Contact

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

DCSA identified entities from Europe and Eurasia region in 12 percent of the incidents reported by cleared industry in FY18. Incidents associated to this region decreased by 8 percent in FY18. Entities from this region most frequently targeted aeronautic systems and electronics, targeting each in 10 percent of the incidents. The most commonly targeted subcomponents of aeronautic systems were UAVs and flight simulator software and training. The most targeted electronics were integrated circuits, RADHARD, and wafers. RFI/solicitation and attempted acquisition of technology MOs collectively accounted for more than half of these incidents. Email was the MC used in 48 percent of the incidents. The application of the RFI/solicitation MO combined with the email MC occurred in 19 percent of the incidents related to this region.

SOUTH AND CENTRAL ASIA REGION

Top 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 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 Methods of Contact

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

In FY18, entities from South and Central Asia were identified in 11 percent of cleared industry reporting. Entities from this region were identified in 13 percent fewer incidents than in FY17. These entities predominantly targeted electronics. The targeting of electronics accounted for 20 percent of the activity noted from this region. The volume of incidents relating to electronics more than doubled the targeting of aeronautic systems. They targeted integrated circuits in 39 percent of the incidents relating to electronics. They also targeted RADHARD integrated circuits and FPGAs to a much lesser degree. In industry reports that DCSA associated to this region, attempted acquisition and RFI/solicitation were the MOs used in 70 percent, and email was the MC used in 66 percent of the incidents.

WESTERN HEMISPHERE REGION

Top Targeted Technologies

Aeronautic Systems	14%
C4	8%
Armament & Survivability	8%
Electronics	5%
Space Systems	5%
Software	4%
Optics	4%
Marine Systems	4%
Positioning, Navigation, & Time	2%
Radars	2%

Top Methods of Operation

RFI/Solicitation	22%
Exploitation of Insider Access	18%
Exploitation of Security Protocols	15%
Exploitation of Relationship	14%
Attempted Acquisition of Technology	11%

Top Methods of Contact

Personal Contact	44%
Email	30%
Phishing Operations	4%
Conferences, Conventions, & Trade Shows	4%
Web Form Submission	4%

Cleared industry reporting associated to entities from the Western Hemisphere region dropped by 8 percent in FY18 from FY17. DCSA identified entities from this region in just 8 percent of reporting in FY18. For the second year in a row, individual was the most common affiliation for collectors from this region, followed by commercial entities. Targeting of aeronautic systems accounted for 14 percent of the incidents assessed as originating from this region. The most sought after aeronautic systems subcomponents were UAV, flight simulator software and training, and airframes and structural components. These collectors used RFI/solicitation and exploitation of insider access as the most common MOs, used in 22 and 18 percent of the incidents, respectively. Personal contact was the most common MC, used in 44 percent of the incidents.

AFRICA REGION

Top Targeted Technologies

Aeronautic Systems	15%
C4	13%
Electronics	8%
Armament & Survivability	7%
Ground Systems	4%
Positioning, Navigation, & Time	3%
Radars	3%
Software	2%
Space Systems	2%
Chemical	1%

Top Methods of Operation

RFI/Solicitation	32%
Attempted Acquisition of Technology	26%
Résumé Submission	15%
Exploitation of Cyber Operations	13%
Exploitation of Business Activity	10%

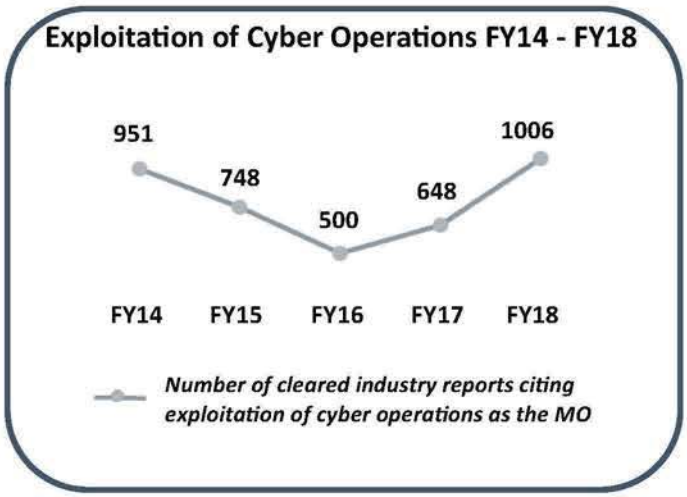
Top Methods of Contact

Email	56%
Résumé—Professional	11%
Phishing Operations	9%
Personal Contact	5%
Conferences, Conventions, & Trade Shows	3%

Incidents associated to entities from the Africa region increased by 32 percent in FY18. However, this volume of reporting still represented less than 1.5 percent of all reporting in FY18. DCSA identified commercial entities as being involved in over half of the incidents originating from this region. Entities from this region most frequently were identified targeting aeronautic systems and C4 in 15 and 13 percent of the incidents, respectively. The most sought after aeronautic systems subcomponents were UAV and fixed wing aircraft. The most targeted C4 subcomponents were wide area surveillance systems, telecommunication devices, and identification friend/foe (IFF). African entities used the RFI/solicitation MO in 32 percent and attempted acquisition in 26 percent of the incidents. A majority of the incidents (56 percent) used email as the MC. The application of the RFI/solicitation MO in conjunction with email MC was reported in approximately 28 percent of the incidents originating from the Africa region.

SECTION 5: SPECIAL INTEREST TOPICS

CYBER ACTIVITY TARGETING CLEARED INDUSTRY



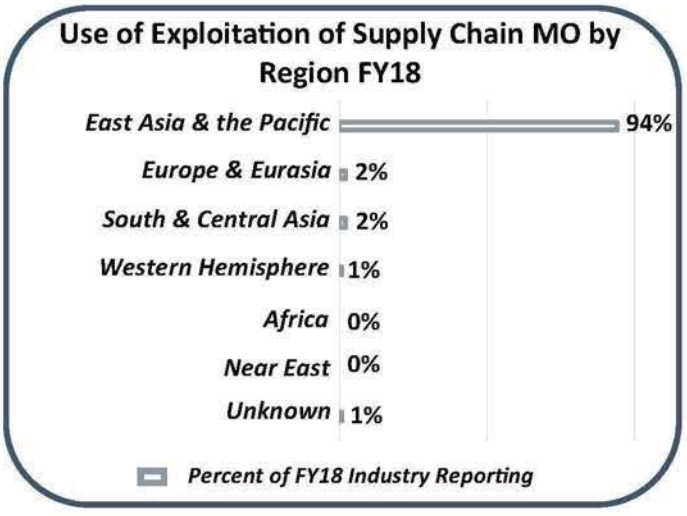
Exploitation of cyber operations was the third most commonly identified MO in FY18 cleared industry reporting. It accounted for 17 percent of the incidents in FY18. Identification of this MO increased by 55 percent from FY17.

In this report, exploitation of cyber operation is not covered significantly in the technology and region sections above because most cyber incidents cannot be linked to a specific actor nor can the targeted technology be determined. Seventy-five percent of the incidents cannot be, with sufficient confidence, associated to a specific actor, and in 91 percent the targeted technology is unknown. When an actor was identified the most common region of origin for the incident was East Asia and the Pacific region, identified in 11 percent of the reporting. Aeronautic systems was the most targeted technology, but represented just less than 1 percent of reporting of exploitation of cyber operations.

The most common MC used in conjunction with this MO was phishing operation, noted in 50 percent of the reports. A phishing operation involves including a link to a site or an attachment that has malicious code embedded with the intent of loading the malicious code to the targeted network. The next most common MC was cyber operations, identified in 48 percent of the reports. Cyber operations are activities taken directly against a targeted system and include cyber network attack (CNA) and cyber network exploitation (CNE).

The most common cyber operations exploits were network scanning and probing, noted in 22 percent, and web site exploitation, noted in 6 percent of reporting.

EXPLOITATION OF SUPPLY CHAIN



Another lightly reported MO is exploitation of supply chain. Exploitation of supply chain is compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication. Successful application of this MO can lead to devastating impacts to warfighters.

DCSA identified exploitation of supply chain as the MO in just 5 percent of industry reporting in FY18. DCSA associated nearly all reported incidents of this MO to entities from East Asia and the Pacific. Similarly, DCSA identified commercial entities in 96 percent of the incidents of this MO.

In 93 percent of the reported incidents the targeted technology was not identified. Electronics was the most commonly identified IBTL category, cited in 2 percent of the reports of exploitation of supply chain.

Cyber operations and exploitation of insider threat are methods for adversaries to exploit access to code or the actual component to inject malicious content or substandard parts into DoD supply chains. Furthermore, counterfeit or altered components can enter the supply chain through procuring electronics on the gray market or from unscrupulous brokers.

Another vector to gain access to DoD supply chains is foreign investment in U.S. companies. Through joint ventures or foreign ownership, a foreign entity could gain access to vital segments of U.S. economy. One especially vulnerable sector is telecommunications. Foreign involvement or control over parts of this sector could provide a foreign actor the ability to disrupt government and private communication, and potentially gain access to data transiting the communications infrastructure.

CHINA TECHNOLOGY TRANSFER

In 2017, the President of the United States directed Office of the United States Trade Representative (USTR) "...to determine whether to investigate China's laws, policies, practices, or actions that may be unreasonable or discriminatory and that may be harming American intellectual property rights, innovation, or technology development."

On March 22, 2018, the White House released a Presidential Memorandum on the USTR 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."*

https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/

On November 1, 2018, the Justice Department released its China Initiative Fact Sheet and included a statement from the Federal Bureau of Investigation (FBI) Director relating to China's threat to U.S. economic security:

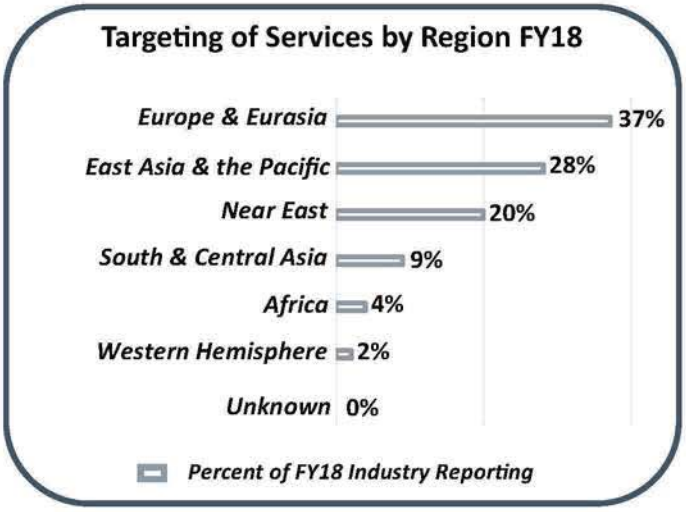
"No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China... The Chinese government is determined to acquire American technology, and they're willing [to] use a variety of means to do that – from foreign investments, corporate acquisitions, and cyber intrusions to obtaining the services of current or former company employees to get inside information. If China acquires an American company's most important technology – the very technology that makes it the leader in a field – that company will suffer severe losses, and our national security could even be impacted."

Christopher Wray, Director, FBI

https://www.justice.gov/opa/speech/file/1107256/

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.

TARGETING OF SERVICES



Targeted Services in FY18

Translation Services	Education and Training
Delivery & Freight Services	Analytic Services
Security & Protection Services	Consulting Services
Hardened Building Construction	Construction
Information Technology Services	Engineering

Although not included as part of the IBTL, cleared industry reports incidents of probable foreign collection targeting services. The number of SCRs identifying targeting of services was less than 1 percent in FY18. However, targeting of services still represents a threat to DoD and cleared industry.

The most common MOs were résumé submission and RFI/solicitation accounting for 33 and 30 percent of the reporting, respectively. Email was the most common MC used, in 54 percent of the incidents and résumé – professional was the next most common MC at 24 percent of reporting.

Targeting of services can be used to identify potential targets for traditional human intelligence (HUMINT) collection, or to attempt to infiltrate an asset into DoD via services such as translation services or security and protective services contracts.

Targeting of services could be useful to foreign adversaries in improving their weapons, countermeasures, and facilities. An adversary developing underground facilities or hardening critical infrastructure could gain from cleared industry involved in construction and engineering services. They could also gain information on DoD methods for hardening critical infrastructure, which could be useful in determining how to target U.S. critical infrastructure.

CATEGORY DESCRIPTIONS

INDUSTRIAL BASED TECHNOLOGY LIST (IBTL)

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 (C4)

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 (PNT)

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.

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.

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.

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.

METHODS OF OPERATION

Distinct patterns or methods of procedure thought to be characteristic of or habitually followed by an individual or organization involved in intelligence activity. These generally include attempts at:

Attempted Acquisition of Technology

Acquiring protected information in the form of controlled technologies, via direct contact or through the use of front companies or intermediaries, including the equipment itself or diagrams, schematics, plans, spec sheets, or the like.

Exploitation of Business Activities

Establishing a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service provider; leveraging an existing commercial relationship in order to obtain access to personnel or protected information and technology.

Exploitation of Cyber Operations

Foreign intelligence entities or other adversaries compromising the confidentiality, integrity, or availability of targeted networks, applications, credentials or data with the intent to gain access to, manipulate, or exfiltrate personnel information or protected information and technology.

Exploitation of Experts

Gaining access to personnel or protected information and technology via requests for, or arrangement of, peer or scientific board review of academic papers or presentations; requesting a consult with faculty members or subject matter experts; or attempting to invite or otherwise entice subject matter experts to travel abroad or consult for foreign entities.

Exploitation of Insider Access

Trusted insiders exploiting their authorized placement and access within cleared industry or cause other harm to compromise personnel or protected information and technology.

Exploitation of Relationships

Leveraging existing personal or authorized relationships to gain access to protected information.

Exploitation of Security Protocols

Visitors or unauthorized individuals circumventing or disregarding security procedures or behaviors by cleared or otherwise authorized persons that indicate a risk to personnel or protected information and technology.

Exploitation of Supply Chain

Compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.

Resume Submission

Foreign persons submitting resumes for academic or professional placement that would facilitate access to protected information to enable technological or economic advancements by the foreign entity.

Request for Information/Solicitation

Collecting protected information by directly or indirectly asking or eliciting personnel for protected information and technology.

Search/Seizure

Temporarily accessing, taking, or permanently dispossessing someone of property or restricting freedom of movement via tampering or physical searches of persons, environs, or property.

Surveillance

Systematically observing equipment, facilities, sites, or personnel associated with contracts via visual, aural, electronic, photographic, or other means to identify vulnerabilities or collect information.

Theft

Acquiring protected information with no pretense or plausibility of legitimate acquisition.

METHODS OF CONTACT

Approaches used to connect the foreign actor to the targeted individual, information, network, or technology in order for the foreign actor to execute the MO(s).

Conferences, Conventions, and Tradeshows
Contact regarding or initiated during an event, such as a conference, convention, exhibitions, or tradeshow.

Cyber Operations
Activities taken directly against a targeted system; to include cyber network attack, cyber network exploitation, and collection.

Email
Unsolicited requests received via email for information or purchase requests.

Foreign Visit
Activities or contact occurring before, during, or after a visit to a contractor's facility.

Mail
Contact initiated via mail or post.

Personal Contact
Person-to-person contact via any means where the foreign actor, agent, or co-optee is in direct or indirect contact with the target.

Phishing Operation
Emails with embedded malicious content or attachments for the purpose of compromising a network to include but not limited to spear phishing, cloning, and whaling.

Resume – Academic
Resume or curricula vitae (CV) submissions for academic purposes.

Resume – Professional
Resume or CV submissions for professional purposes (e.g., seeking a position with a cleared company).

Social Networking Service
Contact initiated via a social or professional networking platform.

Web Form
Contact initiated via a company-hosted web submission form.

Telephone
Contact initiated via a phone call by an unknown or unidentified entity.

COLLECTOR AFFILIATIONS

Commercial
Entities whose span of business includes the defense sector.

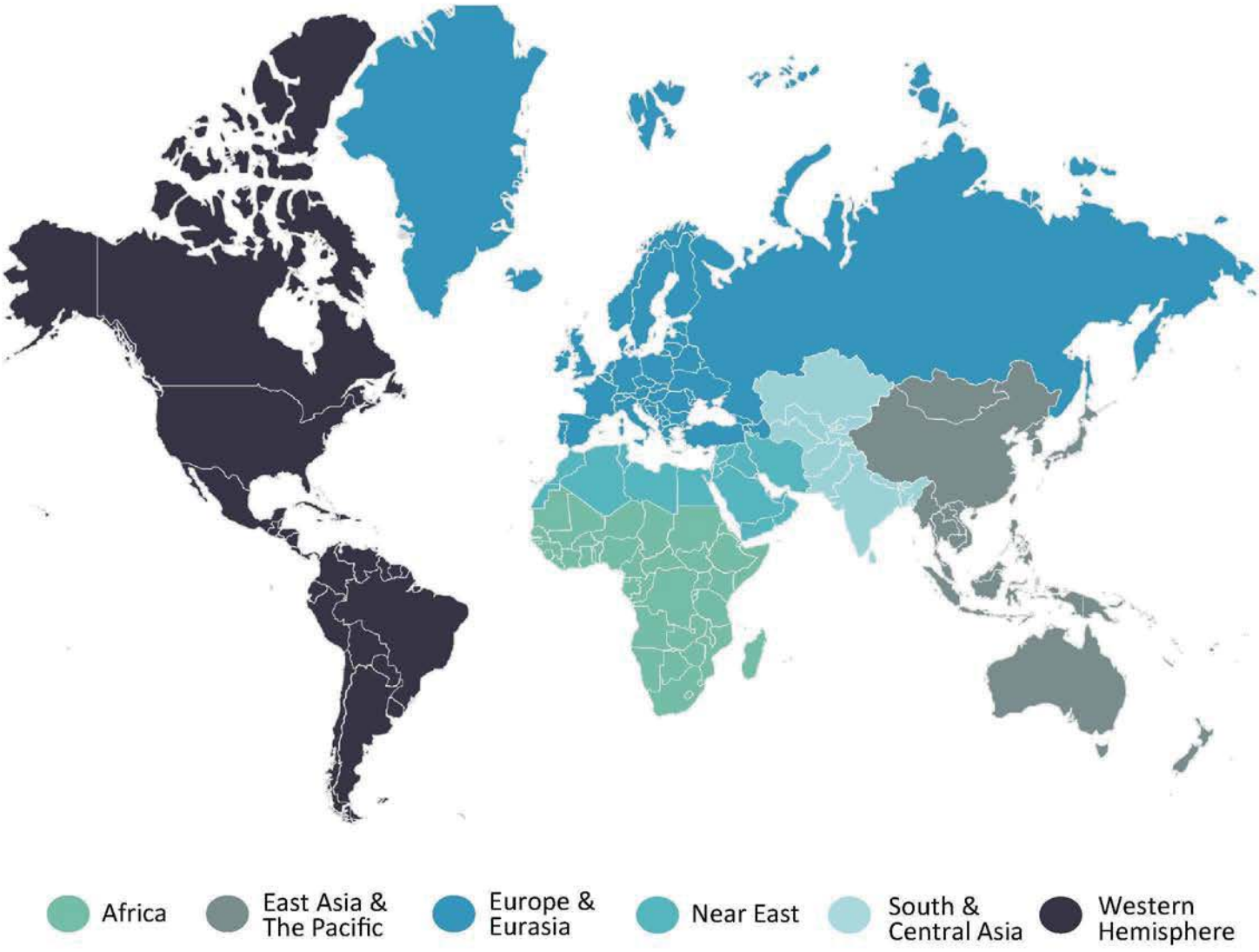
Government
Ministries of Defense and branches of the military, as well as foreign military attaches, foreign liaison officers, intelligence services, and the like.

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.

REGION BREAKDOWN



AFRICA

Angola
Benin
Botswana
Burkina Faso
Burundi
Cameroon
Cabo Verde
Central African Republic
Chad
Comoros
Congo, Democratic Republic of the
Congo, Republic of the
Cote d'Ivoire
Djibouti
Equatorial Guinea
Eritrea
Ethiopia
Gabon
Gambia, the
Ghana
Guinea
Guinea-Bissau
Kenya
Lesotho
Liberia
Madagascar
Malawi
Mali
Mauritania
Mauritius
Mozambique
Namibia
Niger
Nigeria
Rwanda
Sao Tome and Principe
Senegal
Seychelles
Sierra Leone
Somalia
South Africa
South Sudan
Sudan
Swaziland
Tanzania
Togo
Uganda
Zambia
Zimbabwe

EAST ASIA & THE PACIFIC

Australia
Brunei
Burma
Cambodia
China
Fiji
Indonesia
Japan
Kiribati
Korea, North
Korea, South
Laos
Malaysia
Marshall Islands
Micronesia, Federated States of
Mongolia
Nauru
New Zealand
Palau
Papua New Guinea
Philippines
Samoa
Singapore
Solomon Islands
Taiwan
Thailand
Timor-Leste
Tonga
Tuvalu
Vanuatu
Vietnam

EUROPE & EURASIA

Albania
Andorra
Armenia
Austria
Azerbaijan
Belarus
Belgium
Bosnia and Herzegovina
Bulgaria
Croatia
Cyprus
Czech Republic
Demark
Estonia
Finland
France
Georgia
Germany
Greece
Holy See
Hungary
Iceland
Ireland
Italy
Kosovo
Latvia
Liechtenstein
Lithuania
Luxembourg
Macedonia
Malta
Moldova
Monaco
Montenegro
Netherlands
Norway
Poland
Portugal
Romania
Russia
San Marino
Serbia
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom

NEAR EAST

Algeria
Bahrain
Egypt
Iran
Iraq
Israel
Jordan
Kuwait
Lebanon
Libya
Morocco
Oman
Palestinian Territories
Qatar
Saudi Arabia
Syria
Tunisia
United Arab Emirates
Yemen

SOUTH & CENTRAL ASIA

Afghanistan
Bangladesh
Bhutan
India
Kazakhstan
Kyrgyzstan
Maldives
Nepal
Pakistan
Sri Lanka
Tajikistan
Turkmenistan
Uzbekistan

WESTERN HEMISPHERE

Antigua and Barbuda
Argentina
Aruba
Bahamas, the
Barbados
Belize
Bermuda
Bolivia
Brazil
Canada
Cayman Islands
Chile
Colombia
Costa Rica
Cuba
Curacao
Dominica
Dominican Republic
Ecuador
El Salvador
Grenada
Guatemala
Guyana
Haiti
Honduras
Jamaica
Mexico
Nicaragua
Panama
Paraguay
Peru
St. Kitts and Nevis
St. Lucia
St. Maarten
St. Vincent and the Grenadines
Suriname
Trinidad and Tobago
United States
Uruguay
Venezuela

Page Intentionally Left Blank