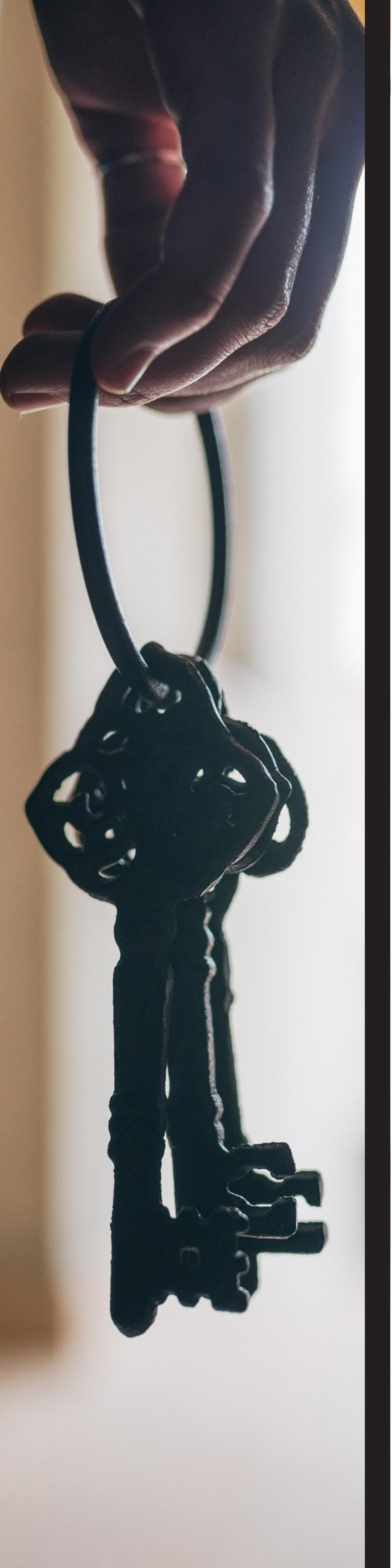
2023

Targeting U.S. Techologies:
A Report of Threats to Cleared Industry

Defense Counterintelligence and Security Agency



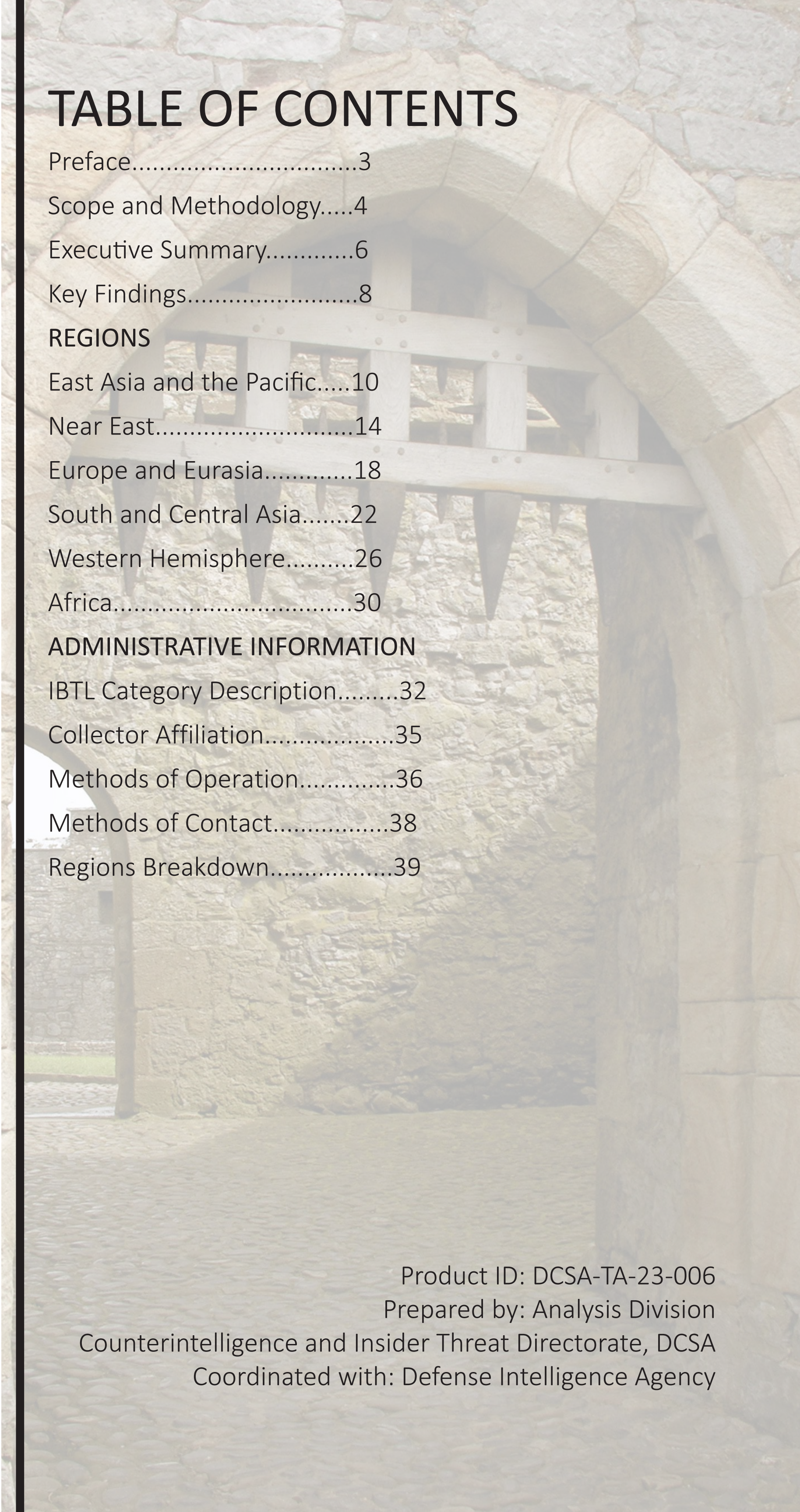


TABLE OF CONTENTS

REGIONS

ADMINISTRATIVE INFORMATION

Product ID: DCSA-TA-23-006
Prepared by: Analysis Division
Counterintelligence and Insider Threat Directorate, DCSA
Coordinated with: Defense Intelligence Agency

PREFACE

With the mission of securing the trustworthiness of the Federal Government's workforce, the integrity of its Cleared Contractor support, and the uncompromised nature of its technologies, services, and supply chains, the Defense Counterintelligence and Security Agency continues to transform to meet the substantially increased threat associated with great power competition. For the first two decades of the 21st century, counterterrorism dominated the strategic landscape. Today, the Nation's most pressing threat comes from near-peer adversaries that target our personnel and industrial base with the goal of competing with or surpassing the United States as the premier economic and military power.

Today's rivalry is far more complex than the 19th century's Great Game, the 20th century's Cold War, or the beginning of the 21st century's War on Terror. It transcends traditional diplomatic and military solutions to yield a full-spectrum contest of powers vying for strategic advantage through diplomacy, military strength, and economic and technological superiority.

The competition is a long game—taking place over decades—as well as a team sport that requires commitment from all sectors of government and industry. This era is complicated by the advent of new technologies, particularly the developing technologies associated with artificial intelligence and the exploitation of near-Earth space. Industrial security sits at the center of a landscape where intellectual property, academic research, and applied research intersect with industrial capacity to develop weapons systems and more general supply chain capabilities that are essential for any sustained conflict. Government and industry must fully cooperate if we are to successfully defend against adversaries who are gaining an advantage by exploiting our free and open society.

In addition, great power competition is an "all weather" sport, in that the threat environment is ever present, dynamic, relentless, and occasionally able to defy prediction. The threats our near-peer adversaries pose to the industrial base come from a variety of avenues, such as cyberattacks, espionage, exploitation of business relationships, insider threats, academia exploitation, intellectual property theft, and supply-chain disruptions. A lack of appreciation of the threat environment along with lack of preparation and urgency in mitigating threats can lead to disastrous outcomes.

This annual assessment provides a critical lens to shape our understanding of the foreign threat to cleared industry. We provide it as an aid for developing, maintaining, and updating security measures to mitigate the risk posed by foreign collectors. Please read it. The complexity of today's full-spectrum conflict requires everyone's effort.

William K. Lietzau
Director
Defense Counterintelligence and Secuirty Agency

Scope and Methodology

Each year the Defense Counterintelligence and Security Agency (DCSA) publishes *Targeting U.S. Technologies: A Report of Threats to Cleared Industry,* in accordance with Department of Defense (DOD) Instruction 5200.39, *Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)*, effective 1 October 2020. The purpose of this assessment is to inform stakeholders on foreign intelligence entity (FIE) efforts to target, compromise, or exploit cleared personnel and/or to obtain unauthorized access to classified information or technologies resident in cleared industry and academia. For widest dissemination, this assessment provides an unclassified snapshot of DCSA findings on the most pervasive actors that targeted U.S. cleared industry and academia in fiscal year (FY) 2022. A more comprehensive view of FIE threats to cleared industry and academia is included in the classified version of this assessment.

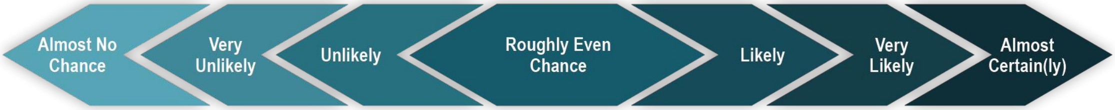
Throughout FY 2022, approximately 12,550 cleared contractor (CC) facilities were required to report suspicious activities in accordance with the 32 Code of Federal Regulations Part 117, *National Industrial Security Program Operating Manual* (NIPSOM). DCSA received and processed suspicious contact reports (SCRs) from cleared industry containing indicators that either likely, very likely, or almost certainly involved an individual—regardless of nationality—attempting to obtain illegal or unauthorized access to a cleared facility, classified information, technology, or compromise a cleared employee. However, DCSA cannot estimate in this forum the volume of suspicious FIE activity that goes unnoticed or unreported by cleared industry or academia.

DCSA organized this assessment by geographic regions, then considered the technology targeted, methods of operation and methods of contact used, and collector affiliation. DCSA evaluated regions based on the number of SCRs received: East Asia and the Pacific, Near East, Europe and Eurasia, South and Central Asia, Western Hemisphere, and Africa. Each regional section addresses the unique sources used and provides different and distinct analysis of the threat to cleared industry. Although DCSA also considered relevant reporting and finished intelligence products from the DOD and the Intelligence Community (IC), SCRs served as the basis for the assessment's threat levels and numeric listing of regional threats to cleared industry. 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.

Expressing Analytic Certainty

Likelihood Array

We base certainty on both likelihood and confidence. Likelihood uses estimative language to express the probability that an event or development will happen.



Almost No Chance

Very Unlikely

Unlikely

Roughly Even Chance

Likely

Very Likely

Almost Certain(ly)

DCSA Confidence Levels

Confidence reflects our assessment of the strength of our analysis and is based primarily on information gaps or assumptions, reasoning, quality and diversity of sources, and the potential for deception.

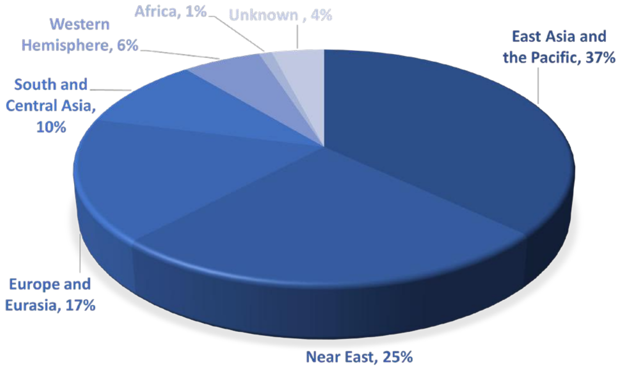
HIGH	MODERATE	LOW
The nature of the issue is knowable	The nature of the issue is knowable or sufficient evidence minimizes uncertainty	The nature of the issue may not be knowable
Well-corroborated information from proven sources	Partially corroborated information from good sources	Uncorroborated information from marginal to good sources
Low potential for deception	Moderate potential for deception	High potential for deception
Non-critical gaps or assumptions	Assumptions or a mix of inferences used to fill potentially critical gaps	Assumptions or mix of inferences used to fill critical information gaps
Undisputed reasoning		

Executive Summary

In FY 2022, DCSA received more than 26,000 SCRs from CC facilities operating as part of the National Industrial Security Program (NISP)—more than an 8-percent increase from FY 2021. Of these, DCSA reviewed and identified thousands of incidents that likely involved foreign entities attempting to illicitly obtain classified information and/or technology resident in cleared industry, or attempts to compromise cleared employees. Throughout FY 2022, foreign entities directed their targeting efforts against various classified U.S. technologies resident within cleared industry, very likely to bypass export restrictions and bolster domestic capabilities. Electronics; software; and command, control, communication, and computers (C4) remained the top three targeted Industrial Base Technology List (IBTL) categories in FY 2022, accounting for 36 percent of all reporting. The other 64 percent of reported collection efforts targeted a variety of technologies covering the remaining 27 IBTL categories.

East Asia and the Pacific and Near East regions remained the most significant collectors of classified U.S. information and technology, collectively accounting for 62 percent of overall SCRs. Entities from these regions continued to target enabling technologies, such as dual-use, export-controlled microelectronics, artificial intelligence (AI) software, quantum technologies, satellite communication systems, and sensors. DCSA attributed 17 percent of SCRs to entities from Europe and Eurasia, as well as South and Central Asia. Entities from Europe and Eurasia focused on obtaining hardware with military applications, which would help modernizing their military capabilities and improve effectiveness on the battlefield. Entities from the Western Hemisphere and Africa collectively accounted for just 7 percent of reported SCRs, and 4 percent were from unknown regions.

FY 2022
Suspicious Contact Reports by Region



Résumé submission was the top method of operation, accounting for 27 percent of reported attempts. Near East, East Asia and Pacific, and South and Central Asia regions accounted for close to 91 percent of reported résumé submissions, including students seeking to conduct postgraduate-level research at U.S. academic centers involved in sensitive or classified research.

East Asia and Pacific, Near East, and Europe and Eurasia entities accounted for 85 percent of all exploitation of business activities reported. Entities in these regions attempted to leverage existing relationships with CCs or sought to establish new business-to-business relationships. Unidentified cyberactors followed by state-sponsored and for-profit cyberactors continued to conduct cyberoperations against cleared industry's unclassified networks and exfiltrate sensitive, defense-related information and data.

Individual entities with no confirmed affiliation accounted for 36 percent of overall reported suspicious contacts, mostly related to résumé submission. Commercial-affiliated entities, mainly from East Asia and the Pacific region, accounted for close to 30 percent of the overall SCRs. On several occasions, commercial collectors offered manufacturing services and requested to serve as overseas distributors for CC's products in regional markets. Government-affiliated entities, mainly from East Asia and the Pacific and Europe and Eurasia regions, accounted for almost 19 percent of overall reporting. Most government-affiliated entities were state-sponsored cyberactors leveraging access to CC's networks to obtain sensitive data about U.S. defense and intelligence programs and capabilities.

Executive Summary

1 East Asia and the Pacific

Top Targeted Technology

Electronics Software C4

Top Methods of Operation

Exploitation of Business Activities · Exploitation of Experts · Résumé

Top Collector Affiliation

Commercial

2 Near East

Top Targeted Technology

Software Electronics Aeronautic Systems

Top Methods of Operation

Résumé · Exploitation of Business Activities · RFI/ Solicitation

Top Collector Affiliation

Individual

3 Europe and Eurasia

Top Targeted Technology

C4 · Aeronautic Systems · Software

Top Methods of Operation

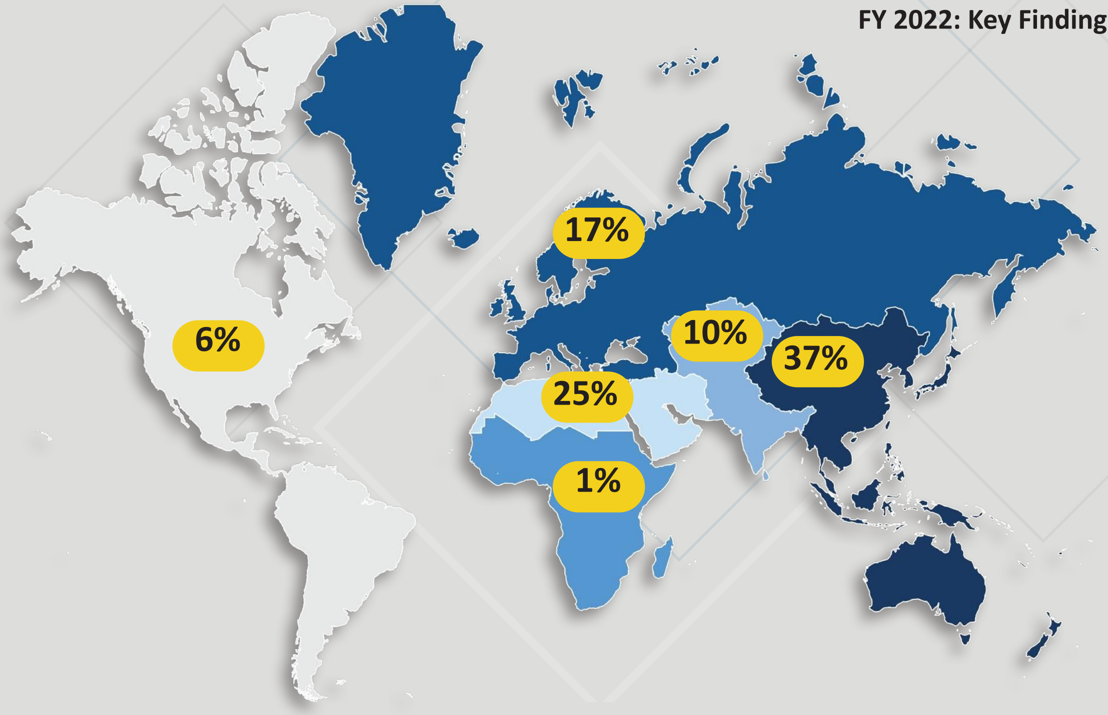
RFI/ Solicitation · Exploitation of Cyber Operations · Exploitation of Business Activities

Top Collector Affiliation

Government Affiliated

Key Findings

FY 2022: Key Findings



East Asia and the Pacific

- Strategic goals and military modernization plans fueled collection attempts aimed at transferring critical and emerging U.S. technology from cleared industry to East Asia and Pacific entities.
- Commercial, individual, and government-affiliated entities from this region continued targeting U.S. technologies, information, and talent within cleared industry, which could be used to spur innovation in defense-related technologies, reduce reliance on foreign technologies, and aid in military power-projection in the region and throughout the world.

Near East

- Entities from this region continued to rely on non-traditional collectors and illicit procurement networks to acquire U.S. information and technology from cleared industry.
- Students and researchers attempted to study and work with cleared academia and federally funded professors.
- Commercial and governmental entities leveraged foreign visits to gain access to U.S. information and technology.

Europe and Eurasia

- Entities from this region continued seeking U.S. information and technology to upgrade defense capabilities through both licit and illicit means, and in violation of export restrictions.
- State-sponsored cyberactors leveraged access to CC's networks and used common and effective tactics to obtain sensitive data about U.S. defense and intelligence programs and capabilities.

South and Central Asia

- Cross-border incursions, airspace violations by drones, and regional military competition proved to be dominant themes across South and Central Asia, informing national priorities in regard to modernization efforts.
- Modernization of aeronautic technologies remained a priority driven by regional competition and informed by a tense climate along national borders and aging aeronautic systems, particularly in South Asia as key powerbrokers modernize aeronautic systems.

Western Hemisphere

- Entities from this region continued seeking classified U.S. information and technology resident in cleared industry, often serving as conduits for foreign threat actors and restricted end users.
- Cyberactors successfully targeted multiple CCs using network intrusions, with some actions resulting in data exfiltration.

Africa

- Internal security challenges and foreign influence very likely were the main driving factors for Africa entities seeking access to sensitive and classified U.S. information and technology resident in cleared industry.
- Entities continued to focus almost exclusively on acquiring complete systems instead of individual components used to manufacture defense-related technology.

East Asia and the Pacific

Overview

In FY 2022, entities from the East Asia and Pacific region continued to be the most prominent threat to U.S. sensitive and classified information resident in cleared industry, accounting for nearly 37 percent of all reporting. The East Asia and Pacific region is laden with regional tension, evident by multiple, long-standing territorial disputes and acts of military aggression, which has led multiple countries in the region to increase their defense budgets and accelerate military modernization projects. Throughout the fiscal year, strategic goals and military modernization plans fueled collection attempts—from both strategic competitors and allies—aimed at transferring critical and emerging U.S. technology from cleared industry to East Asia and Pacific entities. These entities continued targeting U.S. technologies, information, and talent within cleared industry that could be used to spur innovation in defense-related technologies, reduce reliance on foreign technologies, and aid in military power-projection in the region and throughout the world.

East Asia and the Pacific Summary			
Most Targeted Technology Categories	Most Common Methods of Operation	Most Common Methods of Contact	Top Collector Affiliation
Electronics	Exploitation of Business Activities	Email	Commercial
Software	Explotiation of Experts	Résumé-Academic	Government Affiliated
C4	Résumé Submissions	Social Networking Service	Individual

Although some East Asia and Pacific countries remain committed to acquiring U.S. technology deemed necessary to gain global primacy, others sought access to existing and emerging U.S. technologies to support regional security and defense objectives. East Asia and Pacific entities targeted almost all technology areas of the IBTL; however, electronics, software, and C4 ranked as the top three targeted technology categories. East Asia and Pacific entities continued to prioritize targeting enabling technologies that the region is challenged to produce indigenously, such as dual-use, export-controlled microelectronics; AI software; quantum technologies; satellite communication systems; and sensors. East

Asia and Pacific region entities continued efforts to leverage relationships with cleared personnel to gain access to defense-related U.S. technology and information. Exploitation of business activities was the most reported method of operation, which consisted of East Asia and Pacific entities leveraging existing relationships with CCs or seeking to establish new business-to-business relationships. East Asia and Pacific entities also sought to exploit experts in critical and emerging technology fields by encouraging subject matter experts to apply for talent recruitment programs or job opportunities, which would allow East Asia and Pacific countries to enhance innovation. Résumé submission also remained a top method of operation. Academics from East Asia and Pacific countries sought entry into U.S. post-graduate academic programs related to hypersonics, thermodynamics, propulsion, robotics, AI, and signal processing, while maintaining ties to their country through government-sponsored scholarships. Although not a top-reported method of operation, DSCA continued to observe East Asia and Pacific governments leverage state-sponsored and for-profit cyberactors to conduct zero-day exploits, brute-force attacks, web-shell exploits, supply-chain attacks, and spear-phishing campaigns against cleared industry's unclassified networks and exfiltrate sensitive, defense-related information and data.

DSCA observed traditional and non-traditional collection attempts directed against cleared industry. East Asia and Pacific state-owned enterprises, researchers from state-funded universities, business practitioners, students, and foreign diplomats attempted to engage with cleared industry to gain access to U.S. technology and information. Commercial collectors remained the most predominant in FY 2022, collectively accounting for nearly 45 percent of overall reported attempts. Individuals and government-affiliated and individual entities ranked second and third respectively as the most prevalent collectors.

Vignettes

- In February 2022, a presumed student from an East Asia and the Pacific university submitted an unsolicited résumé via email to a CC seeking a research position in quantum computation. The U.S. Department of Commerce sanctioned the university for its role in using quantum computing to support military modernization efforts of an East Asia and Pacific country.
- In November 2021, an East Asia and the Pacific military servicemember visited a CC to attend a conference and asked questions regarding the weaponization of vehicles used in space operations—an unauthorized topic of discussion.
- In October 2021, an East Asia and the Pacific state-sponsored cyberactor exploited a known zero-day vulnerability to gain unauthorized access to a CC's unclassified network. The cyberactor harvested credentials to maintain persistent access to the network to exfiltrate data on directed energy.

Near East

Overview

The Near East region continues to face a series of complex and multifaceted issues, including political tensions, ongoing conflicts, and economic instability. In addition to these issues, there is also a growing trend toward diversification in Near East economies, with several countries in the region pursuing military modernization efforts. One key driver of military modernization is the regional arms race; countries are competing to build up military capabilities to exert regional influence and pursue ambitious foreign policy agendas. This competition is fueled by a range of factors, including geopolitical rivalries, security concerns, and the desire for prestige and influence. As a result, some

Near East Summary			
Most Targeted Technology Categories	Most Common Methods of Operation	Most Common Methods of Contact	Top Collector Affiliation
Software	Résumé Submissions	Résumé-Academic	Individual
Electronics	Explotiation of Business Activities	Foreign Visits	Commercial
Aeronautic Systems	RFI/Solicitation	Résumé-Professional	Government Affiliated

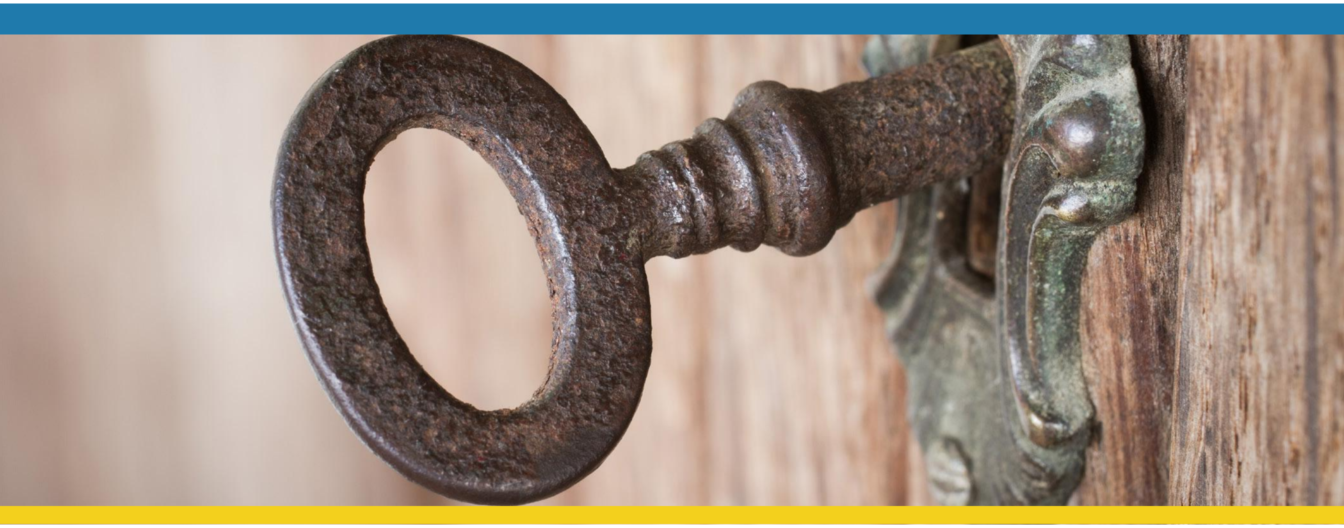
Near East countries are investing heavily in counterterrorism and internal security capabilities, including military hardware, intelligence gathering, and surveillance technologies. To secure these capabilities and technologies, Near East entities continue to rely on non-traditional collectors and illicit procurement networks to acquire U.S. sensitive and classified information to assist in researching and developing their country's defense efforts. According to DCSA FY 2022 cleared industrial reporting, Near East entities targeted nearly every category of the IBTL, with an emphasis on software, electronics, aeronautic systems, manufacturing equipment and manufacturing processes, and armament and survivability to advance scientific, economic, and military modernization developmental goals.

In FY 2022, résumé submission was the most commonly used method of operation, which consisted of graduate and post-graduate students, and post-doctorate researchers seeking positions and opportunities with U.S. cleared colleges and universities and with

DOD federally funded professors. Although many of these academic solicitations could be legitimate attempts to study in the United States, we cannot rule out attempts to exploit academic openness to gain access to sensitive and proprietary information and technology developed in cleared industry. Notably, students/researchers identified in most reporting studied and sought placement in advanced science, technology, engineering, and mathematics (STEM) fields. By pursuing advanced STEM degrees in the United States, Near East students are exposed to cutting-edge research, advanced technologies, and world-class faculty members to prepare them for future employment. In some instances, these students/researchers sought enrollment and employment opportunities that would afford them access to sensitive information and technologies, namely hypersonics, additive manufacturing, radar systems, and AI. Further, gaining knowledge at U.S. academic and research institutions would afford Near East students/researchers the ability to acquire information and expertise that could supplement or support foreign entities' economic and military modernization efforts, beyond what the entities could accomplish indigenously.

Also observed in FY 2022, Near East entities—both commercial and governmental—leveraged foreign visits to CC facilities to gain access to sensitive information and technologies not permitted under agreed-upon visit parameters. Such suspicious activity largely involved circumventing the CC's security protocols, including last-minute roster substitutions, prohibited electronic devices in restricted areas, unauthorized photography, and requested information beyond the scope of the visit.

Vignettes



- In August 2022, a Near East university graduate sought a research position under a cleared U.S. senior engineer who had more than 20 years of experience in materials science. The professor highlighted that the foreign national's curriculum vitae focused on the production of metal matrix composites with a wide range of military uses.
- In August 2022, a Near East university graduate sought a research position under a cleared U.S. senior engineer who had more than 20 years of experience in materials science. The professor highlighted that the foreign national's curriculum vitae focused on the production of metal matrix composites with a wide range of military uses, which indicated that the Near East student was likely leveraging placement in these academic programs to facilitate collection or knowledge transfer of critical information and technology to support the Near East region's military modernization efforts. The professor is a full-time researcher at a U.S. defense-affiliated research center engaged in sensitive research.
- Between January and June 2022, a Maryland-based CC received multiple unsolicited web-card requests for access to a restricted imagery database by a suspected Near East entity who claimed to represent an aviation company in the Near East region—the CC denied all requests. Further research on the Near East aviation company noted that it also attempted to acquire radio frequency and microelectronics technologies for military and aerospace applications from other CCs. This could indicate that the entity was possibly involved in several attempts to procure Export Administration Regulations- and International Traffic in Arms Regulations-controlled defense technologies.

- In January 2022, a cleared industry report revealed that a delegation from a Near East country with a close relationship to the United States visited a CC to discuss upgrading future purchases of airframes with more advanced avionics packages. Prior to the visit, the delegation attempted to make a last-minute substitution to its roster, an observed technique a Near East entity uses to circumvent CC security policies. During the visit, the delegation was agitated when CC employees would not answer inquires that extended beyond the scope of the established visit parameters. Finally, a cleared employee reported that one member of the delegation was observed taking notes on a piece of paper and, when confronted, put the paper in his pocket.

Europe and Eurasia

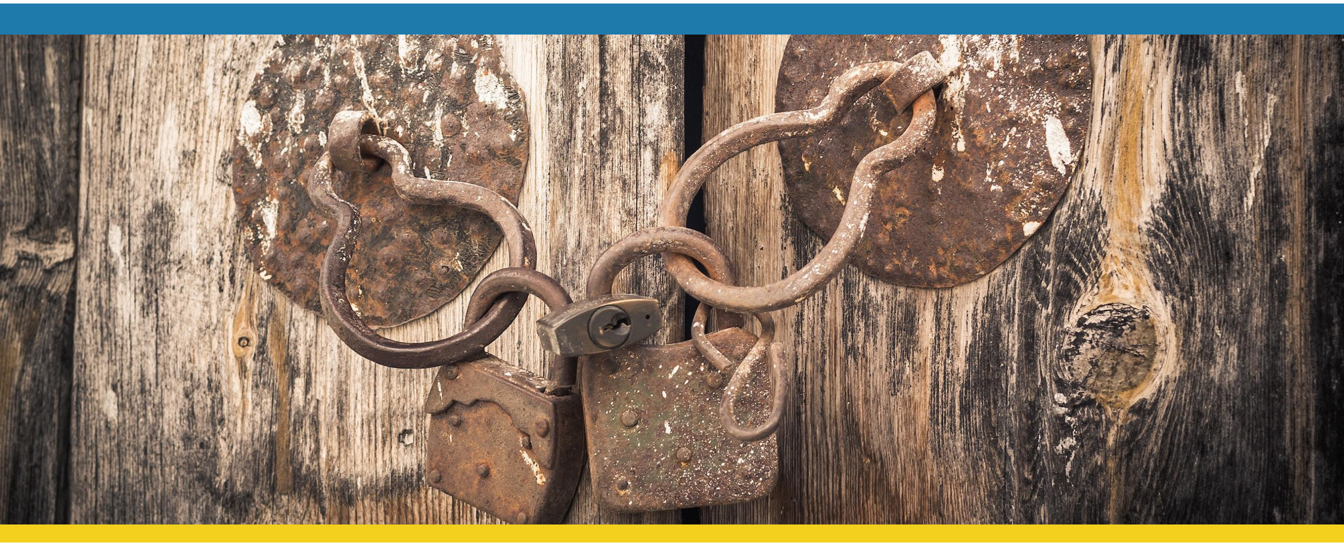
Overview

In FY 2022, Europe and Eurasia entities remained the third most active collectors of sensitive or critical U.S. information and technology resident within cleared industry. Russia's invasion of Ukraine in February 2022 prompted the United States and its global partners to impose sanctions and export controls to target Russia's defense capabilities and its military-industrial complex. The sanctions forced Russia to focus more on using third-nation intermediaries and illicit procurement networks to obtain Western and U.S. technology. In addition, the invasion prompted other Europe and Eurasia nations to reassess defense capabilities and create strategic partnerships, and fueled worldwide defense spending, as countries donated arms to Ukraine and attempted to replenish stocks. As a result, Europe and Eurasia entities continued to seek U.S. information and technology in FY 2022 to achieve these goals through both licit and illicit means, and in violation of export restrictions.

Europe and Eurasia			
Most Targeted Technology Categories	Most Common Methods of Operation	Most Common Methods of Contact	Top Collector Affiliation
Space Systems	RFI/Solicitaiton	Email	Government Affiliated
C4	Exploitation of Cyber Operation	Cyber Operation	Commercial
Services and Other Products	Exploitation of Experts	Web Form	Individual

In FY 2022, entities from Europe and Eurasia targeted a variety of U.S. technologies on the IBTL. In line with regional defense forces' modernization efforts, Europe and Eurasia targeting activities focused on Space Systems, C4, and Services and Other Products. Targeted technologies included hardware with military applications, such as satellite and battlefield communication systems and unmanned aerial vehicles, which would help Europe and Eurasia countries modernize their military capabilities and improve effectiveness on the battlefield. Europe and Eurasia entities primarily used request for information/solicitation, exploitation of cyberoperations, and exploitation of experts to target U.S. information and technologies, accounting for nearly 66 percent of reported incidents. Europe and Eurasia entities with government and commercial affiliation primarily used email and cyber operations in attempts to obtain sensitive U.S. Government information and technology. In addition, most government-affiliated entities were state-sponsored cyberactors leveraging access to CC networks to obtain sensitive data about U.S. defense and intelligence programs and capabilities. As previously observed, Europe and Eurasia state-sponsored cyberactors used common and effective tactics to target networks, including spear phishing, credential harvesting, brute force and password spraying techniques, and known vulnerability exploitation against accounts and networks with weak security.

Vignettes



- In February 2022, an unaffiliated foreign national from the Europe and Eurasia region sent unsolicited emails from his personal account to a CC employee advertising and requesting an evaluation of a computer-aided design software. The CC employee felt the email was suspicious as it contained numerous hyperlinks and a downloadable PDF document. The CC provides engineering software designed for the aerospace and defense industries. The introduction of a third-party software and downloading suspicious attachments could pose a significant threat to the company's network and resident U.S. Government information.
- Beginning in 2017, and culminating after Russia's invasion of Ukraine in 2022, the Russia-based Serniya Engineering facilitated the illicit procurement of dual-use U.S. technology, including microelectronics, from U.S. companies, including cleared industry on behalf of Russia's government. Serniya Engineering used front companies located in Russia, Estonia, Finland, Germany, Hong Kong, Malta, Singapore, Spain, and the UK and operated at the direction of Russia intelligence services to procure millions of dollars' worth of military and sensitive dual-use technologies and components from U.S. companies for Russian end users, in violation of U.S. law, according to the Department of Treasury.
- In FY 2022, Europe and Eurasia state-sponsored cyberactors used brute-force attacks and password spraying and phishing techniques to bypass multi-factor authentication (MFA) and gain access to cleared industry networks running Microsoft 365 environment on Azure Virtual Machines. The cyberactors relied on their Microsoft 365 expertise and used tools native to the environment to further engage in malign activity. The cyberactors were able to successfully guess the password for a dormant

account and enrolled it in MFA with a device the group controls. Once enrolled, the cyberactors used the account to access the organization's VPN infrastructure that was using Azure Active Directory and MFA. The cyberactors used different obfuscation techniques, including Azure Virtual Machines, to reduce the likelihood of detection while mixing administrative actions with malicious ones.

South and Central Asia

Overview

In FY 2022, the South and Central Asia region was the fourth most active collector of sensitive U.S. technology and information, accounting for 9 percent of cleared-industry reporting. Cross-border incursions, drone airspace violations, and regional military competition proved to be dominant themes across South and Central Asia, informing national priorities for modernization efforts. Recent acquisitions of advanced aerospace technology underlined technological acquisition priorities and is driving regional-wide attempts to acquire progressively advanced aerospace platforms in the areas of fixed wing, unmanned aerial vehicle, and space systems.

Entities from South and Central Asia attempted to access restricted U.S. technologies and information in five key categories: aeronautics, software, C4, electronics, and manufacturing, with most attempts related to aeronautic systems, a trend continuing since FY 2021. Modernization of aeronautic technologies remains a priority driven by regional competition, particularly in South Asia as key powerbrokers modernize aeronautic systems and informed by a tense climate along national borders and aging aeronautic systems. South and Central Asia entities sought access to numerous additional classified technologies, including C4, software, electronics, ground vehicle systems, and energy systems. Furthermore, there were various reported efforts to acquire jamming systems and ground-based sensor systems, supporting the intent of entities in South and Central Asia to reinforce border security and prevent regional competition from exploiting contested territory in border areas.

South and Central Asia Summary			
Most Targeted Technology Categories	Most Common Methods of Operation	Most Common Methods of Contact	Top Collector Affiliation
Aeronautic Systems	Résumé Submission	Résumé-Academic	Individual
Software	Exploitation of Business Activity	Résumé-Professional	Commercial
Electronics	Exploitation of Experts	Email	Government Affiliated

Year over year, most South and Central Asia reporting involves individuals seeking employment for cleared positions that potentially could provide access to classified technologies and information; these reports numbered 46 percent in FY 2022 and 66 percent in FY 2021. CCs operating in software, aeronautics, and C4 received most of these requests. Additionally, entities contacted CCs to acquire or serve as distributors for electronic components, mainly circuit boards and other microelectronics.

Vignettes

- A representative of a government in South and Central Asia requested to purchase export-controlled technologies, including signals intelligence collection systems and electronic warfare systems for use by the defense industry of that country. The CC did not approve this request as the technology was not authorized for export.
- A CC's corporate computer system was infected with malware when CC representatives traveled to service the defense equipment owned by a South and Central Asia region military. The CC's computer plugged into the defense equipment to retrieve system data and malware prepared on the defense equipment transferred to the computer system. The CC cyber response team identified the malware intrusion and prevented further infection.
- An individual in South and Central Asia masking themselves as a U.S. person contacted a CC requesting to purchase export-controlled, NSA-certified signals encryption equipment. Through the CC's due diligence, this individual was identified as a potential member of a foreign government, therefore the export request was not approved.

Western Hemisphere

Overview

In FY 2022, Western Hemisphere entities continued seeking sensitive U.S. information and technology, often on behalf or at the behest of sanctioned foreign threat actors. Most incidents from the Western Hemisphere region involved cyberactors, followed by global companies with representatives in the United States, and individuals from foreign countries seeking to establish business relations with a cleared contractor (CC) or a transactional relationship with cleared employees. Actors from this region often knowingly, or otherwise, served as conduits for restricted foreign end users. Western Hemisphere entities targeted most IBTL categories, with emphasis on C4 and electronics. Specific C4 technologies targeted included telecommunication devices, information technology equipment, computer facilities, and data centers, whereas electronics technologies included microelectronic parts, such as semiconductors and integrated circuits. The top method of operation was exploitation of cyber operations, accounting for more than a quarter of Western Hemisphere region reporting. Most cyber operations were perpetrated by commercially affiliated entities using network intrusions, malware, ransomware, and vulnerability exploits to target cleared industry's networks and personnel. Consistent with FY 2021, Western Hemisphere entities also used exploitation of experts through social networking services and email. Most of these incidents involved Western Hemisphere region representatives working on behalf of third-party international firms offering paid consultations and requesting proprietary or sensitive information.

Western Hemisphere			
Most Targeted Technology Categories	Most Common Methods of Operation	Most Common Methods of Contact	Top Collector Affiliation
C4	Exploitation of Cyber Activity	Cyber Operations	Commercial
Electronics	Exploitation of Experts	Email	Individual
Aeronautic Systems	Exploitation of Business Activities	Résumé-Professional	Government Affiliated

Commercial entities and individuals were the most prolific Western Hemisphere region collectors of U.S. information and technology. Western Hemisphere region entities attempted to establish or exploit relationships with cleared employees requesting their expertise for paid consultancies, seeking business development opportunities, or expressing investment interest, likely in attempts to exploit business activities. In addition, there were various attempts by Western Hemisphere region individuals—not affiliated with the United States—seeking employment at CCs specializing in sensor and signals intelligence equipment and satellite communications.

Vignettes

- In April 2022, Western Hemisphere cyberactors successfully targeted multiple CCs using network intrusions, with some actions resulting in data exfiltration. Cyberactors, mostly with a commercial affiliation, gained unauthorized access to networks and encrypted servers. In one instance, CC Internet Protocol (IP) addresses were observed making network connections to a known malicious IP address. The cyberactor executed environmental discovery commands to establish malicious scheduled tasks. On at least two occasions involving network intrusions, cyberactors exploited zero-day vulnerabilities to exfiltrate data, impacting the CC's ability to provide critical operational support to U.S. Government customers.
- In June 2022, during a defense industry conference, a representative from a Western Hemisphere company with distributors in the United States aggressively sought proprietary information from a CC employee in attendance. Throughout the conversation, the representative asked the employee several times to identify specific technology the CC would be working on.

Africa

Overview

In FY 2022, Africa remained the least active region in targeting sensitive or classified U.S. information and technology resident in cleared industry. Reporting related to this region accounted for less than 1 percent of all activity received from cleared industry. Internal security challenges caused by longstanding ethno-national conflict, civil unrest, drug trafficking, maritime piracy, and violent extremism very likely are the main driving factors for Africa entities to seek access to U.S. information and technology.

Africa entities targeted a limited number of IBTL categories (placing an emphasis on services and other products, C4, electronics, and software), in attempts to acquire commerial communication and electronic warfare devices and software to improve domestic security and defense capabilities. Africa entities continued to focus almost exclusively on acquiring complete systems instead of individual components used to manufacture defense-related technology.

Africa Summary			
Most Targeted Technology Categories	Most Common Methods of Operation	Most Common Methods of Contact	Top Collector Affiliation
C4	Résumé Submissions	Web Form	Individual
Electronics	RFI/Solicitation	Résumé-Professional	Government Affiliated
Software	Exploitation of Business Activities	Email	

The most common methods of operation used by Africa entities in FY 2022 included résumé submission, request for information/solicitation, and attempted acquisition of technology. Most the résumé submissions were for positions at cleared contractors (CCs) specializing in C4 and electronics, which could provide access to sensitive or classified U.S. Government information. A variety of individual- and government-affiliated entities attempted to acquire export-controlled technology on behalf of defense and security forces to counter regional threats.

Vignettes

- In April 2022, an unaffiliated individual from the Africa region applied for a cleared position with a CC specializing in military satellite systems. The individual disclosed that they were formerly employed as a software developer with an intelligence service from a country in the Africa region.
- In October 2021, a company from the Africa region submitted a web form inquiry to a CC requesting information on export-controlled, vehicle-mounted radio frequency jammers intended to protect convoys against improvised explosives devices. The individual claimed his company was sourcing products for the country's presidential office. The company also has business partnerships with several East Asia and Pacific companies specializing in high-impact protective materials, products, and technology, which support a military in the East Asia and Pacific region.

Administrative Information

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, communications, 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. 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.

RADAR

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.

SERVICES AND OTHER PRODUCTS

Services and other products not listed above.

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.

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 attachés, foreign liaison officers, 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 targets 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.

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 the following:

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, and 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

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, and 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 Methods of Operation (MOs).

CONFERENCES, CONVENTIONS, OR TRADE SHOWS

Contact regarding or initiated during an event, such as a conference, convention, exhibitions, or trade show.

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-opted is in direct or indirect contact with the target.

CONFERENCES, CONVENTIONS, OR TRADE SHOWS

Contact regarding or initiated during an event, such as a conference, convention, exhibitions, or trade show.

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-opted 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

Résumé or CV submissions for academic purposes.

RÉSUMÉ – PROFESSIONAL

Résumé 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.

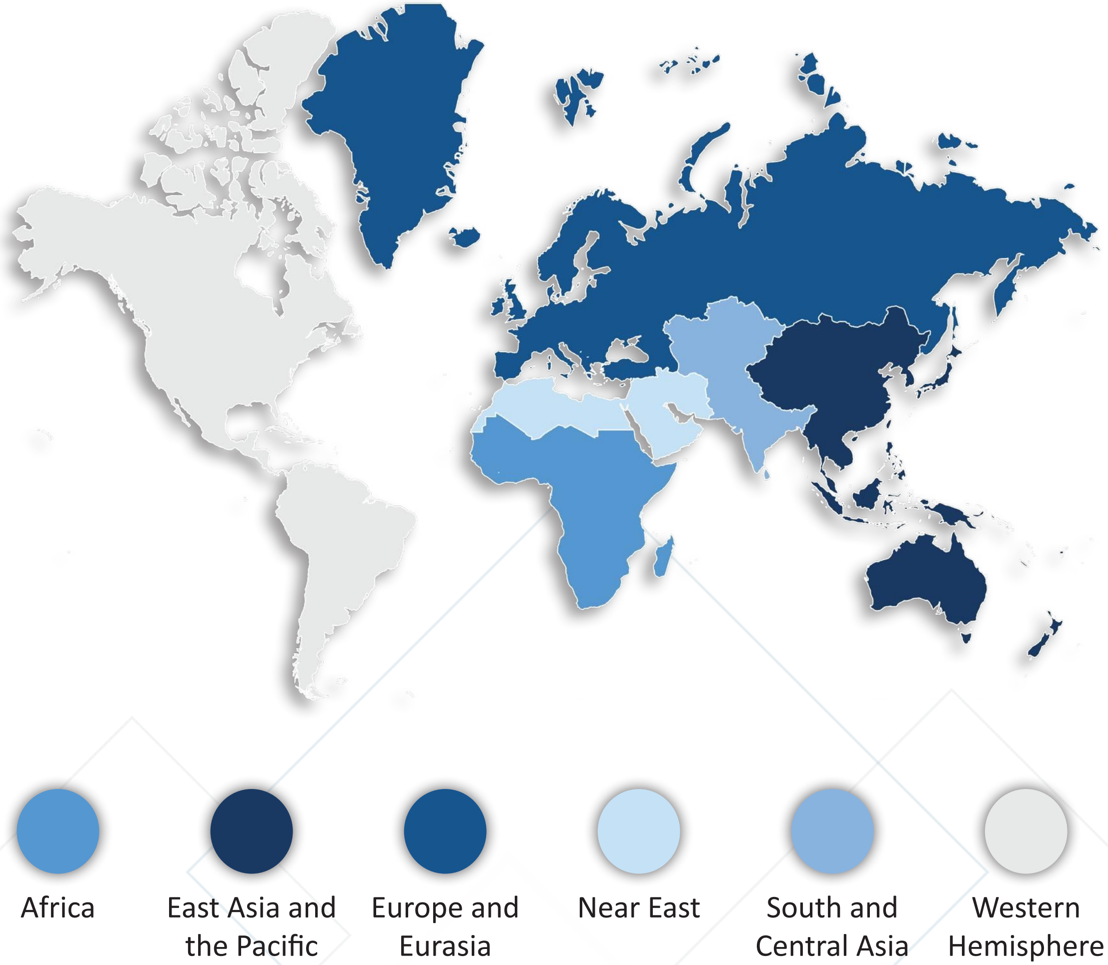
TELEPHONE

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

WEB FORM

Contact initiated via a company-hosted web submission form.

Region Breakdown



Country List

Africa	East Asia and the Pacific	Europe and Eurasia	Near East	South and Central Asia	Western Hemisphere
Angola	Australia	Albania	Algeria	Afghanistan	Antigua and Barbuda
Benin	Brunei	Andorra	Bahrain	Bangladesh	Argentina
Botswana	Burma	Armenia	Egypt	Bhutan	The Bahamas
Burkina Faso	Cambodia	Austria	Iran	India	Barbados
Burundi	China	Azerbaijan	Iraq	Kazakhstan	Belize
Cabo Verde	Fiji	Belarus	Israel	Kyrgyzstan	Bolivia
Cameroon	Indonesia	Belgium	Jordan	Maldives	Brazil
Central African Republic	Japan	Bosnia and Herzegovina	Kuwait	Nepal	Canada
Chad	Kiribati	Bulgaria	Lebanon	Pakistan	Chile
Comoros	Laos	Croatia	Libya	Sri Lanka	Colombia
Côte d’Ivoire	Malaysia	Cyprus	Morocco	Tajikistan	Costa Rica
Democratic Republic of the Congo	Marshall Islands	Czechia	Oman	Turkmenistan	Cuba
Djibouti	Micronesia	Denmark	Palestinian Territories	Uzbekistan	Dominica
Equatorial Guinea	Mongolia	Estonia	Qatar		Dominican Republic
Eritrea	Nauru	Finland	Saudi Arabia		Ecuador
Eswatini	New Zealand	France	Syria		El Salvador
Ethiopia	North Korea	Georgia	Tunisia		Grenada
Gabon	Palau	Germany	United Arab Emirates		Guatemala
Ghana	Papua New Guinea	Greece	Yemen		Guyana
Guinea	Philippines	Holy See			Haiti
Guinea-Bissau	Indonesia	Hungary			Honduras
Kenya	Singapore	Iceland			Jamaica
Lesotho	Solomon Islands	Ireland			Mexico

Africa	East Asia and the Pacific	Europe and Eurasia	Near East	South and Central Asia	Western Hemisphere
🟦	🟦	🟦	🟦	🟦	⬜
Liberia	South Korea	Italy			Nicaragua
Madagascar	Taiwan	Kosovo			Panama
Malawi	Thailand	Latvia			Paraguay
Mali	Timor-Leste	Liechtenstein			Peru
Mauritania	Tonga	Lithuania			Saint Kitts & Nevis
Mauritius	Tuvalu	Luxembourg			Saint Lucia
Mozambique	Vanuatu	Malta			Saint Vincent and the Grenadines
Namibia	Vietnam	Moldova			Suriname
Niger	Fiji	Monaco			Trinidad and Tobago
Nigeria		Montenegro			Uruguay
Republic of the Congo		Netherlands			Venezuela
Rwanda		N. Macedonia			
Sao Tome and Principe		Norway			
Senegal		Poland			
Seychelles		Portugal			
Sierra Leone		Romania			
Somalia		Russia			
South Africa		San Marino			
South Sudan		Serbia			
Sudan		Slovakia			
Tanzania		Slovenia			
Togo		Spain			
Uganda		Sweden			
Zambia		Switzerland			
Zimbabwe		Turkey			
		Ukraine			
		United Kingdom			

Defense Counterintelligence and Security Agency
27130 Telegraph Road
Quantico, VA 22134
DCSA: https://www.dcsa.mil