TARGETING U.S. TECHNOLOGIES: A REPORT OF THREATS TO CLEARED INDUSTRY

Defense Counterintelligence and Security Agency

2022

TABLE OF CONTENTS

PREFACE 3

SCOPE & METHODOLOGY 4

EXECUTIVE SUMMARY 5

KEY FINDINGS 6

REGIONS 8

- East Asia and the Pacific 8
- Near East 10
- Europe and Eurasia 12
- South and Central Asia 14
- Western Hemisphere 15
- Africa 16

ADMINISTRATIVE INFORMATION 17

- IBTL Category Description 17
- Methods of Operation 19
- Methods of Contact 20
- Collector Affiliation 20
- Regions Breakdown 21

Product ID: DCSA-TA-23-001

Prepared by: Analysis Division, Counterintelligence and Insider Threat Directorate, DCSA

Coordinated with: Defense Intelligence Agency

PREFACE

Today, we are at a security inflection point. Two decades ago, the terrorist attacks of September 11th, 2001 yielded a watershed moment that profoundly changed our perception of the strategic landscape we faced as a country. As a consequence, personnel security increased in prominence and even animated the formation of the Defense Counterintelligence and Security Agency (DCSA). During the intervening years, industrial security was given less attention.

The shift in threat picture today may be less dramatic in manner, but it is no less ominous in substance. Great power competition is rightly back in vogue among security professionals, and with it comes the realization that our near-peer competitors have been consistently improving their game. While America was countering terrorist threats, potential adversaries maintained their focus on our industrial base—not only to identify and exploit vulnerabilities, but also to steal technologies to further their own development efforts.

The foreign intelligence threat to this nation's defense industrial base has never been more capable, sophisticated, or complex. Nor could it be more challenging in implication. To a greater degree than ever before, the importance of technology means that tomorrow's conflict is taking place today. As adversaries use illicit methods to acquire classified and sensitive information and technologies, they determine the outcome of future conflicts. The time has passed for us to redouble our industrial security efforts. This edition of The Targeting U.S. Technologies: A Report of Threats to Cleared Industry reflects the threat picture to inform those efforts.

As the largest security organization in the Federal Government, DCSA calls itself "America's Gatekeeper." But the gatekeeper function today is far too complex for any one entity; it requires a whole-of-government approach. America prides itself on having an open society. But our adversaries use this against us to gain technological advantage with challenging tools like forced technology transfers, specially designed corporate acquisitions, strategic international partnerships, and simple academic and intellectual property theft. Mitigating these threats starts with understanding them.

In this increasingly complex and challenging geopolitical environment, securing a workforce and uncompromised defense industrial base depends on understanding the threat picture to a greater degree than ever before. I encourage you to use this report as one tool to help in that endeavor.

William K. Lietzau
Director,
Defense Counterintelligence and Security Agency

SCOPE & METHODOLOGY

Each year, DCSA publishes the *Targeting U.S. Technologies: A Report of Threats to Cleared Industry*. This report is published in accordance with Department of Defense (DOD) Instruction (DODI) 5200.39, Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E), dated May 28, 2015. The focus of the annual report is on foreign efforts to compromise or exploit cleared personnel, or to obtain unauthorized access to classified information or technologies resident in the U.S. cleared industrial base. DCSA provides a snapshot of its findings on foreign collection attempts and provides analysis that covers the most pervasive foreign collectors targeting the cleared contractor (CC) community during fiscal year 2021 (FY21). This report serves to articulate the threat to industry and U.S. Government leaders.

The report includes analysis on foreign intelligence entity (FIE) threats to U.S. technologies residing in cleared facilities. As this report is unclassified, it does not provide a holistic view of the FIE threat to cleared industry. DCSA annually produces a classified companion assessment.

Throughout FY21, an estimated 12,550 CC facilities were required to report information in accordance with Part 117 of Title 32, Code of Federal Regulations, National Industrial Security Program Operating Manual (NISPOM). DCSA examined suspicious contacts received from cleared industry that directly address FIE threats. DCSA receives and processes suspicious contacts from cleared industry containing indicators that are either likely, very likely, or almost certain, that an entity—regardless of nationality—attempted to obtain unauthorized access to classified information or technology or to compromise a cleared employee. However, DCSA cannot estimate in this forum the volume of FIE targeting that goes unnoticed or unreported by cleared industry.

DCSA evaluated suspicious incidents received from cleared industry in FY21 depicting foreign threats to cleared companies and facilities. DCSA also considered relevant reporting and finished intelligence products from DOD and the Intelligence Community (IC) for the purpose of addressing DCSA's analytic line. Additionally, DCSA incorporated relevant reports from the DCSA Joint Cyber Intelligence Tool Suite (JCITS)[i] and assessed cyber threats to cleared industry when reporting was available. The suspicious contacts serve as the foundation for this report.

DCSA organized this report by targeting region, then considered the targeted technology, methods of operation (MO) employed, methods of contact (MC) used, and collector affiliation. DCSA ranked the regions based on the number of suspicious contacts received in FY21 from cleared industry: East Asia and the Pacific, Near East, Europe and Eurasia, South and Central Asia, Western Hemisphere, and Africa. Additionally, when a targeting attempt against a technology was confirmed, the targeted technology was placed into one of the Industrial Base Technology List (IBTL) categories (see Category Descriptions). Additional reporting from cleared industry on foreign intelligence threats has and will continue to improve the accuracy of the analysis and threat levels addressed in DCSA annual assessments.

i Joint Cyber Intelligence Tool Suite (JCITS) is a cyber-intelligence analytic platform that leverages various data feeds and information to identify adversarial behaviors in the cyber domain.

EXECUTIVE SUMMARY

This report reflects foreign collection attempts to obtain unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. In FY21, DCSA received nearly 24,000 reports of suspicious contacts from cleared facilities operating as part of the National Industrial Security Program (NISP). Of these, DCSA reviewed and identified thousands of incidents of counterintelligence concern that likely involved a foreign entity attempting to illicitly obtain classified information or technology resident in cleared industry, or an attempt to compromise a cleared employee.

The large scope and diversity of collection efforts targeting U.S. technologies meant that foreign entities simultaneously directed considerable efforts at many technologies using variations of methods and collectors. In FY21, electronics; software; and command, control, communications, and computers (C4) made up the top three targeted technologies. These three technologies accounted for 40 percent of all reporting for FY21. Aeronautic systems and armament and survivability finished out the top five targeted technologies. The remaining reported collection efforts targeted a variety of technologies covering the remaining 24 IBTL categories.

In FY21, East Asia and the Pacific and Near East entities remained the most significant collectors of sensitive or classified U.S. technology and information, collectively accounting for 61 percent of overall reporting. DCSA attributed nearly 31 percent of suspicious contacts to collectors from Europe and Eurasia, as well as South and Central Asia. Collectors from the Western Hemisphere and Africa, collectively accounted for just 7 percent of reported suspicious contacts.

In FY21, résumé submission was the top MO, accounting for a third of overall reported attempts, more than doubling the next closest MO—exploitation of experts. Near East entities accounted for 35 percent of résumé submission incidents, with students seeking to conduct postgraduate level research at U.S academic centers involved in sensitive or classified research. East Asia and the Pacific entities represented 26 percent of overall résumé submission, despite primarily relying on exploitation of supply chain when targeting cleared industry. The most pervasive MOs used by entities from Africa were résumé submission and request for information (RFI)/solicitation. Each of these two MOs represented 82 percent of the incidents DCSA attributed to this region. Western Hemisphere collectors relied heavily on exploitation of cyber operations, followed by exploitation of insider access and exploitation of experts.

In FY21, individual was the top collector affiliation, collectively accounting for nearly half of overall reported attempts, primarily due to résumé submission. DCSA attributed nearly 27 percent of suspicious contacts to individual collectors from the Near East, as well as South and Central Asia, seeking advanced degrees and employment opportunities at CCs. Reporting indicated that commercial entities from East Asia and the Pacific, constituted 62 percent of the overall reported attempts. On several occasions, commercial collectors offered manufacturing services and requested to serve as overseas distributors for CC products in regional markets.

KEY FINDINGS

DCSA based the following key findings on analysis of FY21 cleared industry reporting:

East Asia and the Pacific

- Entities from this region were the most prolific collectors of classified information and technology resident in the cleared industrial base, accounting for 38 percent of all reports.
- Nearly every IBTL category was targeted with an emphasis on electronics, software, and C4.
- Commercial and individual entities were among the top collectors.

Near East

- The most targeted technologies were C4 and electronics, followed by aeronautic systems.
- Consistent with the previous 2 years, résumé-academic was the most common MC.
- Individual entities continued to be the most prevalent, accounting for 67 percent of collection affiliation.

Europe and Eurasia

- The top three targeted technologies—aeronautic systems, software, and electronics—made up a third of all reporting.
- Individual entities were the most prominent collectors, accounting for 37 percent.
- Entities most commonly used RFI/solicitation via email.

South and Central Asia

- The top technologies targeted included C4, software, and electronics, accounting for 50 percent of total reporting from this region.
- These entities relied heavily on résumé submissions for both academic and professional placement to gain employment and research positions at cleared facilities or institutions associated with classified research.
- Individual entities were the most common collectors in FY21, accounting for 80 percent.

Western Hemisphere

- Entities from this region targeted a wide variety of technologies, including aeronautic systems, electronics, and software, accounting for 42 percent of total reporting.

- Individual entities were the most commonly reported collector affiliation.
- Entities from this region relied heavily on exploitation of cyber operations and exploitation of insider access when targeting technologies. Collectively, these MOs accounted for 36 percent.

Africa

- The region accounted for 2 percent of all reports
- The most common MOs were résumé submission and RFI/solicitation.
- The most targeted technologies were software and C4.

EAST ASIA & THE PACIFIC	NEAR EAST	EUROPE & EURASIA	SOUTH & CENTRAL ASIA	WESTERN HEMISPHERE	AFRICA
38%	23%	16%	15%	5%	2%
Top Targeted Technology	Top Targeted Technology	Top Targeted Technology	Top Targeted Technology	Top Targeted Technology	Top Targeted Technology
Electronics	C4	Other	C4	Aeronautic Systems	Software
Most Reported Method of Operation	Most Reported Method of Operation	Most Reported Method of Operation	Most Reported Method of Operation	Most Reported Method of Operation	Most Reported Method of Operation
Email	Résumé Submission	Email	Résumé Submission	Email	Résumé Submission
Most Reported Method of Contact	Most Reported Method of Contact	Most Reported Method of Contact	Most Reported Method of Contact	Most Reported Method of Contact	Most Reported Method of Contact
Exploitation of Supply Chain	Résumé-Academic	RFI/Solicitation	Résumé-Professional	Exploitation of Cyber Operations	Résumé-Professional
Most Common Collector Affiliation	Most Common Collector Affiliation	Most Common Collector Affiliation	Most Common Collector Affiliation	Most Common Collector Affiliation	Most Common Collector Affiliation
Commercial	Individual	Individual	Individual	Individual	Individual

REGIONS

East Asia and the Pacific

Overview

In FY21, East Asia and the Pacific region entities remained the most prominent threat to U.S. sensitive and classified information resident in the cleared industrial base, accounting for nearly 38 percent of all cleared industry reporting. While some East Asia and the Pacific countries remain committed to acquiring U.S. technology deemed necessary to deter and defeat adversarial power projection within the region, others seek to leverage access to existing and emerging U.S. technologies to aid in military power projection throughout the region and the world. Entities from East Asia and the Pacific region have continuously targeted CCs, focusing on U.S. technologies and information used to enable indigenous production capability or support the development of advanced dual-use technologies.

While most East Asia and the Pacific region entities targeted almost all technology areas of the IBTL; however, electronics, software, C4, aeronautic systems, and energy systems remained the top five targeted technologies. East Asia and the Pacific entities prioritized targeting U.S. technologies they could not produce indigenously. For example, some East Asia and the Pacific entities targeted dual-use microelectronics, aeronautic turbine engines, artificial intelligence software, satellite communication systems, telecommunications equipment, and sensors.

Exploitation of supply chain was the most commonly used MO in FY21, which consisted of commercial entities seeking to sell microelectronic components to CCs that can be used to exploit the U.S. supply chain. Résumé submissions and exploitation of experts collectively accounted for 44 percent of the overall reported attempts. The most conspicuous actors sent unsolicited emails and messages on social networking platforms inviting CC personnel to conferences or offering CC personnel lucrative research opportunities in the host country. Based on cleared industry reporting, East Asia and the Pacific entities placed an emphasis on MOs that facilitate technology transfer via human capital, to obtain indigenous production capabilities and address technological shortfalls.

While most East Asia and the Pacific region entities engage in traditional forms of espionage, some entities use the a whole-of-society approach, utilizing academia, non-governmental organizations, state-owned enterprises, and the private sector to collect intelligence. Commercial collectors remained the most predominant in FY21, collectively accounting for nearly 50 percent of overall reported attempts. Individuals and government-affiliated entities ranked second and third, respectively, as the most prevalent collectors. DCSA attributed a number of requests for U.S. technology and information to state-owned enterprises, researchers from state-funded universities, business practitioner, and students who do not directly serve official government roles.

Top Targeted Technology Categories	Most Reported Methods of Operation	Most Reported Methods of Contact	Most Common Collector Affiliations
Electronics: 24%	Exploitation of Supply Chain: 25%	Email: 45%	Commercial: 49%
Software: 14%	Résumé Submission: 23%	Résumé-Academic: 10%	Individual: 30%
C4: 9%	Exploitation of Experts: 21%	Foreign Visit: 9%	Government-Affiliated: 13%

Vignettes

- In 2021, an East Asia and the Pacific region national representing a foreign electronics company sent multiple unsolicited emails to a CC in an attempt to purchase export-controlled, dual-use microelectronic components. The electronics company is subordinate to an organization that is linked to illicitly acquiring dual-use electronic components for an export-restricted East Asia and the Pacific military end user listed on the Department of Commerce's Entity List.

- In 2021, East Asia and the Pacific region state-sponsored cyber actors exploited previously unknown zero-day vulnerabilities to exchange servers. The cyber actors exploited critical vulnerabilities to gain initial access and deployed web shells that enabled actors to control compromised servers. In early March 2021, a CC discovered the exploitation; however, the CC did not discover evidence of code execution on the servers. Discovery of four files associated with the exploitation are attributed to HAFNIUM, a known East Asia and the Pacific state-sponsored cyber group.

- In 2021, a student from East Asia and the Pacific region applied to be a postdoctoral researcher at a U.S. university involved in classified software research for DOD. The student was a recipient of an East Asia and the Pacific government-sponsored scholarship that facilitates emerging science and technology transfer back to the sponsoring country. The scholarship requires the student to regularly report the progress of their studies to the nearest embassy or consulate and to accept guidance from embassy staff. The scholarship also mandates that students who study abroad must return and remain in the East Asia and Pacific country for at least 2 years after they complete their studies overseas and pledge loyalty to the government.

Near East

Overview

As the Near East region entities continued to experience to experience political instability, civil wars, and economic crises, FIEs diversified collection attempts and targeted a variety of technologies using various MO. In FY21, Near East entities remained the second most significant collector of sensitive or classified U.S technology and information resident in the U.S. cleared industrial base, accounting for 23 percent of overall reporting. Industry reporting indicated that Near East entities targeted nearly every category of the IBTL with an emphasis on C4, electronics, and aeronautic systems, collectively accounting for 30 percent of Near East reporting.

In FY21, résumé submission was the top MO, accounting for half of all reported attempts, more than doubling the next closest MO, RFI/solicitation. The most noteworthy change in MOs occurred in the exploitation of business activities. Reports involving this category decreased by 9 percent in FY21, largely due to COVID-19 pandemic travel restrictions, which led to a decline in the number of international business travelers into the United States. Near East entities accounted for 36 percent of résumé submission incidents, with students seeking to conduct postgraduate-level research at U.S academic centers involved in sensitive or classified research; in some instances, to facilitate collection or knowledge transfer of critical information and technology that would assist in research and development of their home country's defense efforts. Furthermore, impacts of complex academic, economic, personal and social factors contributed to Near East entities seeking education and employment opportunities outside of the region.

In FY21, individual entities were the top collector affiliation, collectively accounting for more than two-thirds of overall reported attempts. DCSA attributed a number of individual affiliated requests to students, professors, and researchers from state-funded universities and technology universities. Near East entities made unsolicited contacts to fellow researchers at U.S. CCs seeking technical information, employment, and assistance with research. Many students persistently pursued postdoctoral and research opportunities under technical subject matter experts employed at cleared facilities. The most noteworthy change in affiliations occurred in the commercial category. Reports involving commercial collectors, decreased by nearly 17 percent in FY21, dropping this affiliation from second to third overall.

Top Targeted Technology Categories	Most Reported Methods of Operation	Most Reported Methods Of Contact	Most Common Collector Affiliations
C4: 11%	Résumé Submission: 50%	Résumé-Academic: 35%	Individual: 67%
Other: 10%	RFI/Solicitation: 18%	Web Form: 16%	Government-Affiliated: 12%
Electronics: 10%	Exploitation of Business Activities: 13%	Résumé-Professional: 15%	Commercial: 10%

Vignette

- According to FY21 cleared industry reporting, members of Near East region government student organizations or students associated with those organizations sought to conduct research at cleared academic institutions studying structural engineering, behaviors of composite materials under impact or blast loads, nanotechnology and smart materials, and earthquake engineering. Most Near East students studying in the United States do so for

legitimate reasons, largely to gain access to advanced technical fields of studies. In some instances, however, these fields of study provide knowledge that could be directly misapplied, which not only poses a significant threat to U.S. national security, but also supports Near East region national development aspirations.

- In November 2021, prior to visiting a CC facility, three Near East region government representatives received a pre-foreign visit briefing outlining the facility's security requirements, which included identification requirements and items prohibited from entering the facility. However, on the day of the visit, the representatives arrived without the required identification, brought prohibited devices into the facility, and attempted to take unauthorized photography of the CC's technology. Additionally, one of the representatives attempted to plug their electronic device into the USB port on the CC's system.

- In January 2021, an executive from a Near East region company visited a CC to discuss business development. During the visit, the executive lacked insight into the Near East company's business development, but solicited information about the CC's interactions with other foreign clients. The executive is known for exhibiting suspicious behavior during previous visits to the CC, including asking the CC about their business relationship with other countries, not knowing anything about her job, and always attending meetings to which she was not invited.

Europe and Eurasia

Overview

In FY21, Europe and Eurasia region entities remained the third most active collector of sensitive or classified U.S. technology and information resident within the U.S. cleared industrial base, accounting for 16 percent of all cleared industry reporting. Due to regional aggression, the Europe and Eurasia region remained an environment for potential military conflict, leading many countries to prioritize their defense modernization efforts. Europe and Eurasia entities continued to seek U.S. technology and information to progress their own indigenous military capabilities through both licit and illicit means.

Cleared industry reporting revealed Europe and Eurasia region entities targeted the majority of all technology areas of the IBTL, with an emphasis on aeronautic systems, software, and electronics, accounting for 33 percent of cleared industry reporting. With defense force modernization efforts as the regional focus, the targeting of systems such as unmanned aerial vehicles (UAV) represented the majority of industry reporting in the aeronautics IBTL category. Additionally, Europe and Eurasia entities sought to integrate into the U.S. supply chain by seeking employment and joint ventures with cleared facilities specializing in developing software and cybersecurity. Commonly targeted electronic components included export-controlled, dual-use microelectronics with applications in wireless and network infrastructure, radar, satellite communications, and space platforms.

In FY21, Europe and Eurasia region entities mostly sought access to U.S. technologies and information through RFI/solicitation and exploitation of experts, accounting for 46 percent of suspicious contacts. Europe and Eurasia entities, consisting mostly of individual and commercial-affiliated collectors, contacted cleared facilities requesting information such as access to imagery databases, product catalogs, and technical data for export-controlled defense platforms. Europe and Eurasia entities also engaged in attempts to exploit U.S. subject matter experts by inviting them to overseas conferences, offering consultancy fees to obtain non-public information on U.S. defense platforms, and seeking to conduct media interviews regarding the capabilities of specific U.S. military systems.

Top Targeted Technology Categories	Most Reported Methods of Operation	Most Reported Methods of Contact	Most Common Collector Affiliations
Other: 16%	RFI/Solicitation: 25%	Email: 29%	Individual: 37%
Aeronautic Systems: 12%	Exploitation of Experts: 21%	Web Form: 17%	Commercial: 36%
Software: 11%	Exploitation of Business Activities: 11%	Social Networking Services: 11%	Government-Affiliated: 11%

Vignettes

- In May 2021, a Europe and Eurasia region commercial company attempted to purchase microelectronics from a CC. The commercial company previously attempted to acquire U.S.-origin electronics from a CC by falsifying the end user's information. When the CC denied the request based on the end user's affiliation to a Europe and Eurasia region military, the commercial company changed the end user to a different company. Days later, a different Europe and Eurasia commercial company contacted a CC's European representative requesting the same quantity and type of electronic component.

- From FY20 to FY21, a Europe and Eurasia region state-sponsored cyber actor conducted a complex software supply chain attack. The cyber actor gained access to a network traffic management system tool, SolarWinds Orion, through a compromised (TROJAN) update to the software. The cyber actor used multiple tools, backdoors, and malware implants to compromise thousands of organizations via the supply chain attack. Specifically, the Europe and Eurasia region cyber actor used the patched SolarWinds Orion monitoring tool, which included a SUNBURST backdoor, to compromise a CC's unclassified network. The SUNBURST malware remained undetected from June 2020 to mid-December 2020.

South and Central Asia

Overview

In FY21, the South and Central Asia region was the fourth most active collector of sensitive or classified information and technology, accounting for 15 percent of cleared industry reporting. Historically afflicted with instability, South and Central Asia region remains fraught with regional conflicts, border disputes, and domestic security concerns. Such regional issues—coupled with domestic technological deficiencies—continue to influence South and Central Asia nations to prioritize modernization efforts aimed at enhancing military capabilities, regional defense industries, and even emerging space programs.

South and Central Asia region entities attempted to access restricted U.S. technologies and information coinciding with military modernization priorities—including border security and developing space programs—outlined in national strategies. In FY21, South and Central Asia entities sought access to C4 technologies, accounting for the most reported at 23 percent. Furthermore, there were various reported efforts to acquire C4, software, avionics, and platforms for enhancing UAV defense capabilities for border surveillance and space programs. Finally, entities within the region sought to acquire export-controlled microelectronics—namely monolithic microwave integrated circuits—which are integral to multiple space and defense platforms.

In FY21, more than 66 percent of South and Central Asia region efforts involved individuals seeking employment for cleared positions that potentially would provide access to classified technologies and information. The majority of these employment solicitations were at CCs specializing in the development of software and communications equipment. Separately, and to a much lesser degree, cleared industry reporting revealed South and Central Asia entities contacting CCs attempting to directly acquire or serve as a regional distributor for such export-controlled technologies as communications equipment and UAV platforms.

Top Targeted Technology Categories	Most Reported Methods of Operation	Most Reported Methods of Contact	Most Common Collector Affiliations
C4: 23%	Résumé Submission: 66%	Résumé-Professional: 54%	Individual: 80%
Software: 18%	Attempted Acquisition of Technology: 9%	Email: 12%	Commercial: 13%
Unknown: 14%	Exploitation of Experts: 8%	Résumé-Academic: 11%	Government-Affiliated: 3%

Vignettes

- A South and Central Asia region individual repeatedly sought employment in information technology and communications positions through a CC's website, submitting résumés across multiple months and multiple job postings. The CC develops and maintains a space-capable communications system for the U.S. military.
- A representative from a South and Central Asia region company emailed a CC seeking to purchase a quantity of a specified UAV platform. The representative claimed the end users would be state government agencies within that representative's country, and offered to become a regional distributor for the CCs products.

Western Hemisphere

Overview

In FY21, the Western Hemisphere region continued to be leveraged by threat actors seeking sensitive and classified information and technology resident in the cleared industrial base. Overall, the Western Hemisphere region accounted for 5 percent of the total cleared industry reporting. Industry reporting indicated Western Hemisphere entities targeted a majority of IBTL categories with an emphasis on aeronautic systems, electronics, and software. Entities in this region targeted aeronautic systems focusing on aviation parts, export-controlled items, and proprietary technology. In FY21, incidents targeting electronics focused on microelectronic parts, to include filters for microwave and radio frequency applications.

In FY21, exploitation of cyber operations was the top MO, accounting for 21 percent of Western Hemisphere region reporting. Spearphishing campaigns remained a common cyber activity, while other activities included brute-force attacks, network intrusions, ransomware, social networking, and website exploitation. Additionally, Western Hemisphere collectors used exploitation of insider access, for personal contact and social networking service in 20 percent of the associated incidents. The most noteworthy change in MO occurred with exploitation of experts. Reports involving exploitation of experts mainly consisted of business networking requests and paid consulting opportunities to CCs.

Western Hemisphere region individuals and commercial entities were the most prolific collectors against U.S. technology, collectively accounting for over one-third of all reported attempts; the entities relied heavily on email in these approaches. A number of individual-affiliated requests were attributed to Western Hemisphere entities seeking collaboration opportunities and employment. In FY21, commercial entities most aggressively targeted electronics, aeronautic systems, and software. In some instances, these requests represented an attempt by foreign governments to make contacts seem more innocuous by using non-government entities as surrogate collectors. Conversely, actors from this region could serve wittingly or unwittingly as conduits for other sanctioned nations, as they are being leveraged by seemingly legitimate cover.

Top Targeted Technology Categories	Most Reported Methods Of Operation	Most Reported Methods Of Contact	Most Common Collector Affiliations
Aeronautic Systems: 17%	Exploitation of Cyber Operations: 21%	Email: 26%	Individual: 34%
Electronics: 14%	Exploitation of Insider Access: 15%	Personal Contact: 21%	Unknown: 32%
Unknown: 12%	Exploitation of Experts: 12%	Cyber Operations: 20%	Commercial: 22%

Vignettes

- In 2021, Western Hemisphere region ransomware actors targeted multiple CCs and successfully exfiltrated data pertaining to U.S. manufacturing/designs and microelectronics. Cyber actors likely gained initial access from exploiting remotely accessible accounts/systems, remote desktop protocols, tailored emails containing malicious links and attachments, and virtual desktop infrastructure. State-sponsored actors used common penetration testing tools, to reveal vulnerabilities on the CCs' computer systems and networks, whereby they were able to move laterally to encrypt Exchange/Window servers, standalone desktops, and other devices.

Africa

Overview

In FY21, Africa region entities accounted for the lowest number of attempts to acquire sensitive or classified information and technology resident in the cleared industrial base. Entities from Africa region entities haveconsistently remained the least reported collectors targeting cleared industry since FY17, accounting for only 2 percent of all reporting received from cleared industry. Due to enduring conflicts in the region, such as civil unrest, violent extremism, intercommunal violence, and organized crime, many African countries are seeking access to U.S. information and technologies that can quickly help bolster their internal security capabilities.

Africa region entities targeted less than half of the IBTL technology areas and placed emphasis on software, C4, radars, and armament and survivability systems, acquiring systems and information related to U.S. counter-UAV systems, surveillance radars, rocket-propelled artillery, mobile network scanners, and communications intelligence software. Distinctive from other regions, Africa region entities focused almost exclusively on completed systems in lieu of individual components used to manufacture defense-related technologies.

In FY21, cleared industry reporting attributed to the Africa region indicated résumé submissions, RFI/solicitation, and attempted acquisition of technology were the most commonly used MOs, accounting for nearly 87 percent of all attributed reporting. The majority of individual collectors sought jobs in the information technology and cybersecurity sectors, which could potentially provide access to sensitive or classified data. Additionally, a variety of individual, commercial and government-affiliated entities attempted to acquire or requested information related to export-controlled U.S. technologies on behalf of government and law enforcement organizations to counter ever evolving threats within the region.

Most Targeted Technology Categories	Most Common Methods Of Operation	Most Common Methods Of Contact	Top Collector Affiliations
Software: 18%	Résumé Submission: 48%	Résumé-Professional: 36%	Individual: 68%
Other: 18%	RFI/Solicitation: 34%	Web Form: 18%	Commercial: 11%
C4: 16%	Attempted Acquisition of Technology: 5%	Email: 14%	Government-Affiliated: 11%

Vignettes

- In 2021, a commercial company from Africa region requested a U.S. radar surveillance system on behalf of an Africa region government. The commercial company claimed to provide solutions to fight terrorism within the region.
- In 2021, an Africa region commercial company requested a counter-UAV system. The company claimed to be a cyber-intelligence and information technology company offering solutions to terrorism and security challenges but did not provide an end user for the requested technology.

Industrial Base Technology List

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 levels 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	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 creates, 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 diffractive 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	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.
Services and Other Products	Services and other products not listed above

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 causing 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.
Résumé Submission	Foreign persons submitting résumés 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 or 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

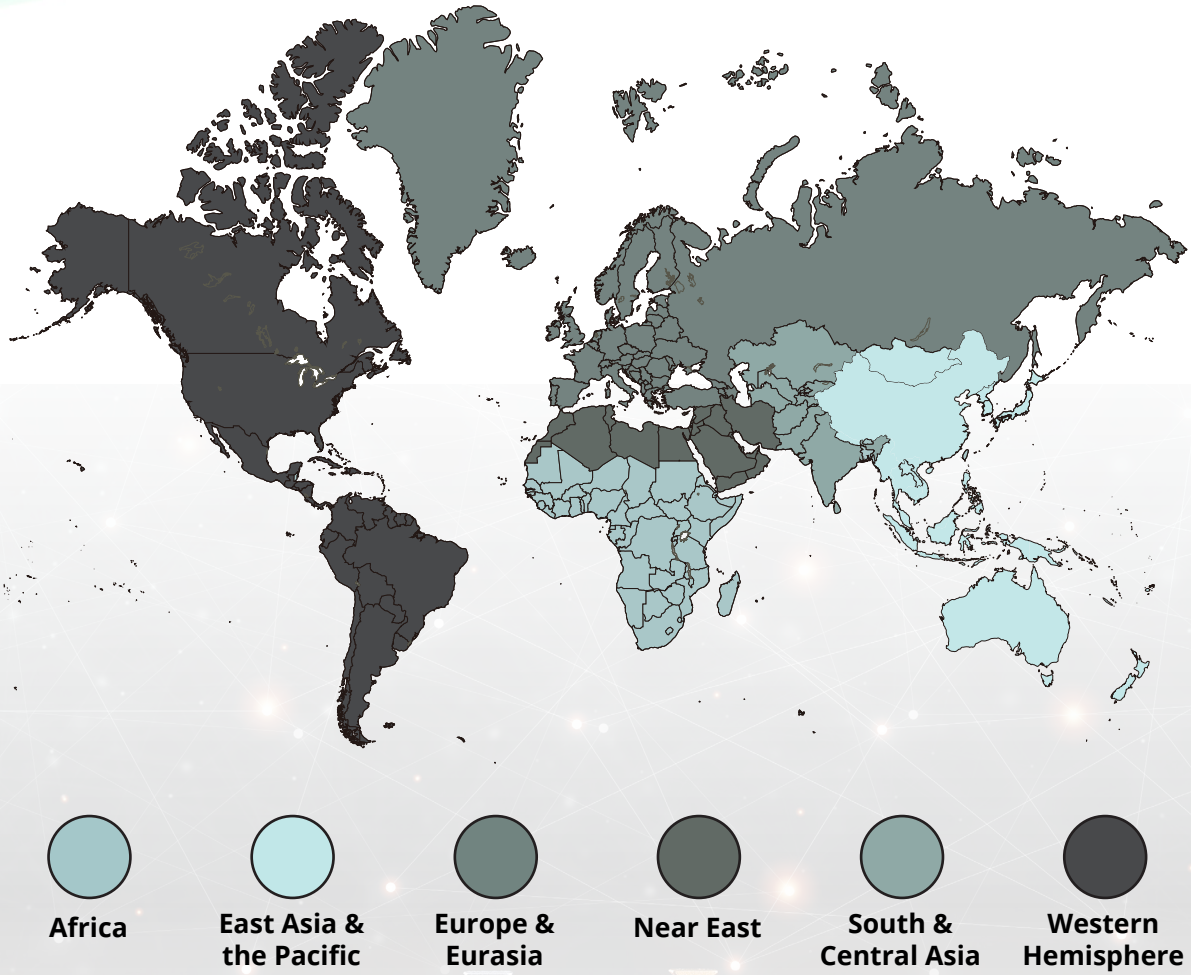
Approaches used to connect the foreign actor to the targeted individual, information, network, or technology in order for the foreign actor to execute the MO(s).

Conferences, Conventions, or 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.
Résumé–Academic	Resume or CV submissions for academic purposes.
Résumé–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.
Telephone	Contact initiated via a phone call by an unknown or unidentified entity.
Web Form	Contact initiated via a company-hosted web submission form.

Collector Affiliation

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.
Individual	Persons who target U.S. information and technologies for financial gain or ostensibly for academic or research purposes.
Unknown	Instances in which no attribution of a connection to a specific end use could be directly made.

Regions Breakdown



Africa	East Asia & the Pacific	Europe & Eurasia	Near East	South & Central Asia	Western Hemisphere
Angola	Australia	Albania	Algeria	Afghanistan	Antigua and Barbuda
Benin	Brunei	Andorra	Bahrain	Bangladesh	Argentina
Botswana	Burma	Armenia	Egypt	Bhutan	Aruba
Burkina Faso	Cambodia	Austria	Iran	India	Bahamas, the
Burundi	China	Azerbaijan	Iraq	Kazakhstan	Barbados
Cameroon	Fiji	Belarus	Israel	Kyrgyzstan	Belize
Cabo Verde	Indonesia	Belgium	Jordan	Maldives	Bermuda
Central African Republic	Japan	Bosnia and Herzegovina	Kuwait	Nepal	Bolivia
Chad	Kiribati	Bulgaria	Lebanon	Pakistan	Brazil
Comoros	Korea, South	Croatia	Libya	Sri Lanka	Canada
Congo, Democratic Republic of the	Korea, North	Cyprus	Morocco	Tajikistan	Cayman Islands
Congo, Republic of the	Laos	Czech Republic	Oman	Turkmenistan	Chile
Cote D'Ivoire	Malaysia	Denmark	Palestinian Territories	Uzbekistan	Colombia
Djibouti	Marshal Islands	Estonia	Qatar		Costa Rica
Equatorial Guinea	Micronesia, Federal States of	Finland	Saudi Arabia		Cuba
Eritrea	Mongolia	France	Syria		Curacao
Ethiopia	Nauru	Georgia	Tunisia		Dominica
Gabon	New Zeeland	Germany	United Arab Emirates		Dominican Republic
Gambia	Palau	Greece	Yemen		Ecuador
Ghana	Papua New Guinea	Holy See			El Salvador
Guinea	Philippines	Hungary			Grenada
Guinea-Bissau	Samoa	Iceland			Guatemala
Kenya	Singapore	Ireland			Guyana
Lesotho	Solomon islands	Italy			Haiti
Liberia	Taiwan	Kosovo			Honduras
Madagascar	Thailand	Latvia			Jamaica
Malawi	Timor-Leste	Liechtenstein			Mexico
Mauritania	Tonga	Lithuania			Nicaragua
Mauritius	Tuvalu	Luxembourg			Panama
Mozambique	Vanuatu	Macedonia			Paraguay
Namibia	Vietnam	Malta			Peru
Niger		Moldova			St. Kitts and Nevis
Nigeria		Monaco			St. Lucia
Rwanda		Montenegro			St. marten
Sao Tome and Principe		Netherlands			St. Vincent and the Grenadines
Senegal		Norway			Suriname
Seychelles		Poland			Trinidad and Tobago
Sierra Leone		Portugal			United States
Somalia		Romania			Uruguay
South Africa		Russia			Venezuela
South Sudan		San Marino			
Sudan		Serbia			
Swaziland		Slovakia			
Tanzania		Spain			
Togo		Sweden			
Uganda		Switzerland			
Zambia		Turkey			
Zimbabwe		Ukraine			
		United Kingdom			

Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134
DCSA.pa@mail.mil
571-305-6562
www.DCSA.mil