2025
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 USPI, contact the DCSA Intelligence Oversight officer, commercial: 571-305-6592.

Product ID: DCSA-TA-26-001
Date of Information: 20230930
Date of Publication: 20251215

Prepared by: Defense Counterintelligence Security Agency, Office of Counterintelligence, Analysis Division. For questions, please contact us on:

- NIPR: dcsa.quantico.dcsa-hq.list.ci-analysis-division@mail.mil
- SIPR: dcsa.quantico.dcsa-hq.list.ci-analysis-division@mail.smil.mil
- JWICS: DCSAMCBQuanticoDCSAHQListCIAnalyisDivision@dss.ic.gov

We appreciate all consumer input and feedback.

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

Table of Contents

Preface	5
Scope and Methodology	6
Executive Summary	8
East Asia and the Pacific	12
Near East (Middle East and Northern Africa)	16
Europe and Eurasia	20
South and Central Asia	24
Western Hemisphere	28
Sub-Saharan Africa	32
Administrative Information	36

Preface

Foreign intelligence entities are persistent in their efforts to steal critical American technology, compromise sensitive data, and undermine our nation's defense capabilities. Using tactics from cyberattacks to supply chain disruption, their objective is not only to exploit vulnerabilities, but also to pilfer technology and talent to advance their own military and economic development at the expense of ours. Vigilance is required to identify, understand, and deter these dynamic threats.

The cleared national industrial base—which includes academia, corporations of all sizes, and the personnel who research, develop, and field our nation's technologies—is a primary target for these foreign threats. As the cleared national industrial base continues to produce innovative capabilities, it becomes an even more attractive target for our adversaries.

The mission of the Defense Counterintelligence and Security Agency (DCSA) is to safeguard America's security by preserving the integrity of the cleared national industrial base and the critical technologies that underpin our military strength. DCSA is uniquely positioned to fulfill this role due to its direct access to industry, which enriches collaboration with the private sector and enhances national security. We serve as a vital link, conveying foreign intelligence threat information to cleared industry partners and relaying industry perspectives back to the Intelligence Community and other security entities. This collaboration is imperative to fortify America's warfighting missions and counter threats to national security.

To that end, DCSA provides this annual assessment—*Targeting U.S. Technologies: A Report of Threats to Cleared Industry*. This report elucidates the nature of the threats facing the cleared national industrial base. It serves as a crucial resource for our industry partners to establish and maintain effective security programs, protecting technology, information, facilities, and personnel to safeguard America's strategic and competitive advantage.

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) DoDI 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 report is to inform stakeholders about 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 report provides an unclassified snapshot of DCSA findings on the most pervasive actors targeting cleared industry and academia in fiscal year (FY) 2024. A more comprehensive view of FIE threats to cleared industry and academia is available in the classified assessment.

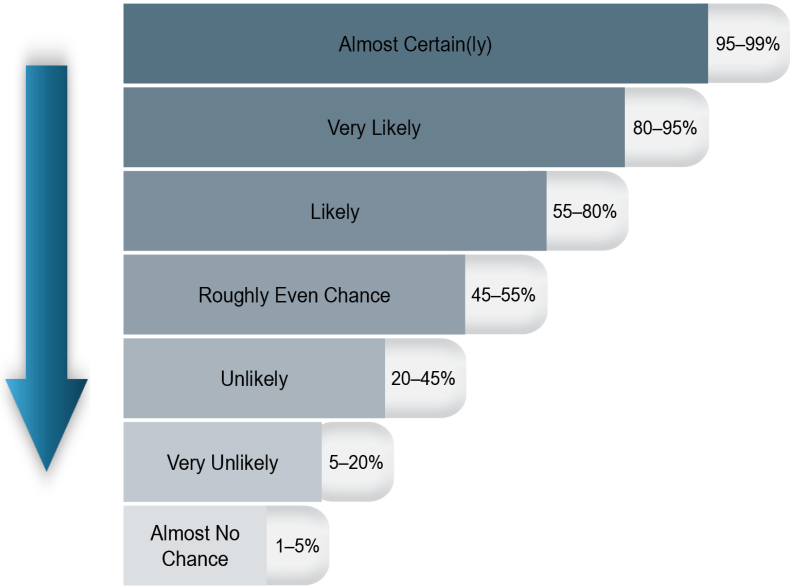
Throughout FY 2024, approximately 13,000 cleared contractor (CC) facilities were required to report suspicious contacts to DCSA IAW 32 Code of Federal Regulation Part 117, National Industrial Security Program Operating Manual. DCSA received and processed suspicious contact reports (SCRs) from cleared 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 compromise a cleared employee. DCSA cannot estimate the volume of suspicious FIE activity that was not reported by cleared industry or academia.

We organized this report by geographic regions, targeted technology, methods of contact (MCs) and methods of operation (MOs), 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 geographical section addresses the unique sources used and provides different and distinct analysis of the threat to cleared industry. Although DCSA considered relevant reporting and finished intelligence products from the DoW and the Intelligence Community, SCRs served as the basis for the 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/reports.

Expressing Analytic Uncertainty

Uncertainty is based on both likelihood and confidence. The following terms use estimative language to express the likelihood an event or development will or will not happen.

ICD 203 Expression of Likelihood



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

- **Situation:** Highly complex or rapidly evolving, with multiple issues or actors; contradictory reporting.
- **Sourcing:** Uncorroborated information, unknown reliability; high potential for deception.
- **Gaps:** Filling gaps could substantially affect major judgments.

Moderate

- **Situation:** Complicated with multiple issues or actors; some previous, well-understood examples; ambiguous reporting.
- **Sourcing:** Partially corroborated information; some potential for deception.
- **Gaps:** Filling gaps could affect major judgments.

High

- **Situation:** Routine, well understood; minimal contradictory reporting.
- **Sourcing:** Well-corroborated; reliable sources; low potential for deception.
- **Gaps:** Filling gaps would have minor impact on judgments.

In 2024, the DCSA received more than 32,000 SCRs from contractors operating under the National Industrial Security Program (NISP). DCSA identified more than 2,700 incidents where foreign entities attempted to illicitly obtain classified information or technology from cleared industry. These entities also tried to circumvent sanctions and compromise cleared employees. Throughout the FY, foreign entities targeted various U.S. technologies to bypass export restrictions and enhance their domestic capabilities. The top three targeted technology categories (Aeronautic Systems, Software, and Services or Other Products) accounted for 34 percent of all reported incidents.

East Asia and the Pacific and the Near East (Middle East and Northern Africa) (hereafter referred to as Near East) remained the most significant collectors of classified and sensitive U.S. information and technology, accounting for nearly 70 percent. These entities targeted enabling technologies, such as communication and electronic warfare components, artificial intelligence (AI), software, and additive manufacturing, including dual-use and export-controlled technologies. East Asia and Pacific entities sought access to U.S.-enabling technologies the region struggles to produce indigenously, such as export-restricted communication and electronic warfare components, to meet their defense modernization goals. They also targeted U.S. technologies to identify shortcomings and drive innovation in long-term modernization efforts. Near East entities focused on acquiring software related to AI, cybersecurity, advanced unmanned aerial systems (UASs), and drone-detection technologies.

Entities from Europe and Eurasia and the Western Hemisphere accounted for 24 percent of reported incidents. Aeronautic Systems was the top targeted technology, with an emphasis on UAS technologies. Europe and Eurasia entities also targeted communication systems and network defense technologies, including encryption and cybersecurity information. Western Hemisphere entities primarily targeted Aeronautic Systems; Command, Control, Communications, and Computers (C4); and Electronics, often on behalf of undisclosed third parties or countries using regional entities as proxies. These technologies are critical for modern warfare and are highly sought after to enhance military effectiveness. In contrast, entities from South and Central Asia and Sub-Saharan Africa (hereafter referred to as Africa) accounted for only 8 percent of reported incidents. South and Central Asia entities sought to acquire helicopters, aircraft parts, and radar countermeasure systems to support regional military modernization initiatives. Africa entities (less than 1 percent of overall reporting) sought access to U.S. technologies to strengthen national security.

Foreign entities employed various MCs to reach CCs. Email accounted for 32 percent of reported incidents, making it the primary MC. Foreign entities frequently used Email to solicit consultation opportunities to establish business partnerships under the guise of legitimate activities, as well as to request information on or to purchase restricted technologies. Résumé submissions were also significant, with Résumé–Academic submissions accounting for 20 percent and Résumé–

Professional submissions accounting for 8 percent. Web Forms were used in 9 percent of incidents, typically to request information or services from CC websites.

The most common MO was Résumé Submission, which accounted for 28 percent of reported attempts. Many résumés were from undergraduate, doctoral, and post-graduate researchers seeking opportunities in U.S. academic institutions and individuals pursuing post-graduate research at cleared universities in emerging fields with dual-use applications. Near East entities continued to employ Résumé Submission as a key MO, with academic researchers seeking to conduct research in areas such as hypersonic flow, radar, antenna design, and computational fluid dynamics. East Asia and Pacific entities also used Résumé Submission, often with students and researchers sponsored by regional governments seeking admission to U.S. university programs conducting defense research in fields like computer science, AI, and robotics. South and Central Asia entities submitted résumés to pursue research in emerging fields with dual-use applications, such as AI, quantum computing, and material sciences.

Although some solicitations were legitimate, DCSA cannot rule out that some attempts were to exploit academic openness and gain access to sensitive information and technology. Exploitation of Cyber Operations played a significant role in FIE attempts to illicitly obtain classified information and technology, with foreign entities using tactics such as malware deployment, data exfiltration, and social-engineering campaigns to gain access to public-facing networks and compromise sensitive information. Near East cyberactors used these tactics to target U.S. defense industry networks, while East Asia and Pacific cyberactors exploited network vulnerabilities and used spear phishing and compromised credentials to target CC networks. Western Hemisphere entities also increasingly relied on Exploitation of Cyber Operations, surpassing other MOs for the region, with tactics like phishing, password-spraying, and credential harvesting to gain access to CC systems.

Individual entities with no confirmed affiliation accounted for 35 percent of reported incidents, mostly related to Résumé Submission. These individuals often presented themselves as independent researchers or job seekers, but their true affiliations and intentions often remained unclear. Commercial entities, mainly from East Asia and the Pacific region, accounted for 32 percent of reported incidents. These commercial entities frequently attempted to establish business partnerships or supplier relationships with U.S. CCs, often under the guise of legitimate business activities, but with the underlying intent of acquiring export-controlled technologies. Government and government-affiliated entities accounted for 28 percent of reported incidents. These entities were often linked to state-sponsored efforts to enhance national defense capabilities, with a particular focus on acquiring advanced technologies that could be used to bolster military and intelligence operations.

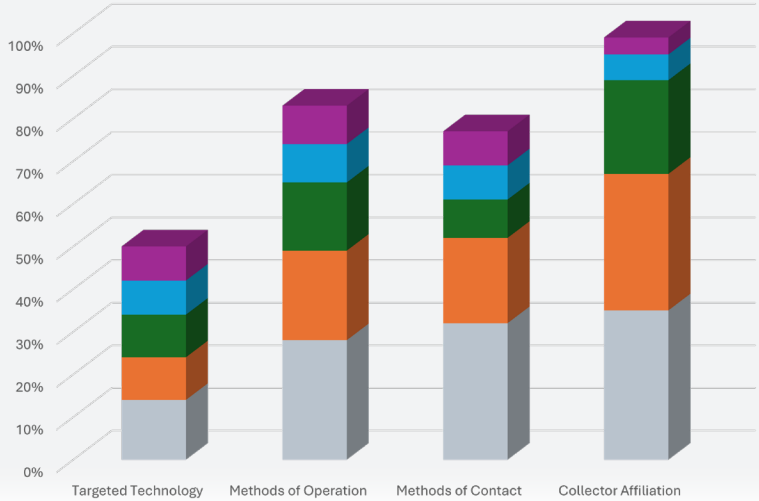
Executive Summary

Top Targeted Technologies	
14% Aeronautic Systems	
Software	10%
Services and Other Products	10%
Electronics	8%
C4	8%

Methods of Operation	
28% Résumé Submission	
Exploitation of Experts	21%
Exploitation of Business Activities	16%
Request for Information/ Solicitation	9%
Attempted Acquisition of Technology	9%

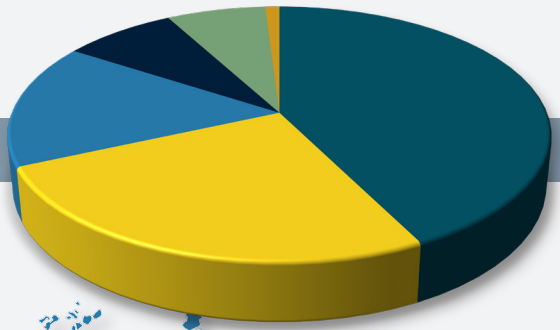
Methods of Contact	
32% Email	
Résumé—Academic	20%
Web Form	9%
Résumé—Professional	8%
Conferences, Conventions and Tradeshows	8%

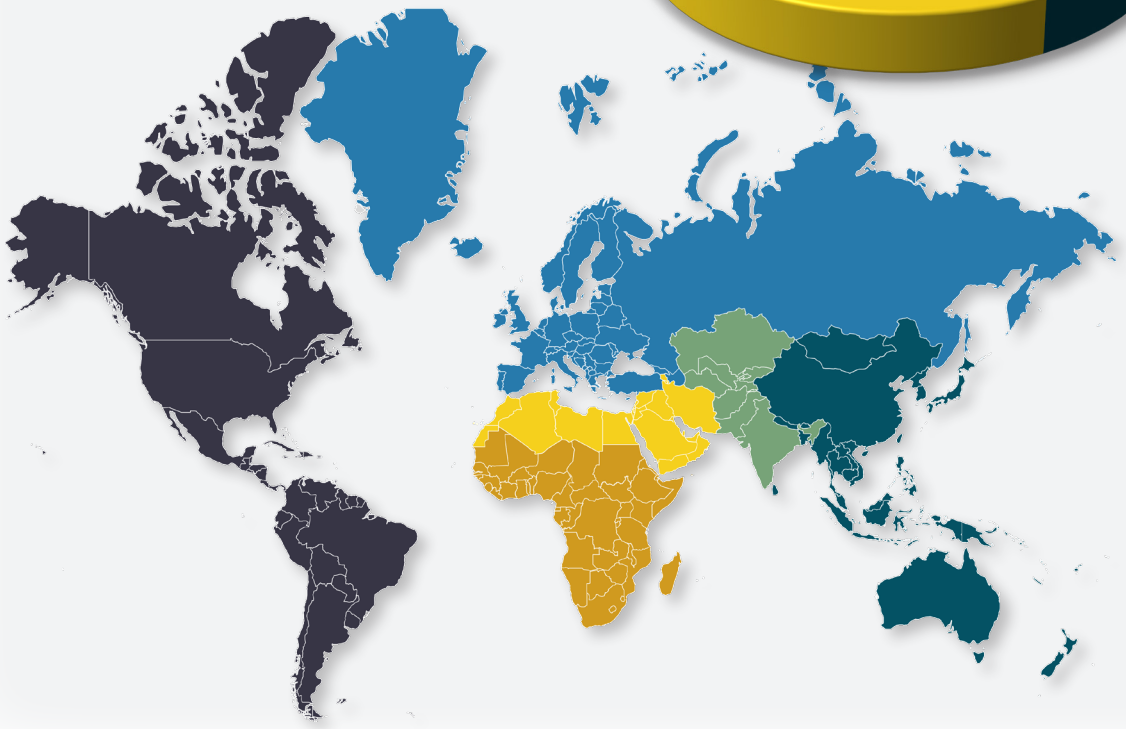
Collector Affiliation	
35% Individual	
Commercial	32%
Government Affiliated	22%
Government	6%
Unknown	4%



Geographical Regions

East Asia and the Pacific	43%	Western Hemisphere	8%
Near East (Middle East and Northern Africa)	26%	South and Central Asia	7%
Europe and Eurasia	16%	Sub-Saharan Africa	<1%





East Asia and the Pacific

Overview

In FY 2024, East Asia and Pacific entities continued to be the most prominent threat to U.S. sensitive and classified information resident in cleared industry, accounting for nearly 43 percent of DCSA reporting received from cleared industry. Longstanding territorial disputes and frequent shows of force in the East Asia and Pacific region have fueled defense modernization efforts among regional governments seeking to project power and maintain a technological edge over regional and global adversaries. Limited by U.S. export controls on dual-use and sensitive U.S. technologies, allied and adversarial East Asia and Pacific entities employed traditional and non-traditional collectors (NTCs)[i] to acquire U.S. technologies and information to bolster defense modernization and indigenous production capabilities. East Asia and Pacific entities primarily relied on a whole-of-society approach by using NTCs, such as business practitioners, academic researchers, students, and talent recruiters, to acquire U.S. export-restricted technologies, while also leveraging government and military officials to conduct traditional collection against the DIB.

East Asia and Pacific entities targeted almost all technology areas of the Industrial Base Technology List (IBTL) in support of their respective short-term and long-term defense modernization goals. Aeronautic Systems, Software, Electronics, C4, and Services and Other Products ranked as the top-targeted U.S. technology areas. East Asia and Pacific entities sought access to U.S.-enabling technologies the region is challenged to produce indigenously, such as export-restricted communication and electronic warfare

Top Targeted Technology	
	Aeronautic Systems
	Software
	Electronics
Methods of Operation	
	Exploitation of Experts
	Exploitation of Business Activities
	Résumé Submission
Methods of Contact	
	Email
	Conferences, Conventions, or Tradeshows
	Résumé—Academic
Collector Affiliation	
	Commercial
	Government Affiliated
	Individual

[i] NTCs are individuals who collect information, technology, or expertise in support of a Nation-State's development goals; but is not tasked or trained as an asset by a foreign intelligence service. NTCs may be witting or unwitting scientists, academics/researchers, businesspersons, prominent members of overseas communities, or other individuals who are neither intelligence officers nor recruiter intelligence assets, but who are well placed and incentivized to leverage that access to advance a foreign government's technological development for incorporation into military and commercial enterprises.

components, to meet short-term defense modernization goals. They also attempted to gain access to U.S. technologies, such as UASs, to identify technology shortcomings and areas for improvement. Additionally, East Asia and Pacific entities sought to drive innovation in long-term modernization efforts by recruiting U.S. cleared employees specializing in emerging technology fields such as quantum computing, AI, fifth-generation telecommunications networking, and biotechnology.

Although East Asia and Pacific entities employed a variety of MOs, the ones most associated with NTCs were Exploitation of Experts, Exploitation of Business Activities, Résumé Submission, Attempted Acquisition of Technology, and Request for Information/Solicitation. East Asia and Pacific headhunting firms and talent programs sought to exploit experts by attempting to recruit CC employees via unsolicited emails by offering lucrative employment benefits. Commercial businesses sought to establish business partnerships and supplier relationships with CCs and requested CC product designs to tailor their services to the CC's needs. Students and researchers from the East Asia and Pacific region, often sponsored by regional governments, sought admission to cleared U.S. university programs conducting defense research in fields such as computer science, AI, robotics, and materials engineering. Commercial businesses attempted to procure export-restricted U.S. technologies, including microelectronics and C4 systems, on behalf of East Asia and Pacific governments, sometimes obfuscating the technologies' intended end users.

During FY 2024, East Asia and Pacific entities' Exploitation of Cyber Operations included exploitating network vulnerabilities and living-off-the-land techniques to exfiltrate sensitive information stored on CC networks and conduct follow-on malicious cyberactivities. East Asia and Pacific government-affiliated cyberactors used network scanning, spear phishing, data exfiltration, and compromised credentials to target and gain access to public-facing network appliances on CC networks. East Asia and Pacific entities frequently obfuscated phishing attempts using spoofed emails for typical business correspondence and solicitation of cleared industry data.

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

East Asia and the Pacific — Vignettes

FY 2024

An East Asia and Pacific business representative submitted a web form to a CC microelectronics specialist requesting to purchase a radar technology device equipped with electronic warfare applications. According to the East Asia and Pacific business's website, the East Asia and Pacific entity conducts research with an East Asia and Pacific university that has acquired sensitive U.S. technologies to support an East Asia and Pacific military.

JAN. 2024

Suspected East Asia and Pacific cyberactors used social-engineering tactics to target CCs. The suspected cyberactors disseminated spear phishing messages in attempts to collect intellectual property, proprietary business information, personally identifiable information, or sensitive information from CC personnel. The suspected cyberactors used an end-to-end encryption communication platform, a social-media platform, and a mobile-phishing text scheme to elicit sensitive U.S. naval engineering and weapons program information.

FY 2024

A representative of an East Asia and Pacific government approached a CC's booth at an electronics tradeshow and drew a picture of the CC's directed-energy counter-unmanned aircraft system (C-UAS). The representative showed the picture to a CC employee and asked what knowledge the CC was willing to share about the C-UAS. The CC employee denied knowledge of the system, and the representative pointed to the antenna dish on the C-UAS in the drawing and asked the CC employee to disclose its radio frequency source.

FY 2024

From September 2023 to July 2024, suspected East Asia and Pacific cyberactors conducted active reconnaissance activity to target cleared contractors. The suspected cyberactors used port-scanning activities to leverage and identify potential points-of-entry into CC networks. The suspected cyberactors executed more than 20-million scans toward CC external system components. The unsuccessful attempts to gain access focused on port 23 and port 6379. Some port-scanning activity occurred after press releases and media coverage of company information.

SEP. 2023-JUL 2024

A technology manager for a Near East defense contractor and a senior manager for a Near East military visited a CC booth at a conference and asked questions regarding the CC's UAS simulator support, and delivery of advanced training systems that support the U.S. military. The defense contractor, who spoke English, asked questions on behalf of the foreign government member, who did not speak English, and instead communicated with the defense contractor in a foreign language. When told the sensitive information related to the UAS and U.S. military could not be provided, the Near East defense contractor asked if the CC could work with other countries without following U.S. export rules.

Page Left Intentionally Blank

Near East (Middle East and Northern Africa)

Overview

In FY 2024, Near East entities accounted for 25 percent of overall reported attempts to access U.S. sensitive and classified information resident in the U.S. cleared DIB. Ongoing conflicts, such as wars, international terrorism, and tensions between regional powers have degraded defensive capabilities, altered international relations, and strained economic conditions in the region. These regional conflicts have highlighted Near East entities' urgent need for military modernization and advanced U.S. technologies to enhance their defense capabilities. Consequently, Near East entities engaged with CCs to procure U.S. technologies of strategic importance, such as advanced missile systems, launch vehicles, weapons systems, naval vessels, and aeronautic systems.
Near East entities leveraged traditional collectors (government and military officials) and NTCs (regional defense contractors, students, and researchers) in attempts to gain access to sensitive U.S. technologies and information. Some countries in the Near East region used various obfuscation techniques to circumvent U.S. export controls and economic sanctions when attempting to acquire restricted technologies from the U.S. DIB.

Near East entities primarily targeted U.S. technologies associated with the Software, Aeronautic Systems, Manufacturing Equipment and Processes, and Electronic categories of the IBTL. Specifically, Near East entities focused on acquiring software related to AI, cybersecurity, and aeronautic systems, including drone-detection technologies and advanced UASs. Near East entities targeted Manufacturing Equipment and Processes for information on advanced metal alloys and coatings. Near East entities also requested dual-use electronic components commonly used in radar, electronic warfare, communications, and satellites, highlighting the breadth of their technological interests.

Top Targeted Technology	
	Software
	Aeronautic System
	Manufacturing Equipment and Processes
Methods of Operation	
	Résumé Submission
	Exploitation of Business Activities
	Request for Information/Solicitation
Methods of Contact	
	Résumé — Academic
	Email
	Résumé — Professional
Collector Affiliation	
	Individual
	Commercial
	Government

Near East entities continued to employ Résumé Submission, Exploitation of Business Activities, and Request for Information/Solicitation to acquire defense-related information and technology from the DIB. Résumé submissions consisted of academic researchers seeking to conduct research at U.S. cleared academic institutions in areas such as hypersonic flow, AI/machine learning, software, radar, antenna design, computational fluid dynamics, material science, and additive manufacturing—fields with applications in both civilian and defense sectors. Near East government, government-affiliated, and commercial entities exploited foreign visits to CCs to gain access to U.S. technologies and information beyond the stated purpose of the visit.

During FY 2024, Near East government-affiliated and unknown cyberactors also used Exploitation of Cyber Operations to gain access to CC public-facing networks. Cyberactors used exploitation of malware deployment, data exfiltration, port scanning, credential harvesting, and social-engineering campaigns. Near East cyberactors mainly targeted the defense, aviation, aerospace, and energy sectors for cyberespionage purposes. Additionally, Near East cyberactors resorted to phishing, impersonation, and other social-engineering techniques to obfuscate malicious cyberactivities and prolong cyberoperations on cleared industry networks.

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

Near East (Middle East and Northern Africa) — Vignettes

JAN 2024

A Master of Science in aerospace engineering graduate from a prominent Near East university (NEU) engaged in military and ballistic missile-related programs for the government, submitted a résumé requesting a research position with a CC. The NEU graduate claimed to be conducting ongoing research with the NEU on computational fluid dynamics analysis of centrifugal compressors and explained he could significantly contribute to the CC's research team because of his background in aerospace engineering. Near East militaries and governments conduct initiatives to collaborate with NEUs on defense and security research. The NEU graduate's participation with the CC would provide access to information and expertise that would advance the defense and security interests of a Near East military and government.

OCT 2023-2024

Three separate foreign visits to a CC, a Near East military officer requested technical information about a marine system outside the scope of the Technical Assistance Agreement (TAA) regarding a marine system manufactured by the CC. This officer was the only member of the delegation to make such requests and continued to do so despite being instructed to stop. The officer also attempted to meet with CC technical personnel and only ceased asking questions when a superior officer intervened, but resumed the questioning when the superior officer left. Information outside the scope of the TAA could provide details that are intentionally withheld from foreign partners and valuable insights into sensitive U.S. military technologies.

FY 2023-2024

A Near East government-affiliated cyberactor targeted a cleared aerospace company. The cyberactor impersonated the company's graphical user interface (GUI) for submitting job applications and installed a backdoor using FalseFont malware to reroute all user logins to the malicious host command and control interface. The malware prompted victims to log in to their account or log in as a guest, allowing the cyberactor to maintain remote access to the victim's compromised system. The remote access enabled the cyberactor to execute commands and processes, download and upload files, receive information about the file system, update malware, steal credentials, and capture the victim's screen.

NOV 2023

A technology manager for a Near East defense contractor and a senior manager for a Near East military visited a CC booth at a conference and asked questions regarding the CC's UAS simulator support, and delivery of advanced training systems that support the U.S. military. The defense contractor, who spoke English, asked questions on behalf of the foreign government member, who did not speak English, and instead communicated with the defense contractor in a foreign language. When told the sensitive information related to the UAS and U.S. military could not be provided, the Near East defense contractor asked if the CC could work with other countries without following U.S. export rules.

Page Left Intentionally Blank

Europe and Eurasia

Overview

In FY 2024, Europe and Eurasia entities remained the third most significant collector of U.S. sensitive and classified information in the cleared DIB, accounting for nearly 16 percent of overall reporting. In response to the ongoing Russia/Ukraine war, some entities in the Europe and Eurasia region focused on modernizing their military forces, bolstering their respective industrial bases, pursuing joint procurement initiatives, and addressing technology gaps exposed by the war. Europe and Eurasia entities sought access to U.S. defense platforms including fighter jets, missiles, UASs, air defense systems, unmanned ground vehicles, and mobile artillery platforms to enhance their deterrence and defense capabilities against regional aggressors. Both traditional and non-traditional Europe and Eurasia entities were observed targeting U.S. technologies in FY 2024, including members of the military, defense industry, expert network companies (ENCs)[ii], and individuals residing in Europe or Eurasia with no specific collector affiliation. In some reported instances, Europe and Eurasia entities attempted to circumvent U.S. export restrictions and economic sanctions by attempting to acquire restricted U.S. technology for prohibited end users.

Europe and Eurasia entities sought access to nearly every technology area of the IBTL, with an emphasis on Aeronautic Systems, Services and Other Products, and C4 systems. These entities demonstrated an interest in UAS and C-UAS segments of Aeronautic Systems, reflecting the increased use of unmanned vehicles and countermeasures in the ongoing war in Russia/Ukraine

Top Targeted Technology	
	Aeronautic Systems
	Services and Other Products
	Command, Control, Communications, and Computers
Methods of Operation	
	Exploitation of Experts
	Request for Information/Solicitation
	Exploitation of Business Activities
Methods of Contact	
	Email
	Web Form
	Cyber Operations
Collector Affiliation	
	Commercial
	Government Affiliated
	Individual

[ii] ENCs are firms that connect clients with experts in specific fields or industries to facilitate the exchange of information and insights for research, due diligence, or strategic decisionmaking. ENCs operate by matching clients with experts who have specialized knowledge or experience, and facilitate communication between the two parties by email, social media, or telephone calls. As previously reported by DCSA in "Targeting U.S. Technologies" (DCSA-TA-25-001), the ENC business model is vulnerable to FIE exploitation given ENC's practice of withholding the identity of the ultimate recipient.

and the growing significance of UASs in modern conflicts. The bulk of reporting related to Services and Other Products pertained to requests for restricted satellite imagery for undisclosed purposes. Finally, targeted products in the C4 category were focused on communication systems and network defense to include requests for network protection, encryption technologies, and cybersecurity information.

Europe and Eurasia entities employed several MOs, relying primarily on Exploitation of Experts, Request for Information/Solicitation, and Exploitation of Business Activities. Representatives from Europe and Eurasia-based ENCs attempted to exploit U.S. experts at CCs by offering paid consultations in exchange for sensitive information on U.S. defense technologies related to quantum-sensing technologies, fighter jets, missile systems, and space technologies for unidentified clients. Requests for Information/Solicitation included attempts to obtain satellite imagery; or acquire capabilities or technical information across a range of technologies, including, but not limited to, UASs and survivability. Europe and Eurasia entities also attempted Exploitation of Business Activities by leveraging requests for collaboration, provision of services, and foreign visits to gain access to restricted U.S. information. Although not a top-reported MO, Europe and Eurasia entities used Exploitation of Cyber Operations to target intelligence, surveillance, reconnaissance, and UAS technologies. Phishing, port scanning, and brute-force attacks were the most commonly reported tactics, techniques, and procedures in FY 2024.

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

APR 2024

A public announcement revealed a CC specializing in C4ISR received a U.S. Government contract. After the public announcement, the CC received increased network traffic accounting for more than 23 million port scans against its public-facing network infrastructure originating from Europe and Eurasia entities. In May 2024, a Europe- and Eurasia-affiliated unknown actor, using a compromised vendor account, targeted the CC with phishing and credential-harvesting attempts.

FEB 2024

Representatives from a state-owned Europe and Eurasia defense conglomerate under U.S. sanctions sought information regarding the manufacturer, location of production, and camera system of a UAS from a CC at a defense tradeshow. The representatives falsely portrayed their nationality to the CC representative throughout the line of questioning. Prior to the tradeshow, the UAS was added to the Defense Innovation Unit "Blue UAS List" for meeting strict guidelines on the prohibition of foreign UAS components. The details requested by the sanctioned entity attempted to undermine U.S. national security by providing the sanctioned conglomerate with sensitive supply chain information.

NOV 2023

A Europe-based ENC representative sent an unsolicited email to a CC requesting a paid consulting interview for an undisclosed third party on the wearable C-UAS market. The representative stated that their client was looking to understand C-UAS market trends, specifically current C-UAS offerings and purchasing cycle trends. To this end, the ENC requested information on U.S. and non-U.S. companies in the sector, their products, how various military echelons might be equipped with C-UAS technology in the future, and the impact of macroeconomic developments in Ukraine and Israel on C-UAS investments. Obfuscation of the ultimate end user in the ENC system presents an opportunity for adversaries to obtain insight into U.S. C-UAS capabilities.

Page Left Intentionally Blank

South and Central Asia

Overview

In FY 2024, South and Central Asia entities accounted for nearly 7 percent of overall reporting regarding attempts to access U.S. sensitive and classified information resident in the U.S. cleared DIB. South and Central Asia entities continued to confront security challenges, such as territorial disputes between neighboring countries, terrorist organizations, and insurgents. South and Central Asia region entities attempted to acquire advanced U.S. technologies to close technological gaps between neighboring adversaries by enhancing their ground, air, and naval military capabilities. South and Central Asia entities also sought enabling technologies commonly used to monitor borders and support counterterrorism operations.

Throughout the FY, South and Central Asia entities' leading IBTL requests were for Aeronautic Systems, Software, Services and Other Products, and Manufacturing Equipment and Processes. Aerospace and defense contractors sought to acquire UASs, helicopters, aircraft parts, software-defined radios, and radar countermeasure systems on behalf of regional government and military entities. These technology sectors align with regional military modernization initiatives to overcome technological shortcomings and improve situational awareness, operational intelligence, communication, and resilience of defense platforms.

Throughout the FY, South and Central Asia entities employed a variety of MOs, including Résumé Submission, Exploitation of Experts, Exploitation of Business Activities, Requests for Information, and Attempted Acquisition of Technology to access U.S. defense-related technologies and information from the cleared DIB. Individuals from the

Top Targeted Technology	
	Aeronautic Systems
	Software
	Services and Other Products
Methods of Operation	
	Résumé Submission
	Exploitation of Experts
	Exploitation of Business Activities
Methods of Contact	
	Email
	Résumé — Academic
	Résumé — Professional
Collector Affiliation	
	Individual
	Commercial
	Government Affiliated

region submitted academic résumés to pursue post-graduate research at cleared universities in emerging fields with dual-use application, such as AI, machine learning, quantum computing, nanotechnology, material sciences, smart manufacturing, hypersonics, and thermal heat transfer. Individuals with prior government affiliation submitted professional résumés to CCs seeking jobs in information technology, manufacturing, engineering, and aviation. Commercial entities primarily attempted to exploit experts through emails and social network services requesting CCs participate in paid consultations for sensitive and proprietary information. Commercial and government-affiliated entities also sought to collaborate on defense projects to enhance military capabilities for South and Central Asia governments.

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

South and Central Asia — Vignettes

JUL. 2024

A South and Central Asia national sent an unsolicited email and résumé to a cleared professor at a U.S. academic cleared university, requesting a PhD research opportunity in the university's aerospace and hypersonic research program. The individual, a hypersonics research and development engineer at a South and Central Asia technological university, expressed keen interest in high-performance computing, aerodynamics, heat and mass transfer, machine learning, and AI. A South and Central Asia government funded the individual's education. Studying under the cleared professor could have enabled the South and Central Asian national to acquire sensitive information on advanced aeronautics and astronautics technologies.

NOV. 2023

A representative of a South and Central Asia defense contractor sent an unsolicited email to a CC requesting a quote for UAS technology and proposed a partnership to satisfy the requirements of a South and Central Asia's armed forces. Open-source information about the defense contractor indicated the existence of ties to the South and Central Asia government and revealed the contractor had previously worked on defense projects for the government. The requested UAS technology is controlled under the International Traffic in Arms Regulations (ITAR) and is not permitted for export to the South and Central Asia government.

JUL. 2023

A South and Central Asia government employee submitted a professional résumé to a U.S. CC for a mechanical design engineer position. The candidate for the position would work on aeronautic systems, requiring U.S. citizenship and a Department of War security clearance. The South and Central Asia government employee listed his current employer as a South and Central Asia government organization and disclosed that he had been employed there for approximately 10 years. Employment with the U.S. CC could have granted the individual access to sensitive U.S. Government information and access to classified workspaces.

Page Left Intentionally Blank

Western Hemisphere

Overview

In FY 2024, entities from the Western Hemisphere accounted for 8 percent of overall reporting of attempts to access sensitive, classified information and technology resident in the cleared DIB. The Western Hemisphere region continued to face significant national security challenges, including transnational organized crime, insurgent activities, and regional power struggles. These challenges drove some Western Hemisphere entities to seek access to U.S. technologies to enhance military and security capabilities, particularly to help combat organized crime and insurgent activities. However, the most significant targeting of sensitive technologies, particularly UASs and aeronautics technology, was driven by other countries using Western Hemisphere entities as proxies or through ENCs with undisclosed clients. These technologies are critical for modern warfare and are highly sought after to enhance military effectiveness. As seen in previous years, entities with ties to U.S.-sanctioned countries continued to leverage Western Hemisphere entities to procure sensitive and export-controlled technologies, often circumventing international sanctions. Additionally, undisclosed third parties used ENCs in the region to reach out to employees of the cleared DIB working on a wide array of technologies.

Throughout FY 2024, Western Hemisphere entities primarily targeted Aeronautic Systems, C4, and Electronics. In some instances, the entities involved indicated the desire to provide technology to foreign interests, signifying a broader demand from third parties outside the region. The Aeronautic Systems targeted included jet engines and UASs and the targeting was often conducted on behalf of undisclosed entities. Similarly, efforts to acquire C4 systems (antennae and C4 architecture) also was on behalf of unknown third parties. The

Top Targeted Technology	
	Aeronautic Systems
	Command, Control, Communications, and Computers
	Electronics
Methods of Operation	
	Exploitation of Cyber Operations
	Exploitation of Experts
	Exploitation of Business Activities
Methods of Contact	
	Cyber Operations
	Email
	Personal Contact
Collector Affiliation	
	Commercial
	Individual
	Government Affiliated

Electronics targeted included microelectronics, integrated circuit design, printed circuit boards, and imaging systems and was driven by both regional needs and demands from unknown third parties. All the primarily targeted technologies can significantly enhance surveillance, transportation, and communication capabilities; disrupt adversarial networks; and strengthen border security, ultimately supporting efforts to counter organized crime and insurgent activities in the Western Hemisphere.

Exploitation of Cyber Operations emerged as the most used Method of Operation in FY 2024, surpassing Exploitation of Experts and Exploitation of Business Activities. CCs experienced reconnaissance and connection attempts from cyberactors against public-facing networks, phishing attempts to email accounts, password-spraying attacks, and the use of credential-harvesting techniques to gain access to CC systems and information. Malicious cyberactors' primarily targeted CCs specializing in C4 and Aeronautic Systems. Additionally, most Exploitation of Experts involved ENCs offering compensation to CC employees for consultation services regarding their technical expertise; in almost all cases ENC clients were unknown or undisclosed and sought a wide variety of technologies, including UASs and microelectronics. Additionally, personal contact attempts involved unannounced or unscheduled individuals arriving and requesting impromptu meetings with CC personnel.

Antigua and Barbuda	Canada	Ecuador	Jamaica	Saint Lucia
Argentina	Chile	El Salvador	Mexico	Saint Vincent and the Grenadines
The Bahamas	Colombia	Grenada	Nicaragua	Suriname
Barbados	Costa Rica	Guatemala	Panama	Trinidad and Tobago
Belize	Cuba	Guyana	Paraguay	Uruguay
Bolivia	Dominica	Haiti	Peru	Venezuela
Brazil	Dominican Republic	Honduras	Saint Kitts and Nevis	

MAY 2024

An unknown cyberactor used a compromised vendor account to contact an employee of a Nevada-based CC that specializes in microelectronics. The cyberactor called the CC employee and claimed to be an employee of a named U.S. entity and urged the CC employee to log in to the vendor console using the link provided via a text message, to complete a security update. When the CC employee was unable to log in through the text message, the cyberactor also sent the link via email from the compromised vendor account. Immediately after the phone call and email, the CC began receiving emails from unknown accounts registered to the CC's domain. CC network logs revealed more than 100 failed log in attempts from the compromised CC employee trying to access the CC's network environment.

MID 2024

A representative of a Western Hemisphere ENC sent an unsolicited email offer for a paid consultation to a CC employee. The representative requested the CC employee provide information about microelectronics design for an unnamed end user. The CC is a trusted supplier for the U.S. Department of War, providing sensitive technology; disclosing microelectronics design information could benefit an adversary's defense technology development.

MID 2024

A representative of a Western Hemisphere aircraft manufacturer sent an unsolicited email to purchase export-controlled jet engines from a CC. The engines were intended for use in a UAS for an unnamed client located in Europe and Eurasia. When the purchase request was denied, the Western Hemisphere manufacturer sent a follow-up email requesting to purchase an ITAR-restricted engine designed for use in cruise missiles, again for an unnamed end user. These technologies have a clear application in weapons systems.

EARLY 2024

A representative of a Western Hemisphere defense company visited several CC display booths after hours at an overseas defense show. The defense company representative was also observed taking multiple photographs of various CC products, which included models of combat aircraft and UASs. Representatives of this same Western Hemisphere defense company were previously observed at another exhibition entering the restricted pavilion of a major East Asia and the Pacific state-owned enterprise.


Page Left Intentionally Blank

Sub-Saharan Africa

Overview

In FY 2024, Africa entities comprised less than 1 percent of overall reporting of attempts to access U.S. sensitive and classified information resident in the cleared DIB. The Africa region continued to face numerous national security challenges, including political instability, transnational terrorism, and intrastate and regional conflicts. Many Africa entities sought access to U.S. technologies and services to strengthen their national security by enhancing military capabilities against local and regional adversaries and to safeguard critical infrastructure. Throughout FY 2024, Africa entities targeted few IBTL categories, emphasizing Space Systems and Services and Oher Products. Africa regional entities from countries currently engaged in ongoing conflicts requested access to a restricted satellite imagery database, military training, anti-jamming technologies, and unmanned combat vehicles.

Africa region entities primarily engaged with cleared industry through Request for Information and Résumé Submissions. In addition to Individuals requesting restricted satellite imagery, Individuals from the region also sought positions at CC facilities and academic institutions. Africa government and commercial entities most often sought military equipment and training on behalf of Africa military forces currently engaged in conflict.

Top Targeted Technology	
	Space Systems
	Services and Other Products
	Software
Methods of Operation	
	Request for Information/Solicitation
	Résumé Submission
	Exploitation of Insider Access
Methods of Contact	
	Web Form
	Email
	Résumé—Professional
Collector Affiliation	
	Individual
	Commercial
	Government

Sub-Saharan Africa — Vignettes

F.Y. 2024

Several individuals from an Africa countries submitted web form requests to a CC for access to a satellite imagery database. The requests each included a separate name, email address, country of citizenship, and country of origin, but did not specify the end user or end use of the requested information. The country is currently involved in a large intrastate conflict.

MID 2024

An African military advisor for an Africa government sent a Web Form request to a CC for tactical special operations training. The advisor stated the intent was to field a military force capable of operating behind enemy lines and requested information about the CC's experience in conducting such training. Additionally, the military advisor asked what other foreign militaries the CC worked with.

MAR 2023

An Africa government representative requested to purchase unmanned ground combat vehicles. The government is currently involved in ongoing conflicts, including military efforts against a transnational terrorist group.

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


Page Left Intentionally Blank

Page Left Intentionally Blank

Industrial Base Technology List

Aeronautic Systems
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
An academic field of research merging psychology and neuroscience. The goal 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)
C4 hardware 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
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
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
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
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

Combat and non-combat vehicle designs and capabilities. This includes the engines and transmissions used to maneuver ground systems.

Lasers

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

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

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 engineereed 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

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 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)
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
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 attachès, foreign liason 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.

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 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.

Request for Information/Solicitation
Collecting protected information by directly or indirectly asking or eliciting personnel or protected information or 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 MC.

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

Cyber Operations
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.

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.

Page Left Intentionally Blank

Defense Counterintelligence and Security Agency
27130 Telegraph Road
Quantico, Virginia 22134