

2024



Targeting U.S. Technologies

A Report of Threats to Cleared Industry



Warnings:

This product may contain information associated with United States Persons as defined by Executive Order 12333 and Department of Defense Manual 5240.01. Such information should be handled and protected in accordance with applicable Intelligence Oversight rules by persons and organizations subject to those rules. DCSA collects, retains, and disseminates United States Persons Information in accordance with all applicable laws, directives, and policies. Should you require minimized United States Persons Information, contact the DCSA Intelligence Oversight officer, Commercial: 571-305-6592.

Product ID: DCSA-TA-25-001

Date of Information: 20230930

Date of Publication: 20241114

Prepared by: Defense Counterintelligence and Security Agency, Office of Counterintelligence, Analysis Division

For questions, please contact us on NIPR at: dcsa.quantico.dcsa-hq.list.ci-analysis-division@mail.mil; on SIPR at: dcsa.quantico.dcsa-hq.list.ci-analysis-division@mail.smil.mil; or on JWICS at: DCSAMCBQuanticoDCSAHQLISTCIAAnalysisDivision@dss.ic.gov.

We appreciate all consumer input and feedback.



Targeting U.S. Technologies

A Report of Threats to Cleared Industry

TABLE OF CONTENTS

Preparatory Information	
Preface	5
Scope and Methodology	6
Executive Summary	8
Regions	
East Asia and the Pacific	12
Near East	16
Europe and Eurasia	20
South and Central Asia	22
Western Hemisphere	24
Africa	26
Special Focus Area	28
Administrative Information	
IBTL Category Descriptions	30
Collector Affiliation	33
Methods of Operation	33
Methods of Contact	34
Country List	36
Region Breakdown	39



Preface

In the ever-evolving foreign intelligence threat landscape, the Defense Counterintelligence and Security Agency (DCSA) stands as a gatekeeper, guarding against foreign intelligence threats that transcend borders and apply diverse, novel collection means. The foreign intelligence threat environment, much like the strategic environment, is increasingly complex and interconnected. DCSA, other U.S. Government agencies, and industries involved in the Defense Industrial Base (DIB) must remain informed and adaptive to counter and mitigate these intelligence collection threats.

Foreign intelligence collectors apply a wide array of methods across a growing spectrum of means to access information. This includes exploiting non-traditional collection methods such as commercial ventures and leveraging social media in coordination with cyberspace operations and traditional intelligence collection methods. To combat this complex, interconnected, and coordinated intelligence threat, we must be aware of current collection methods and adversaries' avenues to access information to enact stout security protocols.

As the leading nation in technology and manufacturing innovation, foreign adversaries and economic competitors target U.S. research and development facilities, production facilities, and personnel to create shortcuts in developing and manufacturing competing products. Acquiring information without expending time and cost on research and development provides a considerable market advantage to foreign competitors and allows potential adversaries to counter or negate the battlefield benefits of our technology advantage.

DCSA has unique access to cleared facilities and a singular role in assessing and reporting the foreign intelligence threat to cleared facilities. This assessment details the depth and breadth of the most virulent collectors targeting U.S. technologies. Along with sharing information with the Intelligence Community, Department of Defense (DoD), and other U.S. Government agencies, DCSA publishes this product to aid cleared industry in establishing and maintaining effective security programs to protect technology, classified information, facilities, and personnel.

David Cattler
Director
Defense Counterintelligence and Security 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 (IAW) *Department of Defense Instruction 5200.39, Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)*, dated 1 October 2020. The purpose of this assessment is to inform stakeholders of foreign intelligence entity (FIE) efforts to target, compromise, or exploit cleared personnel and/or obtain unauthorized access to classified information or technologies resident in cleared industry and academia. This assessment provides an unclassified snapshot of DCSA findings on the most pervasive actors targeting cleared industry and academia in fiscal year (FY) 2023. The classified version of this assessment offers a more comprehensive view of FIE threats to cleared industry and academia.

Throughout FY 2023, approximately 12,800 cleared contractor (CC) facilities were required to report suspicious contacts to DCSA IAW *32 Code of Federal Regulation Part 117, National Industrial Security Program Operating Manual*. DCSA received and processed suspicious contact reports (SCRs) from cleared industry containing indicators that 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, classified technology, or to compromise a cleared employee. DCSA cannot estimate the volume of suspicious FIE activity gone unnoticed or unreported by cleared industry or academia.

We organized this assessment by geographic regions, targeted technology, methods of operation (MOs) and methods of contact (MCs) used, and collector affiliation. DCSA evaluated regions on the basis of 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 sources used and provides different and distinct analysis of the threat to cleared industry. Although DCSA considered relevant reporting and finished intelligence (FINTEL) products from the Department of Defense (DoD) and 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 continues to improve accuracy of analysis and threat levels addressed in DCSA annual assessments.

Expressing Analytic Uncertainty

Uncertainty is based on both likelihood and confidence. The following terms of likelihood express the probability that an event or development will happen. Likelihood uses estimative language to express the probability that an event or development will happen.

ICD 203 Expressions of Likelihood or Probability						
DCSA Standard	Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely
	01 to 05%	05 to 20%	20 to 45%	45 to 55%	55 to 80%	80 to 95%
	Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable
Almost Certain(ly)						
95 to 99%						
Nearly Certain						
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.						
Low		Moderate		High		
- Limited, uncorroborated, or dated information from unknown source reliability - Contradictory reporting - High potential for deception - Highly complex, rapidly evolving, dynamic situation with multiple issues or actors - Filling remaining gaps has the potential to substantially affect major judgments		- Partially corroborated information from reliable sources - Some ambiguity from reporting - Some potential for deception - Complicated situation with multiple issues or actors; some previous examples that are well understood - Filling remaining gaps has the potential to affect major judgments		- Well-corroborated, credible information from reliable sources - Minimal contradictory reporting - Low potential for deception - Routine situation that is well understood - Filling remaining gaps will have little impact on major judgments		

Executive Summary

Executive Summary
Collector Region
East Asia and the Pacific
Near East
Europe and Eurasia
Targeted Technology
Services and Other Products
Software
Electronics
Method of Operation
Résumé Submission
RFI/Solicitation
Exploitation of Business Activities
Method of Contact
Email
Résumé — Academic
Résumé — Professional

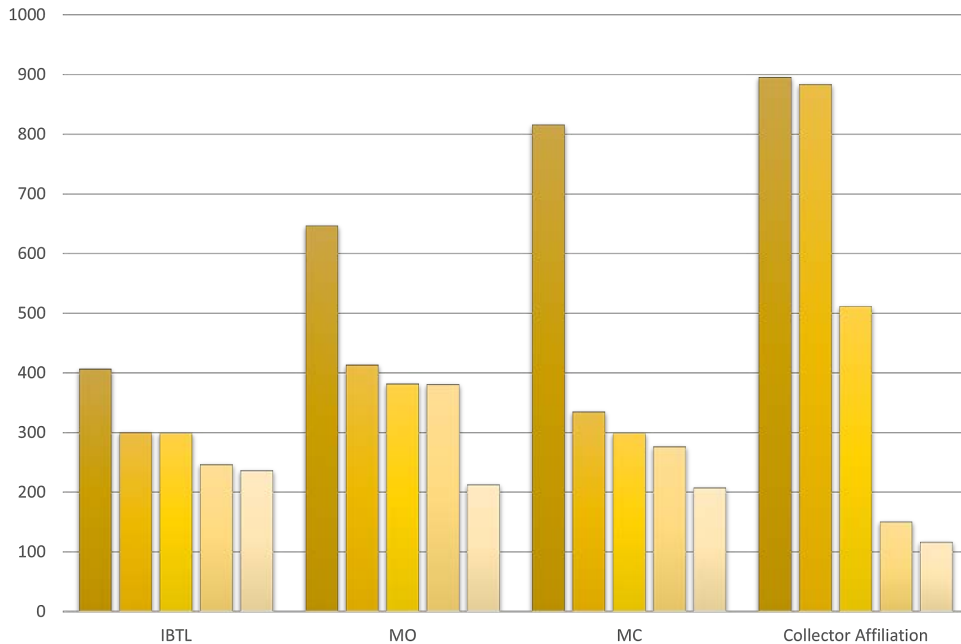
In fiscal year (FY) 2023, DCSA received more than 28,000 suspicious contact reports (SCRs) from cleared contractor (CC) facilities operating as part of the National Industrial Security Program (NISP)—more than a seven percent increase from FY 2022. DCSA reviewed and identified thousands of incidents that likely involved foreign entities attempting to illicitly obtain classified information or classified technology in cleared industry. Entities also attempted to circumvent sanctions or compromise cleared employees. Throughout FY 2023, foreign entities directed targeting efforts against various classified and enabling U.S. technologies resident within cleared industry to bypass export restrictions and bolster domestic capabilities. The top three targeted Industrial Base Technology List (IBTL) categories in FY 2023, software, electronics and aeronautic systems, accounted for 34 percent of all reporting. The other 66 percent of reported collection efforts targeted a variety of technologies, covering the remaining IBTL categories.

East Asia and the Pacific and Near East regions remained the most significant collectors of classified and sensitive U.S. information and technology, collectively accounting for 62 percent of overall SCRs. Entities from these regions continue to target enabling technologies, such as export-controlled microelectronics devices, modeling and simulation software, additive manufacturing, and artificial intelligence (AI) software. DCSA attributed 26 percent of SCRs to entities from Europe and Eurasia and South and Central Asia.

Entities from Europe and Eurasia focused on microelectronics and advanced communications

Executive Summary

Number of Reports FY23



% of Reporting FY23

Targeted Technology		Methods of Operation		Methods of Contact		Collector Affiliation	
Services and Other Products	16%	Résumé Submission	25%	Email	32%	Individual	35%
Software	12%	RFI/ Solicitation	16%	Résumé — Academic	13%	Commercial	34%
Electronics	12%	Exploitation of Business Activities	15%	Résumé — Professional	12%	Government — Affiliated	20%
Aeronautic Systems	10%	Exploitation of Experts	15%	Web Form	11%	Unknown	6%
C4	9%	Exploitation of Cyber Operations	8%	Cyber Operations	8%	Government	5%

Executive Summary

computer systems to support their military industrial complex and alleviate technological shortcomings and obstacles.

Entities from the Western Hemisphere and Sub-Saharan Africa collectively accounted for just eight percent of reported SCRs; four percent were from unknown regions.

Résumé Submission was the top method of operation (MO), accounting for 25 percent of reported attempts. East Asia and the Pacific and Near East regions accounted for close to 75 percent of reported résumé submissions, consisting of undergraduate, doctoral, and post-graduate researchers seeking opportunities within U.S. cleared academic institutions, in some instances under the tutelage of cleared federally funded professors. Although many academic solicitations may be legitimate attempts to study in the United States, DCSA cannot rule out attempts to exploit academic openness to gain access to sensitive information and technology developed in cleared industry and academia. Near East students/researchers studied and sought placement in advanced science, technology, engineering, and math (STEM) fields. By pursuing advanced STEM degrees in the United States, Near East students are exposed to cutting-edge, advanced technologies and cleared professors engaged in sensitive research.

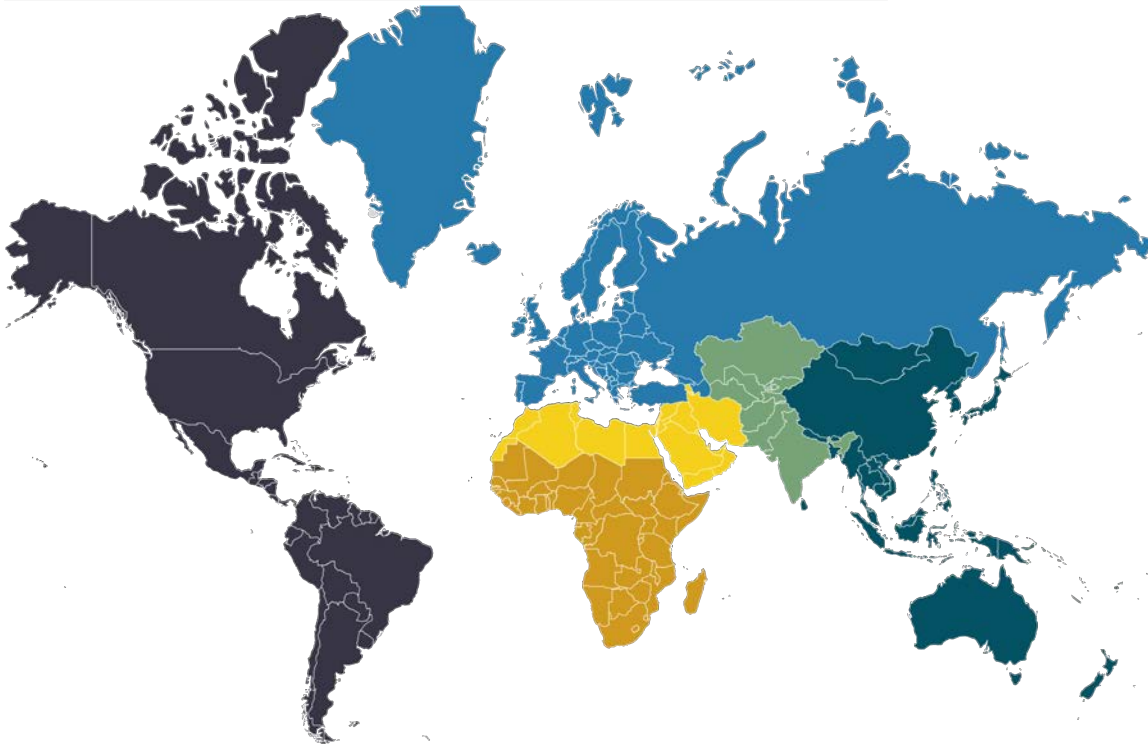
Europe and Eurasia and South and Central Asia entities accounted for almost 40 percent of all Requests for Information (RFIs)/Solicitation reported. Entities in these regions sought access to a restricted satellite imagery database, controlled scientific documents,

and collaboration on defense technologies. Unidentified cyberactors, led the onslaught, followed by state-sponsored and for-profit cyberactors. These entities continued to conduct cyberoperations to obtain sensitive data about U.S. defense and intelligence programs and capabilities.

Individual entities with no confirmed affiliation accounted for 35 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 48 percent of overall SCRs. On several occasions, commercial entities sought to establish new business-to-business relationships with cleared companies. Entities attempted exploitation via email or at conferences, conventions, or tradeshows or attempted to exploit existing relationships. They also violated security protocols during foreign visits. Government-affiliated entities, mainly from East Asia and the Pacific and Europe and Eurasia regions, accounted for almost 14 percent of overall reporting. Most government-affiliated entities were state-sponsored cyberactors conducting network scanning, spear-phishing attempts, data exfiltration, and compromising credentials to target sensitive information stored on CC computer networks.

Executive Summary

Summary of Collector Regions					
East Asia and the Pacific	38%	South and Central Asia	8%	Africa	2%
Near East	24%	Western Hemisphere	6%		
Europe and Eurasia	18%	Unknown	4%		



East Asia and the Pacific

Targeted Technology	Method of Contact	Method of Operation	Collector Affiliation
Electronics	Email	Exploitation of Experts	Commercial
Services and Other Products	Web Form Submissions	Exploitation of Supply Chain	Government — Affiliated
Software	Social Networking Services	RFI/Solicitation	Individual

OVERVIEW

East Asia and Pacific region entities continued to target U.S. technologies, information, and personnel within cleared industry to meet national strategies and initiatives. These entities aim to achieve economic, technological, and military modernization goals. Ongoing territorial disputes were a major factor as allies and adversaries sought access to emerging and enabling U.S. technologies to enhance military platforms to aid in power projection or deter military aggression. New and existing U.S. export controls restricted end-users in the East Asia and Pacific region from accessing dual-use and sensitive U.S. technologies. East Asia and Pacific entities primarily relied on non-traditional collectors, such as business practitioners, researchers, students, and government-affiliated cyberactors, to gain access to U.S. defense-related information and technologies.

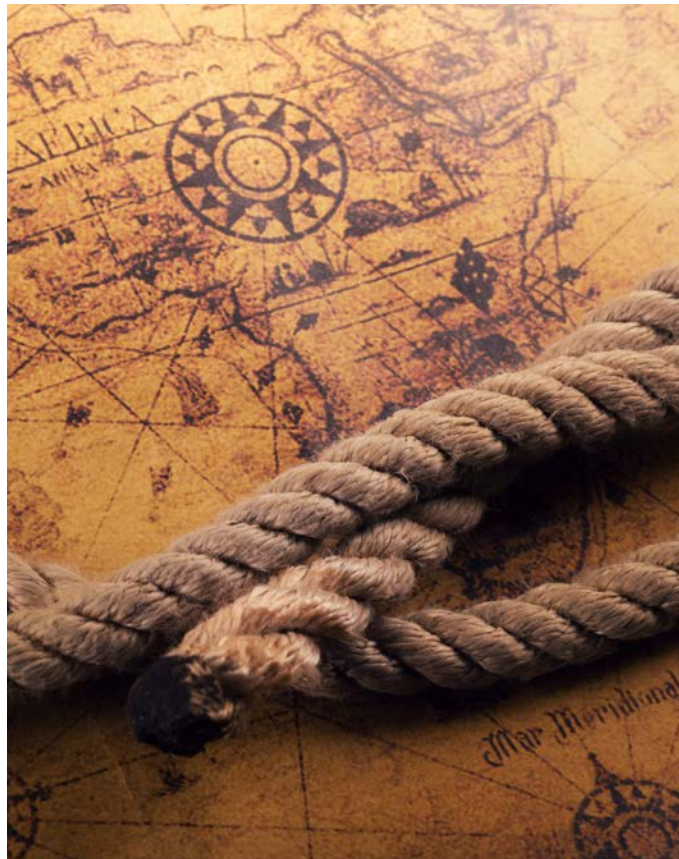
In fiscal year (FY) 2023, East Asia and Pacific region entities continued to be the most prominent threat to U.S. sensitive and classified information resident in cleared industry, accounting for 38 percent of all Defense Counterintelligence and Security Agency (DCSA) reporting received from

cleared industry. During FY 2023, East Asia and Pacific region entities targeted almost all technology areas of the Industrial Base Technology List (IBTL); however, electronics; software; command, control, communication, and computers (C4); manufacturing equipment and processes; optics; and aeronautics ranked as the top-targeted technology areas. East Asia and Pacific entities continued to focus on enabling technologies to meet short-term defense modernization goals and emerging technologies supporting innovation to meet long-term goals. East Asia and Pacific region entities attempted to acquire U.S. enabling technologies, such as export-controlled microelectronic devices, modeling and simulation software, radars, underwater acoustic sensors, and advanced materials used to improve existing defense platforms. East Asia and Pacific region entities also attempted to recruit U.S. subject matter experts (SMEs) in critical and emerging technology fields such as artificial intelligence (AI)/machine learning, quantum technologies, semiconductors, optics, hypersonics, and energy systems.

East Asia and Pacific region entities employed various methods of operations (MOs): Exploitation of Supply Chain, Exploitation of



Experts, Exploitation of Business Activities, Résumé Submission, and Exploitation of Cyber Operations were most associated with non-traditional collectors. Business practitioners representing commercial entities sought to establish new business-to-business relationships with cleared companies via email or at conferences, conventions, or trade shows or attempted to exploit existing relationships by violating security protocols during foreign visits. Commercial companies attempted to procure export-controlled U.S. technologies and materials on behalf of restricted government end-users in the originating country or act as intermediaries for third countries. Researchers and students from East Asia and Pacific region government-affiliated universities or receiving East Asia and Pacific region government scholarships sought to conduct defense-related research at U.S. universities. Exploitation of Cyber Operations consisted of government-affiliated cyberactors conducting network scanning, spear phishing attempts, data exfiltration, and compromising credentials to target sensitive information stored on cleared contractor (CC) computer networks.



East Asia and the Pacific — Vignettes

- In FY 2023, an East Asia and Pacific region consulting firm attempted to recruit CC employees in conjunction with an East Asia and Pacific talent recruitment plan designed to facilitate technology transfer. This consulting firm targeted researchers with notable achievements in science and engineering. The recruitment attempts advertised expedited visa services, annual salary, living accommodations, project funding, post-retirement welfare benefits, and school placement for researchers with children.
- In FY 2023, East Asia and Pacific region cyberactors gained unauthorized access and successfully compromised a CC. Cyberactors compromised the credentials of a general user associated with the CC and used the compromised credentials to initiate a successful virtual private network (VPN) login and bypass weaker two factor authentication on the VPN. Historically, actors maintain persistent access to networks through compromised credentials.
- In FY 2023, an East Asia and Pacific region defense agency asked detailed questions regarding equipment used on a weapons system that fell outside the CC's technical assistance agreement while conducting a foreign visit at the cleared facility. The East Asia and Pacific region defense agency has a history of violating security protocols during foreign visits at CC facilities.
- In FY 2023, an East Asia and Pacific region student requested an International Traffic in Arms Regulation (ITAR)-controlled radar system. The East Asia and Pacific region university is heavily involved in defense-related research for the East Asia and Pacific region government.



Near East

Targeted Technology	Method of Contact	Method of Operation	Collector Affiliation
Services and Other Products	Résumé — Academic	Résumé Submissions	Individual
Aeronautic Systems	Résumé — Professional	Exploitation of Business Activities	Commercial
Manufacturing Equipment and Processes	Foreign Visits	RFI/Solicitation	Government — Affiliated

OVERVIEW

In FY 2023, Near East region entities continued to leverage similar MOs as in previous years to target a variety of technologies. Specific targeted technologies are likely prioritized in response to continued political instability, changes in regional and international foreign relations, and economic conditions. Military modernization (for the purposes of regional power projection) remains a significant motivator of collection activities; however, DCSA believes shifting international relations and trade agreements likely contributed to an observed variation in MOs from previous years. The inclusion of Near East countries in the Brazil, Russia, India, China, and South Africa (BRICS) summit and the Shanghai Cooperation Organization (SCO) signals a greater interconnectedness with international partners and developing trade relations. The growing inclusion of Near East countries in the international trading market provides greater opportunities for Near East countries to obfuscate import and export of U.S. dual-use and military technology through third country proliferators leveraging the increasing regional market. Near East entities remain the second most reported collector of sensitive and classified U.S. technology and information

resident in the U.S. cleared industrial base, accounting for 24 percent of overall reporting. During FY 2023, cleared industry reporting associated with Near East entities indicated that they targeted almost every category of the IBTL, emphasizing on aeronautic systems, manufacturing equipment and processes, and software.

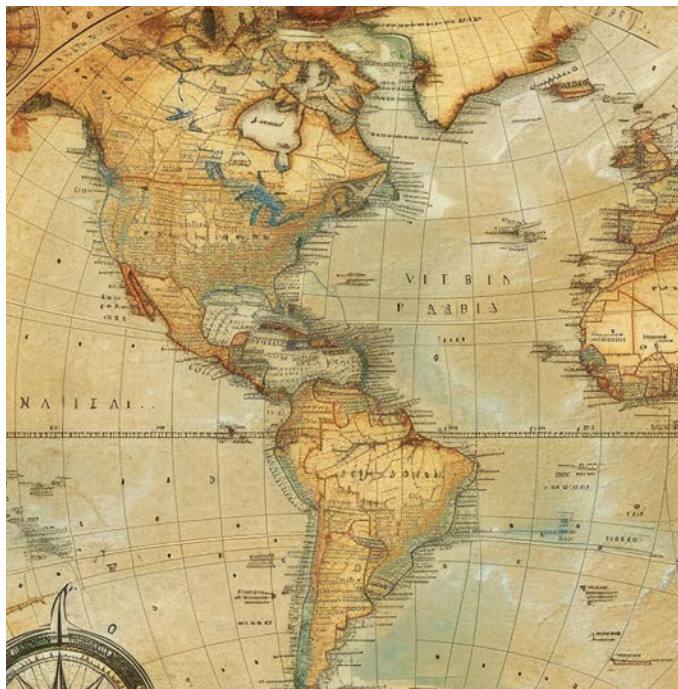
In FY 2023, Résumé Submission remained the top MO, accounting for 54 percent of all reported attempts, more than doubling the next closest MO, Exploitation of Business Activities, representing 19 percent. Résumé Submission consists of undergraduate, doctoral, and post-graduate researchers seeking opportunities within U.S. cleared academic institutions under the tutelage of cleared, federally funded professors. Although many academic solicitations may be legitimate attempts to study in the United States, DCSA cannot rule out attempts to exploit academic openness to gain access to sensitive information and technology developed in cleared industry and academia. Near East students/researchers studied and sought placement in advanced science, technology, engineering, and math (STEM) fields. By pursuing advanced STEM degrees in the



United States, Near East students are exposed to cutting-edge, advanced technologies and cleared professors engaged in sensitive research. These students and researchers chiefly sought degrees and positions affording access to sensitive information and technologies, including additive manufacturing, AI software, and engineering. The most significant change in MOs occurred in Request for Information (RFI)/Solicitation, which decreased five percent. The increase in reports associated with Exploitation of Business Activities and decrease in those associated with RFI/Solicitation may be the result of shifting international relations in the region, changes in international trade relationships resulting from international conflict, and the inclusion of several Near East countries in BRICS and SCO, offering new trading opportunities and affecting import and export markets. In FY 2023, some Near East entities—both commercial and governmental—leveraged existing business partnerships with cleared industry to obtain access to U.S. technologies beyond the scope of established information sharing agreements. Means included surreptitious room entry, unauthorized electronic devices, photography, and RFIs outside the scope of established parameters to cutting-edge, advanced technologies and cleared professors engaged in sensitive research. These students and researchers chiefly sought degrees and positions affording access to sensitive information and technologies, including additive manufacturing, AI software, and engineering. The most significant change in MOs occurred in Request for Information (RFI)/Solicitation, which decreased five percent. The increase in reports

associated with Exploitation of Business Activities and decrease in those associated with RFI/Solicitation may be the result of shifting international relations in the region, changes in international trade relationships resulting from international conflict, and the inclusion of several Near East countries in BRICS and SCO, offering new trading opportunities and affecting import and export markets.

In FY 2023, some Near East entities—both commercial and governmental—leveraged existing business partnerships with cleared industry to obtain access to U.S. technologies beyond the scope of established information sharing agreements. Means included surreptitious room entry, unauthorized electronic devices, photography, and RFIs outside the scope of established parameters.



Near East — Vignettes

- In January 2023, a Near East university graduate student sought admission to a Department of Defense (DoD)-funded hypersonics program at a CC to study under a cleared professor engaged in sensitive research. The program and professor would have provided the Near East graduate student with direct access to advanced hypersonic information and technology with direct applications to Near East military modernization efforts.
- Between December 2022 and August 2023, several high achieving Near East students and researchers applied for advanced programs at cleared academic institutions and under CCs engaged in cutting-edge AI, machine learning, quantum computing, hypersonics, and intelligence systems. All applicants were recognized as highly skilled, experienced, and competitive candidates for these programs with direct applications to Near East military modernization efforts, which could jeopardize the regional military power landscape of the Near East.
- In September 2022, a Near East commercial entity proposed a business collaboration with a CC. The proposed areas of cooperation were military component production, maintenance and servicing of naval vessels, and collaboration in the fields of oil, gas, and communications technology. The proposed fields of collaboration would have provided the Near East commercial entity with sensitive military vehicle, weapons, and electronics component information. The entities would have been able to apply this knowledge in advanced manufacturing and military modernization.
- In October 2022, a Near East national associated with a foreign media organization took unauthorized photographs and videos of multiple CC exhibits during a U.S.-based defense exhibition.
- In June 2023, a U.S. CC's aeronautics systems engineer manager experienced surreptitious entry into their hotel room while on official travel to a Near East country. The CC employee, while showering, witnessed an individual slightly open and quickly close the door to the bathroom.



Europe and Eurasia

Targeted Technology	Method of Contact	Method of Operation	Collector Affiliation
Services and Other Products	Email	RFI/Solicitation	Individual
Software	Web Form Submissions	Résumé Submission	Commercial
Aeronautic Systems	Résumé — Professional	Exploitation of Experts	Government — Affiliated

OVERVIEW

In FY 2023, Europe and Eurasia underwent significant geopolitical and military modernization efforts in response to the evolving security landscape influenced by Russia’s invasion of Ukraine. This conflict prompted reevaluation of defense strategies across the continent, leading to increased collaboration with the North American Treaty Organization (NATO) and the European Union (EU) to enhance military capabilities and strategic autonomy. Europe and Eurasia are focusing on a more robust European defense posture, including increased investment in defense industries and military readiness, emphasizing unified response to threats and commitment to maintaining territorial integrity and sovereignty.

In FY 2023, Europe and Eurasia entities remained the third most significant collector of sensitive or critical U.S. information and technology resident within the cleared industrial base, accounting for 18 percent of overall reporting. Throughout FY 2023, Europe and Eurasia entities targeted nearly every category of the IBTL, with an emphasis on services, software, aeronautic systems, electronics, and C4. Some Europe and Eurasia entities targeted access to a restricted satellite imagery database, AI, hypersonic

research, microelectronics, and ITAR advanced communications computer systems. Entities may attempt procurement of such capabilities, technologies, and topics to overcome technological shortcomings and challenges.

RFI/Solicitation was the most used MO in FY 2023, consisting of individuals seeking access to a restricted satellite imagery database and requesting controlled scientific documents. Résumé Submission and Exploitation of Experts accounted for 34 percent of overall reporting attempts. Europe and Eurasia entities frequently sent Résumé Submissions to the defense industrial base seeking engineering, software development, and program management positions. Although Exploitation of Cyber Operations was not a top-reported MO, DCSA continues to observe Europe and Eurasia entities leveraging hacktivist groups centered on distributed denial-of-service campaigns to attack cleared industry’s unclassified networks. These cybercriminals operate on financial motivation, targeting government and critical infrastructure organizations.



Vignettes

- In May 2023, a representative from a Europe and Eurasia space agency sent an unsolicited email to a CC requesting information on the detection of damage and spinning rate analysis for a satellite in Low Earth Orbit. The CC specializes in development/application of AI capabilities to enhance real-time sensor data utilization. Gaining access to U.S. satellite damage and spinning rate data can advance foreign space technology in increasing low orbit satellite lifespan and functionality, allowing longer influence in lower orbit space.
- In FY 2023, Europe and Eurasia state-sponsored cyberactors used phishing techniques and government network protocol vulnerabilities to gain access to user email accounts and cleared industry information. The cyberactor sent a phishing email to cleared industry employees, which, when clicked, enabled access to vulnerable employees' email. Due to lack of strict network protocols, any employee not enrolled in multi-factor authentication was vulnerable.
- In FY 2023, the Department of Justice and the Department of Commerce announced the first five strike force actions leading to the arrest of a Greek national involved in a procurement scheme to supply U.S. origin military and dual-use technologies to Russia. The highly regulated and sensitive components included advanced electronics and sophisticated testing equipment used in military applications, including quantum cryptography and nuclear weapons testing, as well as tactical battlefield equipment.



South and Central Asia

Targeted Technology	Method of Contact	Method of Operation	Collector Affiliation
Software	Email	Exploitation of Experts	Commercial
Services and Other Products	Résumé—Professional	Exploitation of Supply Chain	Government — Affiliated
Aeronautic Systems	Résumé—Academic	RFI/Solicitation	Individual

OVERVIEW

In FY 2023, South and Central Asia region entities sought access to U.S. defense-related technologies and information in response to ongoing military modernization efforts to enhance military capabilities in air, sea, and ground war-fighting domains and deter regional adversaries. South and Central Asia governments continue to deal with intraregional issues such as border skirmishes, technology races, and terrorism, and seek technologies to address continuing concerns for some countries in the region. While many countries in the South and Central Asia region are seeking to build their defense industrial base to address regional concerns, they are currently reliant on strategic partnerships to address their most critical technology needs. Throughout the fiscal year, South and Central Asia entities commonly sought access to defense-related U.S. technologies and information to enhance military capabilities through Résumé Submission, RFI/Solicitation, Exploitation of Experts, and attempts to purchase export-controlled technologies.

South and Central Asia region entities comprised five percent of DCSA reporting received from cleared industry in FY 2023, representing a decrease from 10 percent in FY 2022. Throughout the fiscal year, South and Central Asia countries requested defense-

related information and technologies on nearly all technologies on the IBTL, including software, services, other products, and aeronautic systems representing technology areas consistent with military modernization initiatives. Top targeted technologies included export-controlled modeling and simulation software, autonomous surface vehicles, ground and air-based radar systems, laser, software-defined radios, and advanced material coatings. Similar to FY 2022 reporting, South and Central Asia entities continue to display interest in U.S. aeronautic systems, including drones, helicopters, and aircraft parts.

Based on industry reporting, many of suspicious contacts from South and Central Asia entities represented individuals submitting résumés for jobs in information technology, manufacturing, and engineering. Individuals submitted academic résumés to conduct post-graduate research at U.S. universities in computational fluid dynamics, propulsion, thermal heat transfer, and material sciences. Commercial entities continue to request information and exploit business activities by seeking information or requesting collaboration on defense technologies. Government-affiliated entities also sought business relationships with cleared industry on behalf of procuring technology for foreign government end-users.



Vignettes

- In early 2023, a representative for a company in South and Central Asia requested purchase quotes for a range of laser technology products, an export-restricted technology that is the subject of numerous classified U.S. government contract vehicles. According to the CC reporting the incident, the components have applications in directed energy systems, though the final customer for this request was not disclosed. Prior DCSA reporting revealed the same South and Central Asian entity previously requested export-restricted satellite technology for their government agency in South and Central Asia.
- In mid-2023, a researcher representing a defense technology institute in South and Central Asia sought to connect with cleared academic researchers and collaborate on software development for military-centric radar systems, a classified program at the CC facility. The academic researcher shared their portfolio, which involves defense research to benefit a government entity in South and Central Asia. Open-source information regarding the defense technology institute indicated a ministry of defense provides at least some funding and direction to the institute and researchers employed there.
- In late 2022, a representative for a company in South and Central Asia contacted a CC on behalf of a ministry of defense in South and Central Asia. The company sought to be a supplier for export-restricted counter-unmanned aerial surveillance systems to military and

police forces in their respective nation. The company reportedly procures advanced technology for the government of a South and Central Asia nation and has a history of reverse-engineering technology to be produced indigenously, according to open-source information.

Western Hemisphere

Targeted Technology	Method of Contact	Method of Operation	Collector Affiliation
Electronics	Email	Exploitation of Experts	Commercial
Services and Other Product	Web Form Submissions	Exploitation of Supply Chain	Government — Affiliated
Software	Social Networking Services	RFI/Solicitation	Individual

OVERVIEW

The geopolitical landscape of the Western Hemisphere is marked by a complex interplay of historical and social issues that continue to shape the region. One prominent concern is China's rising influence in the region through trade agreements and investments, often seen as an attempt to counteract U.S. dominance. As observed in previous years, entities with ties to U.S.-sanctioned countries operate in the Western Hemisphere and contact CCs through a variety of means, including social media networking requests, invitations to overseas conferences, and unsolicited design offers. Other Western Hemisphere entities contacted cleared industry via in-person solicitations of sensitive information, joint venture opportunities, internship offers, and paid consultation opportunities. In several cases, these entities were U.S.-based firms representing foreign entities in sanctioned countries. In other instances, U.S.-based commercial entities solicited services on behalf of unspecified end-users. For more information, reference this assessment's Special Focus Area: International Expert Network Companies section.

In FY 2023, entities from the Western Hemisphere were the fifth highest collector of sensitive or critical U.S. information and

technology within the cleared industrial base, accounting for six percent of overall reporting. Throughout FY 2023, Western Hemisphere entities primarily targeted aeronautic systems, software, services, other products, and C4, all of which accounted for nearly half the region's contacts. The targeting of aeronautic systems included requests for Unmanned Aerial Systems and systems information about manned aircraft.

Exploitation of Experts was the most used MO in FY 2023. The primary Method of Contact (MC) was Email, accounting for nearly a third of Western Hemisphere reporting. Most emails were from commercial actors contacting cleared industry experts with offers for paid consultations concerning engineering or market insights. As observed previously in FY 2022, contacts entailed social network requests, paid consultation offers, and invitations to share expertise at international conferences and seminars. Typically, cleared personnel would receive an email or social media request from the representative of a consultation firm offering to pay large sums of money for the expert's views. In virtually all cases, the firm's client was unknown.



Vignettes

- In 2023, a U.S. national working at a U.S.-based company representing an East Asian country's scholar program used a professional networking site to contact a modeling and simulation SME to apply for a one-year, fully funded graduate school program at an East Asian university. This university conducts high-level defense research for its home country and is alleged to be involved in cyberattacks against global targets, including the United States.
- In 2023, a foreign national from a U.S.-sanctioned country in the Western Hemisphere emailed a CC academic professional and requested collaboration on advanced missile technologies. The requested information would have provided hypersonic missile technology, considerably increasing military capabilities of the foreign national's country. Despite claiming expertise in an unrelated field, the foreign national claimed to have previously worked with U.S. academics on prior work in hypersonics.



Africa

Targeted Technology	Method of Contact	Method of Operation	Collector Affiliation
Electronics	Email	Exploitation of Experts	Commercial
Services and Other Products	Web Form Submissions	Exploitation of Supply Chain	Government — Affiliated
Software	Social Networking Services	RFI/Solicitation	Individual

OVERVIEW

China and Russia are expanding their influence in Africa, with distinct goals and strategies. China's engagement is economic: significant investments in infrastructure, trade, and loans, seeking access to Africa's natural resources, and establishing trade partnerships. Russia's involvement focuses on military and political influence, using private military companies and supporting authoritarian regimes. Russia's economic engagement is limited compared to China but seeks to exploit Africa's resources and gain strategic military footholds. These activities in Africa reflect broader geopolitical ambitions: economic dominance for China and strategic influence for Russia.

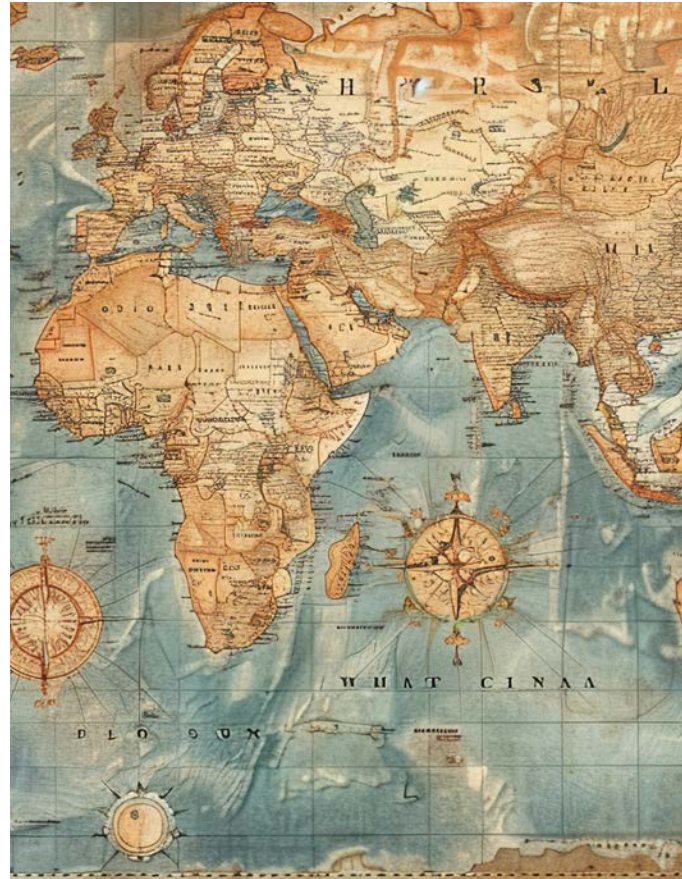
In FY 2023, Sub-Saharan Africa entities remained the sixth most significant collector of sensitive or critical U.S. information and technology resident within the cleared industrial base, accounting for two percent of overall reporting. Throughout FY 2023, Sub-Saharan Africa entities targeted limited aspects of the IBTL, with an emphasis on services, electronics, software, C4, and space systems. Sub-Saharan Africa entities requested access to a restricted satellite imagery database, procurement of vehicle-mounted improvised explosive device (IED) receivers/jammers, and night vision goggles.

Résumé Submission and RFI/Solicitation were the most used MOs in FY 2023. Sub-Saharan Africa individuals applied for positions in civil and structural engineering, human resources, software engineering, and network engineering. RFI/Solicitation from individuals with no discernible government affiliations sought access to a restricted satellite imagery database. One Sub-Saharan Africa company inquired about obtaining sub-meter resolution imagery for a Near East country.



Vignettes

- In 2023, an individual from the Africa region submitted a web form requesting restricted satellite imagery. The submission included the individual's name, citizenship, and email address. The request did not identify an end-user or specific end-use for the information.
- In 2023, a presumed African national with cybersecurity experience applied for an advertised position with a CC specializing in software development. The individual listed his work experience as a cyber security analyst, cyber risk and compliance analyst, and IT specialist. The position, which required a DoD security clearance, could have provided access to sensitive software development and data visualization for the U.S. Navy.
- In 2022, an attaché from the Africa region visited a CC and conveyed an urgent request for export-controlled night vision goggles for his nation's soldiers. The attaché approached the facility unannounced and procured a capabilities presentation. The attaché also discussed potential future border security and surveillance programs. The CC did not conduct a sale during this visit.



Special Focus Area: International Expert Network Companies

OVERVIEW

In FY 2023, international expert network companies (ENCs) facilitated communication between unidentified third parties and CC employees, intending to transfer protected information pertaining to defense technology to suspected foreign entities. According to open-source reporting, ENCs use email, social media, and telephone calls to connect experts in various sectors to clients seeking non-publicly available information. ENC business models obscure the ultimate client and facilitate teleconferences, with hundreds of dollars paid to SMEs. This MO is advantageous because FIEs are connected to cleared employees with a propensity for accepting cash payouts and working with foreign nationals.

Internationally, ENCs face scrutiny for acting as vectors for information theft on behalf of other nations. East Asian nations are curbing ENC's ability to compile and profit from information and expertise by providing information to foreign organizations, as some foreign organizations are accused of spying for foreign governments. ENCs will probably continue to represent a viable, overt means for foreign governments to obtain protected information because the ENC business model is particularly vulnerable to exploitation.

During FY 2023, ENCs sent requests to CC employees via email, social media messaging applications, and telephone calls, offering paid consultations to discuss sensitive technologies, including hypersonic and missile technology, aeronautics systems, 5th generation fighter aircraft, space launch technology, Unmanned Aerial Vehicle (UAV) platforms, and cybersecurity. ENCs occasionally provided a list of questions for CC employees to answer, which would provide export-controlled or sensitive information related to U.S. defense platforms to those third parties. CC employees were contacted by companies based in China, Russia, the United States, Hong Kong, the Philippines, the United Kingdom, Germany, Israel, and Canada, among other nations.

Special Focus Area: International Expert Network Companies—Vignettes

- An ENC based in Germany requested a CC employee provide expertise on space countermeasures in the defense industry and offered compensation for the information. This specific ENC has solicited CC employees for several years, requesting information regarding the F-35 Joint Strike Fighter, command-and-control systems, security software, and other classified and export-restricted technologies.
- In February and March 2023, four ENC employees individually contacted five CC employees at one company, offering paid consultations to CC employees involved in microelectronics and magnetic components with applications in space technology. The requests originated from the ENC's Hong Kong and U.S. offices, with customers unnamed in three solicitations and identified as an East Asian entity in one solicitation.
- In February 2023, an Asia-based employee of a U.S. Business (USBUS1) solicited a CC employee for a paid consultation on hypersonic missile engineering and development. The ultimate customer was not disclosed. The USBUS1 employee stressed the offer did not require relocation, and the customer would not ask about the CC employee's company or confidential information, to entice the CC employee to accept the solicitation.
- In September and October 2022, a UK-based employee for USBUS2 contacted a CC employee on three occasions, soliciting expertise in high performance polymers with defense and space applications. High performance polymers are used in defense applications as a critical structural component for aeronautics, space, and missile systems. The USBUS2 employee used Mandarin characters and was identified as a suspected Chinese national in subsequent reporting. The USBUS2 maintains offices in China, Dubai, India, Germany, Korea, United Kingdom, Spain, and elsewhere.

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 technology.

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, Communications, and Computers (C4)

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 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.

Industrial Base Technology List

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 professional 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 for 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 category 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

Industrial Base Technology List

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 transfers.

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

Person 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 providers; 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

Methods of Operation

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

Exploitation of Supply Chain

Compromising the supply chain, which may include 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 communications.

Résumé Submission

Foreign persons submitting résumés for academic or professional placement that would facilitate access to 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:

Conferences, Conventions, or Tradeshows

Contact regarding or initiated during an event, such as a conference, convention, exhibition, or tradeshow.

Cyber Operation

Activities taken directly against a targeted system including 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 including, but not limited to, spear phishing, cloning, and whaling.

Résumé — Academic

Résumé or CV submission for academic purposes.



Résumé — Professional

Résumé or CV submission 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.

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
Cote 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	Phillippines	Holy See			Haiti

Country List

Africa	East Asia and the Pacific	Europe and Eurasia	Near East	South and Central Asia	Western Hemisphere
Guinea-Bissau	Indonesia	Hungary			Honduras
Kenya	Singapore	Iceland			Jamaica
Lesotho	Solomon Islands	Ireland			Mexico
Liberia	South Korea	Italy			Nicaragua
Madagascar	Taiwan	Kosovo			Panama
Malawi	Thailand	Latvia			Paraguay
Mali	Timor-Leste	Liechtenstein			Peru
Mauritania	Tonga	Lithuania			Saint Kitts and Nevis
Mauritius	Tuvalu	Luxembourg			Saint Lucia
Mozambique	Vanuatu	Malta			Saint Vincent and the Grenadines
Namibia	Vietnam	Moldova			Suriname
Niger		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			

Country List

Africa	East Asia and the Pacific	Europe and Eurasia	Near East	South and Central Asia	Western Hemisphere
South Africa		San Marino			
South Sudan		Serbia			
Sudan		Slovakia			
Tanzania		Slovenia			
Togo		Spain			
Uganda		Sweden			
Zambia		Switzerland			
Zimbabwe		Türkiye			
		Ukraine			
		United Kingdom			

Region Breakdown



East Asia and the Pacific	South and Central Asia	Africa
Near East	Western Hemisphere	
Europe and Eurasia	Unknown	

