ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS

FEBRUARY 2013

Acknowledgement

This strategy is the product of a collaborative effort and reflects the recommendations and input from various entities of the U.S. government, including the Departments of Commerce, Defense, Homeland Security, Justice, State, Treasury, the Office of the Director of National Intelligence and the Office of the United States Trade Representative. This strategy reflects the research and reporting by the Departments of Commerce and Defense as well as the Office of the National Counterintelligence Executive respectively.

Table of Contents

Administration Strategy on Mitigating the Theft of U.S. Trade Secrets

"We are going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century."

—President Barack Obama

Introduction

"We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

—President Barack Obama

The Administration is focused on protecting the innovation that drives the American economy and supports jobs in the United States. As a Nation, we create products and services that improve the world's ability to communicate, to learn, to understand diverse cultures and beliefs, to be mobile, to live better and longer lives, to produce and consume energy efficiently and to secure food, nourishment and safety. Most of the value of this work is intangible—it lies in America's entrepreneurial spirit, our creativity, ingenuity and insistence on progress and in creating a better life for our communities and for communities around the world. These intangible assets are often captured as intellectual property—copyrights, patents, trademarks and trade secrets, and reflect America's advantage in the global economy.

Emerging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating.[1] There appears to be multiple vectors of attack for persons and governments seeking to steal trade secrets. Foreign competitors of U.S. corporations, some with ties to foreign governments, have increased their efforts to steal trade secret information through the recruitment of current or former employees.[2] Additionally, there are indications that U.S. companies, law firms, academia, and financial institutions are experiencing cyber intrusion activity against electronic repositories containing trade secret information.[3] Trade secret theft threatens American businesses, undermines national security, and places the security of the U.S. economy in jeopardy. These acts also diminish U.S. export prospects around the globe and put American jobs at risk.

As an Administration, we are committed to continuing to be vigilant in addressing threats—including corporate and state sponsored trade secret misappropriation—that jeopardize our status as the world's leader for innovation and creativity. We will continue to act vigorously to combat the theft of U.S. trade

1. The Office of the National Counterintelligence Executive (ONCIX), "Foreign Spies Stealing US Economic Secrets In Cyberspace", November 2011, at 1, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

2. See ONCIX Report, supra note 1, at 8. When trade secrets are misappropriated by current or former employees, this method is referred to as an insider or "mole" operation.

3. See ONCIX Report, supra note 1, at 5.

secrets that could be used by foreign companies or foreign governments to gain an unfair economic edge. Departments across the U.S. government have roles in protecting trade secrets and preserving our nation's economic and national security. This strategy recognizes the crucial role of trade secrets in the U.S. economy and sets out a means for improved coordination within the U.S. government to protect them.

Strategy Action Items

1. Focus Diplomatic Efforts to Protect Trade Secrets Overseas

"Where every nation plays by the rules…and intellectual property and new technologies that fuel innovation are protected."

—President Barack Obama

In order to protect American innovation globally, trading partners must treat trade secret theft as a serious issue. The Administration, through the appropriate agencies, will take several steps to ensure this is the case.

Sustained and Coordinated International Engagement with Trading Partners

The Administration will continue to apply sustained and coordinated diplomatic pressure on other countries to discourage trade secret theft. This will be achieved by utilizing a whole of government approach directed at a sustained, consistent and coordinated message from all appropriate agencies to foreign governments where there are regular incidents of trade secret theft. Other governments must recognize that trade secret protection is vital to the success of our economic relationships and that they must take steps to strengthen their enforcement against trade secret theft.

The theft of U.S. trade secrets by foreign competitors or foreign governments has been and will continue to be raised by the most senior levels of the Administration with countries of concern. The relevant Federal agencies, including the Departments of Commerce, Defense, Justice, Homeland Security, State, Treasury and the U.S. Trade Representative, as appropriate, will continue to make it clear to the governments of those nations the importance the U.S. places on the protection of trade secrets and to press those governments to take action to reduce and resolve incidents of trade secret theft.

To assist in this effort, the Department of State will track scheduled diplomatic engagements and meetings by senior Administration officials with governments of countries where there are regular incidents of trade secret theft or that may be complicit in trade secret theft. During these meetings, senior Administration officials will deliver appropriate messages to their foreign counterparts to express the Administration's focus on reducing the incidents of trade secret theft, including improved legal frameworks, stronger enforcement of existing laws and strong and efficient remedies for trade secret owners.

Additionally, the Departments of Commerce and State and the U.S. Trade Representative will seek to build coalitions with other countries to deliver similar messages to countries of concern and to press jointly, or in coordination, for improved protection of trade secrets.

The Department of State and the U.S. Patent and Trademark Office (USPTO), through the USPTO's intellectual property Attachés, will also ensure that U.S. embassies located in countries that are known to present high-risk conditions for trade secret theft will incorporate trade secret protection into their established Intellectual Property Rights (IPR) Working Group plans, with input from appropriate agencies. The annual work plans will include concrete steps to work with the host government to address

trade secret theft. The identified embassies will also include discussions of trade secret issues as part of the IPR Working Groups' regular internal meetings in order to improve communication and coordination inside the embassies. The Embassy-led Working Groups will also enhance engagement with U.S. industry representatives in their host countries on trade secret theft issues.

Theft of Ford Motor Company Trade Secrets

In April 2011, Yu Xiang Dong was sentenced to 70 months in federal prison for theft of trade secrets and economic espionage. Yu was a former Ford Motor Company employee who resigned to work at Beijing Automotive Company. He copied 4,000 Ford documents onto an external hard drive, which he took to China. Ford valued the loss of the trade secrets at $50 million dollars.

Trade Policy Tools

The Administration will utilize trade policy tools to increase international enforcement against trade secret theft to minimize unfair competition against U.S. companies. The U.S. Trade Representative (USTR) will make additional efforts to promote adequate and effective protection and enforcement of trade secrets. These Administration efforts will include:

- Deeper cooperation with trading partners that share U.S. interests with the objective of promoting enhanced trade secret and other intellectual property protection in ways that are consistent with U.S. approaches and helpful in curbing trade in goods and services containing stolen trade secrets;
- Targeting weaknesses in trade secret protection through enhanced use of the annual Special 301 process[4], including the Special 301 Report, action plans and related tools to gather and, where appropriate, act upon information about the adequacy and effectiveness of trade secret protection by U.S. trading partners;
- Seeking, through USTR-led trade negotiations such as the Trans Pacific Partnership, new provisions on trade secret protections requiring parties to make available remedies similar to those provided for in U.S. law; and
- Continuing to raise trade secret protections as a priority issue in all appropriate bilateral, regional, and multilateral trade discussions and appropriate trade and IP-related forums, including the Trade-Related Aspects of Intellectual Property Rights Council and the Asia-Pacific Economic Cooperation, informed by interagency and stakeholder input regarding partners and issues of concern.

4. Through an extensive Special 301 interagency process, USTR publishes a report annually, known as the Special 301 Report, which designates countries of concern on different watch lists, referred to as "priority watch list" (PWL), "watch list" and "priority foreign country." Countries placed on the PWL are the focus of increased bilateral attention concerning the problem areas which will include trade secret protection. USTR also develops action plans and similar documents to establish benchmarks, such as legislative, policy or regulatory action, and as a tool to encourage improvements by countries in order to be removed from the Special 301 list.

International Law Enforcement Cooperation

International law enforcement cooperation is a critical part of combating the global nature of trade secret theft. To assist in domestic investigations of trade secret theft with an international element, Federal law enforcement agencies will also use, as appropriate, formal cooperative agreements or arrangements with foreign governments as a tool to strengthen relationships and investigative efforts. Federal law enforcement agencies will encourage cooperation with their foreign counterparts to:

- Enhance efforts to pursue domestic investigations of trade secret theft by foreign entities; and
- Encourage foreign law enforcement to pursue those targets themselves.

International Training and Capacity Building

The Department of Commerce will use existing programs[5] to educate foreign government officials and increase foreign capacity to protect trade secrets from theft and unlawful commercialization.

The Department of Justice and the Federal Bureau of Investigation, in collaboration with the Departments of Homeland Security and State, will include trade secret theft awareness and enforcement instruction in applicable international law enforcement training forums, such as the International Law Enforcement Academies and in country specific training missions.

International Organizations

The Administration will work with global organizations to strengthen international enforcement efforts and increase cross-border diplomatic and law enforcement cooperation. These efforts will include:

- The Departments of Commerce, Homeland Security, State, and Treasury and USTR will work with international organizations to ensure that there is robust trade secret protection abroad.
- The Department of Justice will continue to work with the European Police Organization and the International Criminal Police Organization on collaborative efforts to address trade secret misappropriation from the U.S. to recipients located abroad.

Theft of DuPont Trade Secrets

Hong Meng was a research chemist for DuPont. He was involved in researching Organic Light Emitting Diodes (OLED). DuPont's OLED research efforts resulted in the development of a breakthrough and proprietary chemical process for OLED displays. Mr. Meng stole trade secret compounds and passed them to a Chinese university. He was caught by the FBI and prosecuted by the U.S. Attorney's Office for the District of Delaware and was sentenced to 14 months in federal prison. DuPont valued the loss of the trade secrets at $400 million dollars.

5. The Department of Commerce has established the Intellectual Property Attaché Program and the USPTO Global Intellectual Property Academy to facilitate capacity building with foreign governments.

2. Promote Voluntary Best Practices by Private Industry to Protect Trade Secrets

"In America, innovation doesn't just change our lives. It's how we make a living."

—President Barack Obama

Advancements in technology, increased mobility, rapid globalization, and the anonymous or pseudonymous nature of the Internet create growing challenges in protecting trade secrets.[6] Companies need to consider whether their approaches to protecting trade secrets keeps pace with technology and the evolving techniques to acquire trade secrets enabled by technology. The Administration encourages companies to consider and share with each other practices that can mitigate the risk of trade secret theft. These best practices should encompass a holistic approach to protect trade secrets from theft via a wide array of vulnerabilities.

Support and Promote Voluntary Best Practices

The U.S. Intellectual Property Enforcement Coordinator (IPEC), working with appropriate U.S. government agencies, including the Departments of Justice and State, will help facilitate efforts by organizations and companies to develop industry led best practices to protect trade secrets. The Administration will encourage companies and industry associations to develop and adopt voluntary best practices, consistent with anti-trust laws, and help highlight those practices. Many private sector companies have recently begun to focus on examining their procedures in order to understand the threat and potential impact of trade secret misappropriation. These organizations are already working to develop best practices that companies can voluntarily implement to protect themselves against trade secret theft. The Administration will work to support groups crafting industry-driven initiatives that meet these objectives.

Identified best practices may not be suitable for every company or organization. Whether or not specific information is regarded as a trade secret is a matter determined by an individual company, not by industry at large. Additionally, for information to be legally protected as a trade secret, businesses need only take reasonable measures to protect the secrecy of such information which may vary by company and by industry. In practice, however, businesses may choose to take additional measures to protect trade secret information where appropriate. In identifying and promoting the adoption of best practices, it should be emphasized that such guidelines are intended solely to offer suggestions to assist businesses in safeguarding information they wish to keep secret and are not designed to be a minimum standard of protection.

The Administration encourages organizations and companies to examine internal operations and policies to determine if current approaches are mitigating the risks and factors associated with trade secret misappropriation committed by corporate and state sponsors. Some areas that private industries could consider for voluntary best practices include:

6. See ONCIX Report, supra note 1, at i-ii

- Research and development compartmentalization;
- Information security policies;
- Physical security policies;
- Human Resources policies; and

Theft of General Motors Trade Secrets

On November 30, 2012, a Federal jury in Detroit found Shanshan Du, a former General Motors (GM) engineer, and her husband, Yu Qin, both found guilty of stealing GM trade secrets related to hybrid vehicle technology worth $40 million. Du and Qin tried to pass the trade secrets to Chinese automaker Chery Automobile Company.

3. Enhance Domestic Law Enforcement Operations

"Our workers are the most productive on Earth, and if the playing field is level, I promise you—America will always win."

—President Barack Obama

As a result of the Attorney General's Task Force on Intellectual Property, established in 2010, the Federal Bureau of Investigation (FBI), which has primary responsibility for investigating domestic offenses under the Economic Espionage Act, increased the number of trade secret theft investigations by 29 percent from 2010.

Investigations and Prosecutions of Trade Secret Theft

The Department of Justice has made the investigation and prosecution of corporate and state sponsored trade secret theft a top priority. The Department of Justice and the FBI will continue to prioritize these investigations and prosecutions and focus law enforcement efforts on combating trade secret theft. The FBI is also expanding its efforts to fight computer intrusions that involve the theft of trade secrets by individual, corporate, and nation-state cyber hackers. The Department of Homeland Security component law enforcement agencies will continue to work cooperatively with the Department of Justice when its investigations uncover evidence of trade secret theft.

Theft of Cargill and Dow Chemical Trade Secrets

In October 2011, Kexue Huang, a former employee of both Cargill and Dow Chemical passed trade secret information to a Chinese university that was developing organic pesticides on behalf of China's government. Financial losses to both companies from his criminal acts exceed $7 million. In December 2011, after many months of hard work by FBI agents, CCIPS prosecutors and the U.S. Attorneys' Offices in Indiana and Minnesota, Huang was sentenced to 87 months in prison—the strongest sentence possible.

Law Enforcement and Intelligence Information Sharing

The Office of the Director of National Intelligence (ODNI)

ODNI will coordinate within the intelligence community to inform the private sector about ways to identify and prevent the theft of trade secrets that benefit a state sponsor or an entity with ties to a foreign government. ODNI will coordinate expanded discussions between the intelligence community and the private sector, focusing on four main aspects of the threat posed by trade secret theft:

- The number and identity of foreign governments involved in trade secret misappropriation;
- The industrial sectors and types of information and technology targeted by such espionage;
- The methods used to conduct such espionage; and
- The dissemination, use, and associated impact of information lost in trade secret misappropriation.

ODNI, though the Office of the National Counterintelligence Executive (ONCIX) will also counter the threat of trade secret misappropriation by sharing threat warning and awareness information with the private sector, as well as imparting counterintelligence tradecraft procedures tailored to the private sector.[7] In order to support this strategy, ONCIX will brief trade association groups and conferences on industry specific threats.

Report to Congress on Foreign Economic Collection & Industrial Espionage

In its November 2011 report to Congress, ONCIX determined that foreign collectors may have the greatest interest in the following areas:

- Information and communications technology;
- Business information that pertains to supplies of scarce natural resources or that provides foreign actors an edge in negotiations with U.S. businesses or the U.S. government;
- Military technologies, particularly marine systems, unmanned aerial vehicles, and other aerospace/aeronautic technologies; and
- Civilian and dual-use technologies in sectors likely to experience fast growth, such as clean energy and health care or pharmaceuticals.

The ONCIX also explored characteristics that make U.S. businesses more vulnerable to trade secret misappropriation including the use of portable devices; storage of information; globalization of economic activities; digitization of business records, research results, and other sensitive economic or technology-related information. A company within one of the four categories identified above is even more susceptible, when these high-risk factors are also present. The report also identified other risk factors. For example:

- The increase in data access points created by conducting business on smartphones and other mobile devices and storing information in the "cloud" increases the opportunities for malicious actors to steal or manipulate information.
- Companies with employees who work remotely are also likely to be at an increased risk of theft.

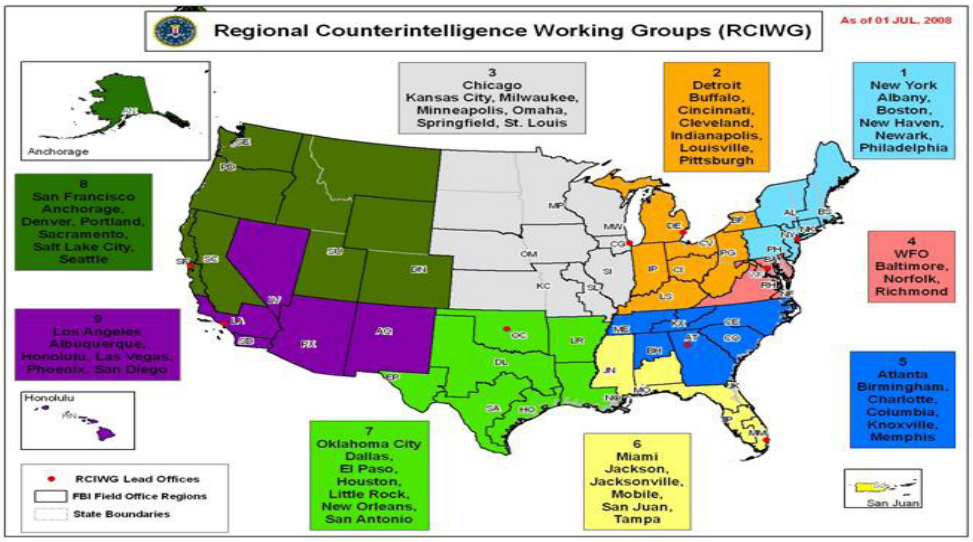
7. The Counterintelligence Enhancement Act of 2002, Public Law 107-306, authorizes ONCIX to carry out and coordinate outreach programs and activities on counterintelligence to other elements of the U.S. government and the private sector. These activities include vulnerability surveys of the private sector.

The Department of Justice

The Department of Justice and the FBI will continue to report on trade secret investigations and prosecutions.[8] Additionally, the FBI will continue its outreach and education efforts with the private sector through various local, regional and national initiatives. At the local level, each of the FBI's 56 field offices will continue to work with academic institutions, manufacturers, laboratories and other entities that are located within the field office's area of responsibility and are perceived as being potentially at risk for trade secret theft. At the regional level, the FBI will continue to meet regularly with other government agencies, industry, and academia to share information about insider threats, economic espionage and trade secret theft.

Theft of Valspar Trade Secrets

David Yen Lee worked for Valspar, an Indiana paint company. He stole trade secrets from Valspar and tried to pass them to Nippon Paint in China. Mr. Lee purchased a plane ticket to China, but was caught by the FBI before he could leave the U.S. On December 8, 2010, Mr. Lee was sentenced to 18 months in prison. Valspar valued the trade secrets between $7 and $20 million.



The FBI's headquarters will review the effectiveness of its local and regional efforts with a focus on the extent of outreach to companies and entities such as cleared defense contractors[9], universities, hospitals, high science companies, and emerging technology firms. The FBI will continue to engage with

8. The Department of Justice and the FBI are required to submit an annual report to the United States Congress pursuant to section 404 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008, Public .Law 110-403.

9. The term "cleared defense contractor" means a private entity granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense.

trade secrets owners through several national outreach organizations, including the Domestic Security Alliance Council, the National Security Business Alliance Council, and InfraGard, and will continue to work closely with various Information Sharing and Analysis Centers. These local, regional and national efforts will continue to reach a broad swath of companies in multiple sectors such as information technology, communications, aeronautics, engineering, energy, financial services, and consumer retail. The FBI's engagement with the private sector promotes reasonable safeguards based on recent intelligence, case studies, and emerging trends.

The Department of Justice and the FBI will continue to train prosecutors and investigators on trade secret theft with the goal of increasing the number of successful investigations and prosecutions for violations of the Economic Espionage Act. These training events will target domestic law enforcement officers, prosecutors, and international partners. These events will include both a trade secret specific curriculum as well as broader intellectual property rights enforcement themes in which trade secret theft is a component

The National Intellectual Property Rights Coordination Center

The National Intellectual Property Rights Coordination Center will obtain leads regarding trade secret misappropriation through its "Report IP Theft" Initiative.

Theft of Motorola Trade Secrets

In November 2011, Customs and Border Protection officers at Chicago's O'Hare Airport stopped Hanjuan Jin, a former Motorola software engineer, while she was allegedly carrying 1,000 sensitive Motorola documents, $30,000 in cash, and a one-way ticket to China. Jin was in the process of traveling to China to turn over stolen trade secret information relating to mobile telecommunications to Kai Sun News Technology Co., also known as SunKaisens, and to the Chinese military.

The Department of Defense

The Department of Defense, through the Defense Security Service, will collect, analyze and report on threat information to cleared industries that support Department of Defense programs and the missions of other U.S. government departments and agencies. The Defense Security Service, in coordination with its partner agencies, will continue to provide advice to those cleared industry partners and deliver security training and education on counterintelligence. Through its annual report on trend analysis of threats targeting to U.S. defense technologies, the Defense Security Service will continue to communicate its analysis to industrial partners of the U.S. government.

The Defense Intelligence Agency will co-chair the National Critical Systems and Joint Technology Task Force with the FBI. This effort will continue to provide a collaborative forum to provide input into the counterintelligence efforts to protect critical and emerging technologies by Federal agencies

4. Improve Domestic Legislation

"Congress should make sure that no foreign company has an advantage over American manufacturing."

—President Barack Obama

In March 2011, the Administration directed federal agencies to review relevant existing Federal intellectual property laws. The goal of this review was to assess if current laws were effective in combatting infringement and protected intellectual property rights. Based on that review, the IPEC sent to Congress the Administration's 2011 White Paper on Intellectual Property Enforcement Legislative Recommendations (White Paper). This document recommended legislation to increase the statutory maximum for economic espionage (18 USC §1831) from 15 years in prison to at least 20 years. Additionally, the Administration also recommended legislation to direct the U.S. Sentencing Commission to consider increasing the U.S. Sentencing Guideline range for the theft of trade secrets and economic espionage, including trade secrets transferred or attempted to be transferred outside the U.S.

The White Paper supported the efforts of Members of Congress who worked in a bicameral and bipartisan manner to introduce legislation to improve the protection of trade secrets in the 112th Congress. President Obama signed two important pieces of legislation into law that will have an immediate and positive impact on prospective trade secret prosecutions:

- **Public Law112-236—*The Theft of Trade Secrets Clarification Act of 2012* (S. 3642)**, closed a loophole in the Economic Espionage Act that had allowed the theft of valuable trade secret source code.[10] This legislation was introduced by Senate Judiciary Chairman Senator Patrick Leahy in response to the Second Circuit decision in United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012), which overturned a verdict that found that the defendant violated 18 U.S.C. §1832(a) by stealing proprietary computer code, a trade secret, from his employer. This legislation was in line with the overall IPEC objective of protecting trade secrets from misappropriation.
- **Public Law 112-269—*The Foreign and Economic Espionage Penalty Enhancement Act of 2012* (H.R. 6029/S. 678)**, bolstered criminal penalties for economic espionage and directed the Sentencing commission to consider increasing offense levels for trade secret crimes.[11] Its passage is an important step in ensuring that penalties are commensurate with the economic harm inflicted on trade secret owners. The passage of this legislation could not have been achieved without the efforts of former House of Representatives Judiciary Chairman Representative Lamar Smith and retired Senator Herb Kohl.

The Administration will continue to ensure that U.S. laws are as effective as possible and that they reflect the seriousness of these crimes and the economic harm inflicted on victims. To supplement the proposals contained in the 2011 White Paper, the IPEC will initiate and coordinate a process, working

10. P.L. 112-236, The Theft of Trade Secrets Clarification Act, available at http://www.gpo.gov/fdsys/pkg/BILLS-112s3642enr/pdf/BILLS-112s3642enr.pdf

11. H.R. 6029EH, Foreign and Economic Espionage Penalty Enhancement Act, available at http://www.gpo.gov/fdsys/pkg/BILLS-112hr6029eh/pdf/BILLS-112hr6029eh.pdf

with appropriate Executive Branch agencies, to review existing Federal laws to determine if legislative changes are needed to enhance enforcement against trade secret theft. The initial review process will conclude within 120 days from the date of the release of this Strategy. The Administration, coordinated through the IPEC, will recommend to Congress any proposed legislative changes resulting from this review process.

Theft of Goldman Sachs Trade Secret

Goldman Sachs spent $500 million dollars developing computer source code to support its high frequency trading program. Sergey Aleynikov, a Goldman Sachs computer programmer, resigned from his job to work for a competitor, and on his final day of employment transferred this extremely valuable proprietary computer code to an external computer server. Mr. Aleynikov had also transferred thousands of proprietary computer code files to his home computers. Mr. Aleynikov was investigated by the FBI and prosecuted by the U.S. Attorney's Office of the Southern District of New York. He was sentenced to 97 months in Federal prison. In February 2012, his conviction was overturned by the Second Circuit based on the court's interpretation of the Economic Espionage Act. This loophole was fixed when President Obama signed Public Law 112-236 *The Theft of Trade Secrets Clarification Act of 2012* (S. 3642) on December 28, 2012

5. Public Awareness and Stakeholder Outreach

"What we can do—what America does better than anyone—is spark the creativity and imagination of our people."

—President Barack Obama

Highlighting can help mitigate the theft of trade secrets by encouraging all stakeholders, including the general public, to be aware of the detrimental effects of misappropriation on trade secret owners and the U.S. economy in general. The Administration will continue to conduct education and outreach efforts through the following actions:

- The Department of Commerce will leverage existing resources like www.stopfakes.gov to provide useful information for the private sector such as general information on the threat of trade secret theft, expanded country specific toolkits with information on how to protect trade secrets in priority markets, developments in the laws and enforcement practices of significant trading partners and webinars on trade secret theft awareness.
- U.S. Patent and Trademark Office and International Trade Administration will utilize current "road show" trainings to provide forums to educate the private sector, particularly small and medium sized businesses, regarding the economic implications of corporate and state sponsored trade secret theft.
- The FBI will continue its current public awareness campaign on bringing public attention to the threat posed to the U.S. from trade secret theft.[12]

12. Federal Bureau of Investigation, "Economic Espionage—How To Spot An Insider Threat", May 11, 2012, http://www.fbi.gov/news/stories/2012/may/insider_051112/insider_051112

Appendix

For more information trade secret theft please visit these websites:

- Department of Commerce STOPfakes.gov IPR training module includes an introduction to trade secrets (available at http://www.stopfakes.gov/business-tools/sme-module).
- Special 301 Report released by the U.S. Trade Representative summarizes troubling trends involving trade secrets and forced technology transfer. Pages 17-19 (available at http://www.ustr.gov).
- The Department of State (available at http://www.state.gov/e/eb/tpp/ipe/).
- DOJ National Security Division (available at http://www.justice.gov/nsd/).
- DOJ Criminal Division—Computer Crimes and Intellectual Property Section (available at http://www.justice.gov/criminal/cybercrime/).
- FBI Counterintelligence Division (available at http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage).
- National Intellectual Property Rights Coordination Center (available at http://www.iprcenter.gov/).
- The Office of the National Counterintelligence Executive (available at http://www.ncix.gov/issues/economic/index.php).
- The Department of Defense – Defense Security Service (available at http://www.dss.mil/documents/ci/Insider-Threats.pdf).
- Create.org study that includes recommendations for companies operating in foreign countries to mitigate the risk of trade secret theft (available at http://www.create.org/views-blog/trade-secret-theft-managing-growing-threat-supply-chains).
- The World Intellectual Property Organization (WIPO) has more trade secret information specifically designed for small and medium-sized enterprises (available at http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm).

Annex

- **ANNEX A:** U.S. Patent and Trademark Office Overview of U.S. Trade Secret Laws and Changed Landscape
- **ANNEX B:** Summary of Department of Justice Trade Secret Theft Cases
- **ANNEX C:** 2011 Office of the National Counterintelligence Executive Report
- **ANNEX D:** 2012 Department of Defense – Defense Security Service Report

Administration Strategy on Mitigating the Theft of U.S. Trade Secrets

Overview of U.S. Law and Changed Landscape

Overview of U.S. Law

Under U.S. law, trade secrets comprise commercially valuable information not generally known or readily ascertainable to the public that are subject to reasonable measures to maintain its confidentiality. Typical examples include confidential formulas, manufacturing techniques, and customer lists. Trade secret law offers protection from trade secret "misappropriation": the unauthorized acquisition, use, or disclosure of such secrets obtained by some improper means. But discovery of a trade secret by fair, lawful methods, such as reverse engineering or independent development, is permitted.

In the United States, civil private enforcement of trade secret protection is primarily a state law matter. However, the federal Economic Espionage Act of 1996 criminalizes some forms of trade secret theft and also empowers the U.S. Attorney General to initiate civil public enforcement proceedings. State law protection of trade secrets has its origin in the common law. These common law principles were first gathered and summarized in the 1939 Restatement (First) of Torts, and later in the 1995 Restatement (Third) of Unfair Competition. Beginning in the 1980s, states began to adopt provisions set forth in the Uniform Trade Secrets Act (UTSA) as a statutory basis for trade secret law. The UTSA, and various state measures provide for injunctive relief, damages, and in some instances attorney's fees as remedies to trade secret misappropriation. Under the UTSA, injunctive relief may be granted for "[a]ctual or threatened misappropriation." An injunction will be terminated when the trade secret ceases to be a trade secret. However, the injunction may be "continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation," or "head start," that the misappropriator gained over one who set out to discover the trade secret through legitimate means such as reverse engineering. The UTSA also provides for recovery of damages, calculated by the actual loss caused by the misappropriation and any separate unjust enrichment. Exemplary damages up to twice that amount may be awarded in the case of willful and malicious misappropriation. Under the UTSA, a court may award attorney's fees to the prevailing party in instances of bad faith or willful and malicious misappropriation.

A controversial and regularly recurring issue in U.S. civil trade secret law is the doctrine of inevitable disclosure. Courts accepting the doctrine reason that an employee who learns a trade secret on the job and then leaves to work for a competitor may "inevitably" disclose the trade secret. To address this perceived problem, these courts frequently enter injunctions prohibiting such employees from working for competitors because the inevitable disclosure of the trade secrets would constitute misappropriation. The practical effect of adopting this principle is that, even absent a formal non-compete agreement, employers may be able to enjoin former employees from working for competitors, because the employee is bound by an implied covenant. Not all courts have adopted this principle.

The federal government currently protects trade secrets through both the criminal and the public civil enforcement sections of the Economic Espionage Act of 1996 ("EEA"), which is codified in 18 U.S.C. §§ 1831-39. Under section 1831, which addresses the more severe crime of economic espionage, it is a felony to knowingly steal or misappropriate a trade secret to "benefit any foreign government, foreign instrumentality, or foreign agent." Section 1832 addresses the theft of trade secrets "related to or included in a product that is produced for or placed in interstate or foreign commerce." It makes it a crime to knowingly steal or misappropriate a trade secret "to the economic benefit of anyone other

than the owner thereof" if the accused party "intend[s] or know[s] that the offense will . . . injure any owner of that trade secret."

The EEA applies to trade secret violations committed both domestically and outside the United States. However, it is only applicable to conduct occurring outside of the United States if the offender is a U.S. citizen or permanent resident alien or an organization organized under U.S. law, or if an act in furtherance of the offense was committed in the United States. The Attorney General may, in a public civil enforcement action, obtain injunctive relief to prevent further violations of the EEA, but the EEA does not provide a private civil right of action.

CHANGED LANDSCAPE

Current literature on trade secret protection points to significant shifts in the nature of trade secret theft and the resulting challenges presented. The nature, protection, and enforcement of a trade secret are distinct from other forms of intellectual property. Unlike other forms of intellectual property, once disclosed publicly, the property right itself ceases to exist. Protection is provided to trade secrets only when steps are taken by the owner to maintain the secrecy of the information. Liability is not imposed for mere theft absent a showing of reasonable efforts to maintain secrecy; continual vigilance is required. What constitutes reasonable efforts is often a pivotal issue in trade secret litigation and particularly important in the digital environment.

The technologies that have made the digital revolution possible also present significant threats to the protection of intellectual property, and trade secrets in particular. Advancements in technology, increased mobility, globalization, and the anonymous/pseudonymous nature of the internet are all working together to create growing challenges in protecting trade secrets. This technology has resulted in companies needing to re-evaluate what constitutes adequate protection of trade secrets in digital format and has impacted the manner in which the trade secrets are stolen. The same technologies that have been a catalyst to the economic growth of both businesses and economies have created a new and threatening environment for the protection of vital assets. These new technologies make it easier to store, access, disseminate, and publish confidential information, thereby enhancing the likelihood that a trade secret may be lost.

The internet in particular has become an innovation that can significantly affect trade secrets. Once a trade secret has been posted on the internet, it has the potential to become "generally known" within a short time period, thereby losing its status as a trade secret. It is in the best interest of the owner of the proprietary information to have the trade secret removed as quickly as possible. Many courts have taken the position that the publication of a trade secret on the internet results in the loss of the secret status of the information, making the claim unenforceable. Given the incomplete remedial nature of removing information from the internet, prevention from disclosure is the strongest weapon and immediate removal should be sought if prevention failed.

In the ONCIX 2011 *Report to Congress on Foreign Economic Collection and Industrial Espionage* there is a shift in focus from previous reports and the threat from cyberspace is highlighted. The report notes that:

> Nearly all business records, research results, and other sensitive economic or technology-related information now exist primarily in digital form. Cyberspace makes it possible for foreign collectors to gather enormous quantities of information quickly and with little risk, whether via remote exploitation of victim's computer networks,

downloads of data to external media devices, or e-mail messages transmitting sensitive information.

The pace of change in information and communications technology is projected to increase, bringing additional pressures on maintaining both the secrecy and ownership of trade secrets. The sharing of resources through cloud computing will facilitate a workforce even more mobile than today. Technologies providing greater access to information anytime and anywhere will increasingly rely on the internet, and present new challenges to companies seeking to protect information transmitted by, or contained on, mobile devices. This mobility will contribute to a future in which the defense provided by national borders to trade secret theft is diminished. Technology, however, can also provide tools to prevent and combat theft of electronic information. Through new technology, companies can better determine when and where confidential information has been accessed, copied, distributed, destroyed, etc. Companies can also better monitor the source of information that was misappropriated; for example, digital watermarking can assist in identifying the source of information. The threat to U.S. business of economic espionage coordinated by foreign governments, as opposed to industrial espionage, is of particular concern. Such acts would not only deprive U.S. companies of their valuable information, often to the benefit of foreign competitors who may receive that information from the foreign government, but countering the vast intelligence resources that a foreign government can utilize for such purpose may be a particular challenge for individual companies.

Summary of Department of Justice Economic Espionage and Trade Secret Criminal Cases January 2009 – Present (Updated January 2013)[1]

Trade Secrets to China – On Nov. 30, 2012, a former General Motors engineer and her husband were convicted by a federal jury today in Detroit for conspiring to steal hybrid technology trade secrets from GM with the intent to use them in a joint venture with an automotive competitor in China. Shanshan Du and her husband, Yu Qin were convicted of unlawful possession of trade secrets. The evidence at trial showed that from December 2003 through May 2006, the defendants conspired to steal GM's trade secret information. Du, while employed with GM's hybrid vehicle technology group, provided GM trade secret information relating to hybrid vehicles to her husband, Qin, for the benefit of their private company, Millennium Technology International Inc. (MTI), which the defendants jointly owned and operated. Approximately five days after Du was offered a severance agreement by GM in January 2005, she copied more than 16,000 GM files, including trade secret documents, to an external computer hard drive used for MTI business. A few months later, Qin moved forward on a business venture to provide hybrid vehicle technology to Chery Automobile, an automotive manufacturer based in China and a competitor of GM. This investigation was conducted by the FBI.

Trade Secrets to South Korea – On Oct. 18, 2012, South Korea-based Kolon Industries Inc. and several of its executives and employees were indicted in the Eastern District of Virginia for allegedly engaging in a multi-year campaign to steal trade secrets related to DuPont's Kevlar para-aramid fiber and Teijin Limited's Twaron para-aramid fiber. The indictment seeks forfeiture of at least $225 million in proceeds from the alleged theft of trade secrets from Kolon's competitors and charges Kolon with one count of conspiring to convert trade secrets, four counts of theft of trade secrets and one count of obstruction of justice. Kolon makes a product called Heracron, which is a recent entrant into the para-aramid fiber market as a competitor to products called Kevlar and Twaron. Para-aramid fibers are used to make, for example, body armor, fiber optic cables and automotive and industrial products. Kevlar is produced by E. I. du Pont de Nemours and Company (DuPont), one of the largest chemical companies in the United States. For decades, Kevlar has competed against Twaron, a para-aramid fiber product produced by Teijin Limited, one of the largest chemical companies in Japan. According to the indictment, from July 2002 through February 2009, Kolon allegedly sought to improve its Heracron product by targeting current and former employees at DuPont and Teijin and hiring them to serve as consultants, then asking these consultants to reveal information that was confidential and proprietary. The indictment alleges that in July 2002, Kolon obtained confidential information related to an aspect of DuPont's manufacturing process for Kevlar, and within three years Kolon had replicated it. This successful misappropriation of DuPont's confidential information, the indictment alleges, spurred Kolon leadership to develop a multi-

[1] Available at http://www.justice.gov/nsd/docs/export-case-fact-sheet.pdf

phase plan in November 2005 to secure additional trade secret information from its competitors, by targeting people with knowledge of both pre-1990 para-aramid technology and post-1990 technologies. Kolon is alleged to have retained at least five former DuPont employees as consultants. Kolon allegedly met with these people individually on multiple occasions from 2006 through 2008 to solicit and obtain sensitive, proprietary information that included details about DuPont's manufacturing processes for Kevlar, experiment results, blueprints and designs, prices paid to suppliers and new fiber technology. This investigation was conducted by the FBI.

Military Technical Data and Trade Secrets to China – On Sept. 26, 2012, Sixing Liu, aka "Steve Liu," a native of China with a PhD in electrical engineering who worked as a senior staff engineer for Space & Navigation, a New Jersey-based division of L-3 Communications, was convicted in the District of New Jersey of exporting sensitive U.S. military technology to China, stealing trade secrets and lying to federal agents. The jury convicted Liu of nine of 11 counts of an April 5, 2012 second superseding indictment, specifically six counts of violating the Arms Export Control Act, one count of possessing stolen trade secrets in violation of the Economic Espionage Act, one count of transporting stolen property, and one count of lying to federal agents. The jury acquitted Liu on two counts of lying to federal agents. According to documents filed in the case and evidence presented at trial, in 2010, Liu stole thousands of electronic files from his employer, L-3 Communications, Space and Navigation Division. The stolen files detailed the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles. Liu stole the files to position and prepare himself for future employment in China. As part of that plan, Liu delivered presentations about the technology at several Chinese universities, the Chinese Academy of Sciences, and conferences organized by Chinese government entities. However, Liu was not charged with any crimes related to those presentations. On Nov. 12, 2010, Liu boarded a flight from Newark to China. Upon his return to the United States on Nov. 29, 2010, agents found Liu in possession of a non-work-issued computer found to contain the stolen material. The following day, Liu lied to ICE agents about the extent of his work on U.S. defense technology. The State Department later verified that several of the stolen files on Liu's computer contained technical data that relates to defense items listed on the United States Munitions List. The jury also heard testimony that Liu's company trained him about the United States' export control laws and told him that most of the company's products were covered by those laws. Liu was first arrested on March 8, 2011, in Chicago on a complaint in the District of New Jersey charging him with one count of exporting defense-related technical data without a license. The investigation was conducted by the FBI, ICE and CBP.

Theft of Trade Secrets for Potential Use in China – On Sept. 19, 2012, Chunlai Yang, a former senior software engineer for Chicago-based CME Group, Inc., pleaded guilty in the Northern District of Illinois to two counts of theft of trade secrets for stealing source code and other proprietary information while at the same time pursuing plans to improve an electronic trading exchange in China. Yang admitted that he downloaded more than 10,000 files containing CME computer source code that made up a substantial part of the operating systems for the Globex electronic trading platform. The government maintains that the potential loss was between $50 million and $100 million. Yang began working for CME Group in 2000 and was a senior software engineer at the time of his arrest. Between late 2010, and June 30, 2011, Yang downloaded more than 10,000 computer files containing CME computer source code from CME's secure internal computer system to his CME-issued work computer. He then transferred many of these files from his work computer to his personal USB flash drives, and then transferred many of these files from his flash drives to his personal computers and hard drives at his home. Yang also admitted that he downloaded thousands of others CME files. Yang admitted that he and two unnamed business partners

developed plans to form a business referred to as the Tongmei (Gateway to America) Futures Exchange Software Technology Company (Gateway), whose purpose was to increase the trading volume at the Zhangjiagang, China, chemical electronic trading exchange (the Zhangjiagang Exchange.) The Zhangjiagang Exchange was to become a transfer station to China for advanced technologies companies around the world. Yang expected that Gateway would provide the exchange with technology through written source code to allow for high trading volume, high trading speeds, and multiple trading functions. Yang was indicted on Sept. 28, 2011. This investigation was conducted by the FBI.

Trade Secrets to China – On Sept. 4, 2012, Chinese citizens Ji Li Huang and Xiao Guang Qi were charged in a criminal complaint in the Western District of Missouri with attempting to purchase stolen trade secrets stolen from Pittsburgh Corning for the purpose of opening a plant in China to compete with Pittsburgh Corning. Pittsburgh Corning, headquartered in Pittsburgh, manufactures various grades or densities of cellular glass insulation sold under the trade name FOAMGLAS and had recently made technological advances in the formulation and manufacturing process of FOAMGLAS insulation. According to the complaint, the defendants attempted to pay $100,000 to an FBI cooperating source for confidential and proprietary information stolen from Pittsburgh Corning. The defendants were arrested on Sept. 2, 2012 after meeting with the confidential source who provided them documents that were purportedly stolen trade secrets from the company. The investigation was conducted by the FBI.

Motorola Trade Secrets to China – On Aug. 29, 2012, Hanjuan Jin, a former software engineer for Motorola, was sentenced in the Northern District of Illinois to four years in prison for stealing trade secrets from Motorola, specifically Motorola's proprietary iDEN telecommunications technology, for herself and for Sun Kaisens, a company that developed products for the Chinese military. According to court documents filed in the case, Motorola spent more than $400 million researching and developing iDEN technology in just a matter of years. On Feb. 8, 2012, Jin was found guilty of three counts of stealing trade secrets. Jin, a naturalized U.S. citizen born in China, possessed more than 1,000 electronic and paper Motorola proprietary documents when she was stopped by U.S. authorities at Chicago's O'Hare International Airport as she attempted to travel to China on Feb. 28, 2007. The judge presiding over the case found her not guilty of three counts of economic espionage for the benefit of the government of China and its military. According to the evidence at trial, Jin began working for Motorola in 1998, and took medical leave in February 2006. Between June and November 2006, while still on sick leave, Jin pursued employment in China with Sun Kaisens, a Chinese telecommunications firm that developed products for the Chinese military. Between November 2006 and February 2007, Jin returned to China and did work for Sun Kaisens on projects for the Chinese military. On Feb. 15, 2007, Jin returned to the United States from China and reserved a flight to China scheduled to depart on Feb. 28, 2007. Jin advised Motorola that she was ready to return to work at Motorola, without informing Motorola that she planned to return to China to work for Sun Kaisens. On Feb. 26, 2007, she returned to Motorola, and accessed hundreds of technical documents belonging to Motorola on its secure internal computer network. As she attempted to depart from Chicago to China, authorities seized numerous materials, some of which provided a description of communication feature that Motorola incorporates into its telecommunications products. Authorities also recovered classified Chinese documents describing telecommunication projects for the Chinese military. Jin was charged with theft of trade secrets in an April 1, 2008 indictment. A superseding indictment returned on Dec. 9, 2008 charged her with economic espionage. The investigation was conducted by the FBI, with assistance from U.S Customs and Border Protection.

Trade Secrets to Competitors in China – On May 7, 2012, an indictment returned in the District of Utah in April 2012 was unsealed charging two people and two companies with theft of trade secrets, wire fraud, and conspiracy to commit wire fraud in connection with the alleged theft of trade secrets from Orbit Irrigation Products, an irrigation company headquartered in Utah. The defendants are Janice Kuang Capener and Luo Jun, both citizens of China, as well as Sunhills International LLC, a California company established by Capener; and Zhejiang Hongchen Irrigation Equipment Co., LTD, a Chinese company under contract with Orbit. According to court documents, Capener worked at Orbit from June 2003 through Nov. 1, 2009, including serving chief of operations at Orbit's manufacturing plant in Ningbo, China. Capener allegedly stole Orbit trade secrets relating to sales and pricing and used that information for herself and others to the detriment of Orbit. Capener also allegedly worked with Jun, Sunhills International and Zhejiang Hongchen Irrigation Equipment to devise a scheme to undermine Orbit's position in the marketplace using illegally obtained proprietary pricing information. Capener and Jun were arrested on May 4, 2012. This case was investigated by the FBI.

Military Technical Data and Trade Secrets to China – On April 5, 2012, a second superseding indictment was returned in the District of New Jersey against Sixing Liu, aka "Steve Liu," a native of China with a PhD in electrical engineering who worked as a senior staff engineer for Space & Navigation, a New Jersey-based division of L-3 Communications, from March 2009 through Nov. 2010. The superseding indictment charged Liu with six counts of illegally exporting defense articles / technical data to China, one count of possessing stolen trade secrets, one count of interstate transportation of stolen property, and three counts of false statements to federal agents. Liu, of Deerfield, Ill., was first arrested on March 8, 2011 in Chicago on a criminal complaint filed in the District of New Jersey charging him with one count of exporting defense-related technical data without a license. At Space & Navigation, Liu allegedly worked on precision navigation devices for rocket launchers, missile launch systems, field artillery, smart munitions, and other components being used by and prepared for the U.S. Department of Defense. Liu was never approved to present information related to Space & Navigation's programs or the technology underlying its programs to any outside person or audience. In 2009 and again in 2010, the indictment alleges that Liu traveled to China where he attended and delivered presentations on export-restricted technical data at technology conferences sponsored by Chinese government entities, including the 863 Program. Before leaving for the 2010 conference in China, Liu allegedly downloaded some 36,000 computer files from Space & Navigation to his personal laptop. Upon his return to the United States in November 2010,
U.S. Customs inspectors found him to be in possession of a laptop computer that contained hundreds of documents related to the company's projects, as well as images of Liu making a presentation at a technology conference sponsored by the PRC government. Many of the documents on his computer were marked as containing sensitive proprietary company information and/or export-controlled technical data. The State Department verified that information on the Liu's computer was export-controlled technical data that relates to defense items on the U.S. Munitions List. The investigation was conducted by the FBI and ICE.

DuPont Trade Secrets to China – On March 2, 2012, former DuPont scientist Tze Chao pleaded guilty in the Northern District of California to conspiracy to commit economic espionage, admitting that he provided trade secrets concerning DuPont's proprietary titanium dioxide manufacturing process to companies he knew were controlled by the government of the People's Republic of China (PRC). On Feb. 7, 2012, a grand jury in San Francisco returned a superseding indictment charging Chao and four other individuals, as well as five companies, with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets from DuPont for the benefit of companies

controlled by the PRC. The five individuals named in the indictment were Walter Liew, his wife Christina Liew, Hou Shengdong, Robert Maegerle, and Tze Chao. The five companies named as defendants are Pangang Group Company Ltd; Pangang Group Steel Vanadium Industry Company Ltd; Pangang Group Titanium Industry Company Ltd., Pangang Group International Economic & Trading Co; and USA Performance Technology, Inc. According to the superseding indictment, the PRC government identified as a priority the development of chloride-route titanium dioxide (TiO2) production capabilities. TiO2 is a commercially valuable white pigment with numerous uses, including coloring paint, plastics and paper. To achieve that goal, companies controlled by the PRC government, specifically the Pangang Group companies named in the indictment, and employees of those companies conspired and attempted to illegally obtain TiO2 technology that had been developed over many years of research and development by DuPont. The Pangang Group companies were aided in their efforts by individuals in the United States who had obtained TiO2 trade secrets and were willing to sell those secrets for significant sums of money. Defendants Walter Liew, Christina Liew, Robert Maegerle and Tze Chao allegedly obtained and possessed TiO2 trade secrets belonging to DuPont. Each of these individuals allegedly sold information containing DuPont TiO2 trade secrets to the Pangang Group companies for the purpose of helping those companies develop large-scale chloride route TiO2 production capability in the PRC, including a planned 100,000 ton TiO2 factory at Chongqing, PRC. The Liews, USAPTI, and one of its predecessor companies, Performance Group, entered into contracts worth in excess of $20 million to convey TiO2 trade secret technology to Pangang Group companies. The Liews allegedly received millions of dollars of proceeds from these contracts. The proceeds were wired through the United States, Singapore and ultimately back into several bank accounts in the PRC in the names of relatives of Christina Liew. The object of the defendants' conspiracy was to convey DuPont's secret chloride-route technology to the PRC companies for the purpose of building modern TiO2 production facilities in the PRC without investing in time-consuming and expensive research and development. DuPont invented the chloride-route process for manufacturing TiO2 in the late-1940s and since then has invested heavily in research and development to improve that production process. The global titanium dioxide market has been valued at roughly $12 billion, and DuPont has the largest share of that market. This investigation was conducted by the FBI.

Trade Secrets to U.S. Subsidiary of Chinese Company – On Jan. 17, 2012, Yuan Li, a former research chemist with the global pharmaceutical company Sanofi-Aventis, pleaded guilty in the District of New Jersey to stealing Sanofi's trade secrets and making them available for sale through Abby Pharmatech, Inc., the U.S. subsidiary of a Chinese chemicals company. According to court documents, Li worked at Sanofi headquarters in Bridgewater, N.J., from August 2006 through June 2011, where she assisted in the development of several compounds (trade secrets) that Sanofi viewed as potential building blocks for future drugs. While employed at Sanofi, Li was a 50 percent partner in Abby, which sells and distributes pharmaceuticals. Li admitted that between Oct. 2008 and June 2011, she accessed internal Sanofi databases and downloaded information on Sanofi compounds and transferred this information to her personal home computer. She also admitted that she made the stolen compounds available for sale on Abby's website. This investigation was conducted by the FBI.

Dow Trade Secrets to China – On Jan. 12, 2012, Wen Chyu Liu, aka David W. Liou, a former research scientist at Dow Chemical Company in Louisiana, was sentenced in the Middle District of Louisiana to 60 months in prison, two years supervised release, a $25,000 fine and was ordered to forfeit $600,000. Liu was convicted on Feb. 7, 2011 of one count of conspiracy to commit trade secret theft for stealing trade secrets from Dow and selling them to companies in China, and he was also convicted of one count of perjury. According to the evidence presented in court, Liou came to the United States from China for

graduate work. He began working for Dow in 1965 and retired in 1992. Dow is a leading producer of the elastomeric polymer, chlorinated polyethylene (CPE). Dow's Tyrin CPE is used in a number of applications worldwide, such as automotive and industrial hoses, electrical cable jackets and vinyl siding. While employed at Dow, Liou worked as a research scientist on various aspects of the development and manufacture of Dow elastomers, including Tyrin CPE. The evidence at trial established that Liou conspired with at least four current and former employees of Dow's facilities in Plaquemine, Louisiana, and in Stade, Germany, who had worked in Tyrin CPE production, to misappropriate those trade secrets in an effort to develop and market CPE process design packages to Chinese companies. Liou traveled throughout China to market the stolen information, and he paid current and former Dow employees for Dow's CPE-related material and information. In one instance, Liou bribed a then-employee at the Plaquemine facility with $50,000 in cash to provide Dow's process manual and other CPE-related information. The investigation was conducted by the FBI.

Dow and Cargill Trade Secrets to China – On Dec. 21, 2011, Kexue Huang, a Chinese national and former resident of Indiana, was sentenced to 87 months in and three years supervised release on charges of economic espionage to benefit a foreign university tied to the People's Republic of China (PRC) and theft of trade secrets. On Oct. 18, 2011, Huang pleaded guilty in the Southern District of Indiana to these charges. In July 2010, Huang was charged in the Southern District of Indiana with misappropriating and transporting trade secrets to the PRC while working as a research scientist at Dow AgroSciences LLC. On Oct. 18, 2011, a separate indictment in the District of Minnesota charging Huang with stealing a trade secret from a second company, Cargill Inc., was unsealed. From January 2003 until February 2008, Huang was employed as a research scientist at Dow. In 2005, he became a research leader for Dow in strain development related to unique, proprietary organic insecticides marketed worldwide. Huang admitted that during his employment at Dow, he misappropriated several Dow trade secrets. According to plea documents, from 2007 to 2010, Huang transferred and delivered the stolen Dow trade secrets to individuals in Germany and the PRC. With the assistance of these individuals, Huang used the stolen materials to conduct unauthorized research to benefit foreign universities tied to the PRC. Huang also admitted that he pursued steps to develop and produce the misappropriated Dow trade secrets in the PRC. After Huang left Dow, he was hired in March 2008 by Cargill, an international producer and marketer of food, agricultural, financial and industrial products and services. Huang worked as a biotechnologist for Cargill until July 2009. Huang admitted that during his employment with Cargill, he stole one of the company's trade secrets – a key component in the manufacture of a new food product, which he later disseminated to another person, specifically a student at Hunan Normal University in the PRC. According to the plea agreement, the aggregated loss from Huang's conduct exceeds $7 million but is less than $20 million. This investigation was conducted by the FBI.

Trade Secrets to India – On Nov. 14, 2011, Prabhu Mohapatra was arrested on a criminal complaint in the District of Utah (filed on Nov. 10, 2011) charging him with stealing proprietary information from his employer, a Utah scientific company, and providing it to a relative in India who was starting up a competing company. According to the charges, Mohapatra worked as a senior scientist for Frontier Scientific, Inc., a company that makes large pure quantities of an organic chemical, 2,2'-dipyrromethane, that has several applications, including as an ingredient in new drugs, as well as in solar cells and batteries. The complaint alleges that Mohapatra emailed proprietary information from Frontier Scientific about the chemical to his brother-in-law in India, who was setting up an unregistered, competing company called Medchemblox. The complaint further alleges that Mohapatra had a financial interest in Medchemblox. This investigation was conducted by FBI.

Trade Secrets to Foreign Government – On Aug. 30, 2011, Elliot Doxer, of Brookline, Mass., pleaded guilty in the District of Massachusetts to one count of foreign economic espionage for providing trade secrets over an 18-month period to an undercover FBI agent posing as an Israeli intelligence officer. Neither the government of Israel nor anyone acting on its behalf committed any offense under U.S. laws in this case. Doxer was a former employee of Akamai Technologies, Inc., who in June 2006 sent an e-mail to the Israeli consulate in Boston stating that he worked in Akamai's finance department and was willing to provide information that might help Israel. In Sept. 2007, an undercover FBI agent posing as an Israeli intelligence officer spoke to Doxer and established a "dead drop" where the agent and Doxer could exchange information. From Sept. 2007 through March 2009, Doxer visited the dead drop at least 62 times to leave information, retrieve communications or check for new communications. Doxer provided the undercover agent with Akamai customer lists, employee lists, contract information and other trade secrets. He was arrested on Oct. 6, 2010 on a complaint charging him with wire fraud. That charge was dismissed as part of the plea agreement. Doxer was ultimately sentenced on Dec. 19, 2011 to six months in prison and two years supervised release. The case was investigated by the FBI.

Wire Fraud in Trade Secrets Case Involving China – On April 6, 2011, Yan Zhu, a Chinese citizen in the U.S. on a work visa, was convicted in the District of New Jersey on seven counts of wire fraud in connection with his scheme to steal confidential and proprietary business information relating to computer systems and software with environmental applications from his New Jersey employer. He was acquitted on the charge of conspiracy to steal trade secrets and two counts of unauthorized transmission of trade secrets in interstate or foreign commerce. April 10, 2009, Zhu was arrested on charges of theft of trade secrets, conspiracy, wire fraud, and theft of honest services fraud in connection with a plot to steal software from his former U.S. employer and sell a modified version to the Chinese government after he was fired. Zhu was employed as a senior environmental engineer from May of 2006 until his termination in July of 2008. Zhu worked for a comprehensive multi-media environmental information management portal that developed a proprietary software program for the Chinese market which allows users to manage air emissions, ambient water quality, and ground water quality. Zhu was sentenced on Jan. 5, 2012 to three years of probation and a $700 special assessment. This investigation was conducted by the FBI.

Valspar Trade Secrets to China – On Dec. 8, 2010, David Yen Lee, a former chemist for Valspar Corporation, a Chicago paint manufacturing company, was sentenced in the Northern District of Illinois to 15 months in prison for stealing trade secrets involving numerous formulas and other proprietary information valued up to $20 million as he prepared to go to work for a competitor in China. Lee, formerly a technical director in Valspar Corp's architectural coatings group since 2006, pleaded guilty in Sept. 2010 to using his access to Valspar's secure internal computer network to download approximately 160 original batch tickets, or secret formulas for paints and coatings. Lee also obtained raw materials information, chemical formulas and calculations, sales and cost data, and other internal memoranda, product research, marketing data, and other materials from Valspar. Lee admitted that between September 2008 and February 2009, he had negotiated employment with Nippon Paint, in Shanghai, China and accepted employment with Nippon as vice president of technology and administrator of research and development. Lee was scheduled to fly from Chicago to Shanghai on March 27, 2009. He did not inform Valspar that he had accepted a job at Nippon until he resigned on March 16, 2009. Between November 2008 and March 2009, Lee downloaded technical documents and materials belonging to Valspar, including the paint formula batch tickets. He further copied certain downloaded files to external thumb drives to store the data, knowing that he intended to use the confidential

information belong to Valspar for his own benefit. There was no evidence that he actually disclosed any of the stolen trade secrets. This investigation was conducted by the FBI.

Ford Motor Company Trade Secrets to China – On Nov. 17, 2010, Yu Xiang Dong, aka Mike Yu, a product engineer with Ford Motor Company pleaded guilty in the Eastern District of Michigan to two counts of theft of trade secrets. According to the plea agreement, Yu was a Product Engineer for Ford from 1997 to 2007 and had access to Ford trade secrets, including Ford design documents. In December 2006, Yu accepted a job at the China branch of a U.S. company. On the eve of his departure from Ford and before he told Ford of his new job, Yu copied some 4,000 Ford documents onto an external hard drive, including sensitive Ford design documents. Ford spent millions of dollars and decades on research, development, and testing to develop and improve the design specifications set forth in these documents. On Dec. 20, 2006, Yu traveled to the location of his new employer in Shenzhen, China, taking the Ford trade secrets with him. On Jan. 2, 2007, Yu emailed his Ford supervisor from China and informed him that he was leaving Ford's employ. In Nov. 2008, Yu began working for Beijing Automotive Company, a direct competitor of Ford. On Oct. 19, 2009, Yu returned to the U.S. Upon his arrival, he was arrested. At that time, Yu had in his possession his Beijing Automotive Company laptop computer. Upon examination of that computer, the FBI discovered that 41 Ford system design specifications documents had been copied to the defendant's Beijing Automotive Company work computer. The FBI also discovered that each of those design documents had been accessed by Yu during the time of his employment with Beijing Automotive Company. Yu was ultimately sentenced to 70 months in prison in April 2011. This case was investigated by the FBI.

DuPont Trade Secrets to China – On Oct. 26, 2010, Hong Meng, a former research chemist for DuPont, was sentenced in the District of Delaware to 14 months in prison and $58,621 in restitution for theft of trade secrets. Meng pleaded guilty on June 8, 2010. Meng was involved in researching Organic Light Emitting Diodes (OLED) during his tenure at DuPont. In early 2009, DuPont's OLED research efforts resulted in the development of a breakthrough chemical process (trade secret) that increased the performance and longevity of OLED displays. In the Spring of 2009, while still employed at DuPont and without DuPont's permission or knowledge, Meng accepted employment as a faculty member at Peking University (PKU) College of Engineering, Department of Nanotechnology in Beijing, China, and thereafter began soliciting funding to commercialize his OLED research at PKU. In June 2009, he emailed to his PKU account the protected chemical process from DuPont. He also downloaded the chemical process from his DuPont work computer to a thumb drive which he uploaded to his personal computer. In August 2009, he mailed a package containing 109 samples of DuPont intermediate chemical compounds to a colleague at Northwestern University and instructed his colleague at Northwestern to forward the materials to Meng's office at PKU. Eight of the 109 samples were trade secret chemical compounds. Meng also made false statements to the FBI when questioned about these samples. This investigation was conducted by the FBI.

GM Trade Secrets to China – On July 22, 2010, an indictment returned in the Eastern District of Michigan charging Yu Qin and his wife Shanshan Du, both of Troy, Michigan, was unsealed. The indictment charged the defendants with conspiracy to possess trade secrets without authorization, unauthorized possession of trade secrets and wire fraud. According to the indictment, from December 2003 through May 2006, the defendants conspired to possess trade secret information of General Motors Company relating to hybrid vehicles, knowing that the information had been stolen, converted, or obtained without authorization. The indictment alleges that Du, while employed with GM, provided GM trade secret information relating to hybrid vehicles to her husband, Qin, for his benefit and for the benefit of a company, Millennium Technology International Inc. (MTI), which the defendants owned and

operated. Five days after Du was offered a severance agreement by GM in January 2005, she copied thousands of GM documents, including trade secret documents, to a computer hard drive used for MTI business. A few months later, Qin moved forward on a new business venture to provide hybrid vehicle technology to Chery Automobile, a Chinese automotive manufacturer based in China and a competitor of GM. The indictment further alleges that in May 2006, the defendants possessed GM trade secret information without authorization on several computer and electronic devices located in their residence. Based on preliminary calculations, GM estimates that the value of the stolen GM documents is over $40 million. This investigation was conducted by the FBI.

Economic Espionage / Theft of Space Shuttle and Rocket Secrets for China – On Feb. 11, 2010 former Rockwell and Boeing engineer Dongfan "Greg" Chung was sentenced to 188 months imprisonment and three years supervised release after his July 16, 2009 conviction in the Central District of California. Chung was convicted of charges of economic espionage and acting as an illegal agent of the People's Republic of China (PRC), for whom he stole restricted technology and Boeing trade secrets, including information related to the Space Shuttle program and the Delta IV rocket. According to the judge's ruling, Chung served as an illegal agent of China for more than 30 years and kept more than 300,000 pages of documents reflecting Boeing trade secrets stashed in his home as part of his mission of steal aerospace and military trade secrets from Boeing to assist the Chinese government. Chung sent Boeing trade secrets to the PRC via the mail, via sea freight, via the Chinese consulate in San Francisco, and via a Chinese agent named Chi Mak. On several occasions, Chung also used the trade secrets that he misappropriated from Boeing to prepare detailed briefings that he later presented to Chinese officials in the PRC. Chung was originally arrested on Feb. 11, 2008, in Southern California after being indicted on eight counts of economic espionage, one count of conspiracy to commit economic espionage, one count of acting as an unregistered foreign agent, one count of obstruction of justice, and three counts of making false statements to the FBI. The investigation was conducted by the FBI and NASA.

COUNTERINTELLIGENCE SECURITY

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE

Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011

October 2011

Table of Contents

Annex A

Annex B

List of Text Boxes

List of Charts

Executive Summary

Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect.

US Technologies and Trade Secrets at Risk in Cyberspace

Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cyber tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the economic espionage threat, and the Intelligence Community (IC) judges the use of such tools is already a larger threat than more traditional espionage methods.

Economic espionage inflicts costs on companies that range from loss of unique intellectual property to outlays for remediation, but no reliable estimates of the monetary value of these costs exist. Many companies are unaware when their sensitive data is pilfered, and those that find out are often reluctant to report the loss, fearing potential damage to their reputation with investors, customers, and employees. Moreover, victims of trade secret theft use different methods to estimate their losses; some base estimates on the actual costs of developing the stolen information, while others project the loss of future revenues and profits.

Pervasive Threat from Adversaries and Partners

Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.

- Chinese actors are the world's most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC cannot confirm who was responsible.
- Russia's intelligence services are conducting a range of activities to collect economic information and technology from US targets.
- Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities.

Outlook

Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment.

- Over the next several years, the proliferation of portable devices that connect to the Internet and other networks will continue to create new opportunities for malicious actors to conduct espionage. The trend in both commercial and government organizations toward the pooling of information processing and storage will present even greater challenges to preserving the security and integrity of sensitive information.

- The US workforce will experience a cultural shift that places greater value on access to information and less emphasis on privacy or data protection. At the same time, deepening globalization of economic activities will make national boundaries less of a deterrent to economic espionage than ever.

We judge that the governments of China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace.

The relative threat to sensitive US economic information and technologies from a number of countries may change in response to international economic and political developments. One or more fast-growing regional powers may judge that changes in its economic and political interests merit the risk of aggressive cyber and other espionage against US technologies and economic information.

Although foreign collectors will remain interested in all aspects of US economic activity and technology, we judge that the greatest interest may be in the following areas:

- Information and communications technology (ICT), which forms the backbone of nearly every other technology.
- Business information that pertains to supplies of scarce natural resources or that provides foreign actors an edge in negotiations with US businesses or the US Government.
- Military technologies, particularly marine systems, unmanned aerial vehicles (UAVs), and other aerospace/aeronautic technologies.
- Civilian and dual-use technologies in sectors likely to experience fast growth, such as clean energy and health care/pharmaceuticals.

Cyberspace provides relatively small-scale actors an opportunity to become players in economic espionage. Under-resourced governments or corporations could build relationships with hackers to develop customized malware or remote-access exploits to steal sensitive US economic or technology information, just as certain FIS have already done.

- Similarly, political or social activists may use the tools of economic espionage against US companies, agencies, or other entities, with disgruntled insiders leaking information about corporate trade secrets or critical US technology to “hacktivist” groups like WikiLeaks.

Scope Note

This assessment is submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359, as amended, which requires that the President biennially submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the *14th Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2008* and draws primarily on data from 2009-2011.

New Focus and Additional Resources Used for This Year's Report

This report differs from previous editions in three important ways. The first and most significant is the focus. This report gives special attention to foreign collectors' exploitation of cyberspace, while not excluding other established tactics and methods used in foreign economic collection and industrial espionage. This reflects the fact that nearly all business records, research results, and other sensitive economic or technology-related information now exist primarily in digital form. Cyberspace makes it possible for foreign collectors to gather enormous quantities of information quickly and with little risk, whether via remote exploitation of victims' computer networks, downloads of data to external media devices, or e-mail messages transmitting sensitive information.

The second difference from prior reports is that, in addition to researching the large body of intelligence reporting and analysis on economic espionage produced by the Intelligence Community, the Department of Defense (DoD), and other US Government agencies, the drafters of this report consulted new sources of government information.

Third, the Office of the National Counterintelligence Executive (ONCIX) mobilized significant resources from outside the IC during the course of this study. This included outreach to the private sector and, in particular, sponsorship of a conference in November 2010 on cyber-enabled economic espionage at which 26 US Government agencies and 21 private-sector organizations were represented. ONCIX also contracted with outside experts to conduct studies of the academic literature on the cost of economic espionage and the role of the cyber "underground economy."

Definitions of Key Terms

For the purposes of this report, key terms were defined according to both legal and analytic criteria.

The **legal criteria** derive from the language in the Economic Espionage Act (EEA) of 1996 (18 USC §§ 1831-1839). The EAA is concerned in particular with economic espionage and foreign activities to acquire US **trade secrets**. In this context, trade secrets are all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored or unstored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, if the owner (the person or entity in whom or in which rightful legal or equitable title to, or license in, is reposed) has taken reasonable measures to keep such information secret and the information derives independent economic value, actual, or potential from not being generally known to, and not being readily ascertainable through, proper means by the public. Activities to acquire these secrets include the following criminal offenses:

- **Economic espionage** occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality or agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1831).

- **Industrial espionage**, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmiting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1832).

The following definitions reflect the experience of IC cyber, counterintelligence, and economic analysts:

- **Cyberspace** is the interdependent network of information technology (IT) infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
- **Sensitive** is defined as information or technology (a) that has been classified or controlled by a US Government organization or restricted in a proprietary manner by a US corporation or other institution, or (b) that has or may reasonably be expected to have military, intelligence, or other uses with implications for US national security, or (c) that may enhance the economic competitiveness of US firms in global markets.

Contributors

ONCIX compiled this report using inputs and reporting from many US Government agencies and departments, including the Air Force Office of Special Investigations (AFOSI), Army Counterintelligence Center (ACIC), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Defense Security Service (DSS), Department of Energy (DoE), Department of Health and Human Services (HHS), Department of State (DoS), Federal Bureau of Investigation (FBI), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Naval Criminal Investigative Service (NCIS).

Foreign Spies Stealing US Economic Secrets in Cyberspace

US Technologies and Trade Secrets at Risk in Cyberspace

The pace of foreign economic collection and industrial espionage activities against major US corporations and US Government agencies is accelerating. FIS, corporations, and private individuals increased their efforts in 2009-2011 to steal proprietary technologies, which cost millions of dollars to develop and represented tens or hundreds of millions of dollars in potential profits. The computer networks of a broad array of US Government agencies, private companies, universities, and other institutions—all holding large volumes of sensitive economic information—were targeted by cyber espionage; much of this activity appears to have originated in China.

Increasingly, economic collection and industrial espionage occur in cyberspace, reflecting dramatic technological, economic, and social changes that have taken place in recent years in the ways that economic, scientific, and other sensitive information is created, used, and stored. Today, nearly all business records, research results, and other sensitive economic data are digitized and accessible on networks worldwide. Cyber collection can take many forms, including: simple visits to a US company's website for the collection of openly available information; a corporate insider's downloading of proprietary information onto a thumb drive at the behest of a foreign rival; or intrusions launched by FIS or other actors against the computer networks of a private company, federal agency, or an individual.

The Appeal of Collecting in Cyberspace

Cyberspace is a unique complement to the espionage environment because it provides foreign collectors with relative anonymity, facilitates the transfer of a vast amount of information, and makes it more difficult for victims and governments to assign blame by masking geographic locations.

Security and attribution. Collectors operating in a cyber environment can collect economic information with less risk of detection. This is particularly true for remote computer network exploitation (CNE). Foreign collectors take advantage of the fact that it is difficult to detect and to attribute responsibility for these operations.

There is increasing similarity between the tools, tactics, and techniques used by various actors, which reduces the reliability of using these factors to identify those responsible for computer network intrusions.

- The proliferation of malicious software (malware) presents opportunities for intelligence services and other actors to launch operations with limited resources and without developing unique tools that can be associated with them.
- Hacker websites are prevalent across the Internet, and tool sharing is common, causing intrusions by unrelated actors to exhibit similar technical characteristics.
- FIS and other foreign entities have used independent hackers at times to augment their capabilities and act as proxies for intrusions, thereby providing plausible deniability.
- Many actors route operations through computers in third countries or physically operate from third countries to obscure the origin of their activity.

Another factor adding to the challenge of attribution is the diverging perspectives of the actual targets of economic espionage in cyberspace.

- At a conference sponsored by ONCIX in November 2010, US private industry representatives said they saw little difference between cybercrime—for example, identity theft or the misappropriation of intellectual property such as the counterfeiting of commercial video or audio recordings—and the collection of economic or technology information by intelligence services or other foreign entities. Private sector organizations are often less concerned with attribution and focus instead on damage control and prevention; moreover, few companies have the ability to identify cyber intruders.

- US Government law enforcement and intelligence agencies, on the other hand, seek to establish attribution as part of their mission to counter FIS and other clandestine information collectors. They, unlike companies, also have the intelligence collection authorities and capabilities needed to break multiple layers of cover and to establish attribution where possible.

Cyberspace also offers greater security to the perpetrator in cases involving insiders. Although audits or similar cyber security measures may flag illicit information downloads from a corporate network, a malicious actor can quickly and safely transfer a data set once it is copied. A physical meeting is unnecessary between the corrupted insider and the persons or organizations the information is being collected for, reducing the risk of detection.

Faster and cheaper. Cyberspace makes possible the near instantaneous transfer of enormous quantities of economic and other information. Until fairly recently, economic espionage often required that insiders pass large volumes of documents to their handlers in physical form—a lengthy process of collection, collation, transportation, and exploitation.

- Dongfan Chung was an engineer with Rockwell and Boeing who worked on the B-1 bomber, space shuttle, and other projects and was sentenced in early 2010 to 15 years in prison for economic espionage on behalf of the Chinese aviation industry. At the time of his arrest, 250,000 pages of sensitive documents were found in his house. This is suggestive of the volume of information Chung could have passed to his handlers between 1979 and 2006.[a] The logistics of handling the physical volume of these documents—which would fill nearly four 4-drawer filing cabinets—would have required considerable attention from Chung and his handlers. With current technology, all the data in the documents hidden in Chung's house would fit onto one inexpensive CD.[b]

[a]Chung was prosecuted only for possession of these documents with the intent to benefit the People's Republic of China (PRC) and acting as an unregistered foreign agent for China. He was not charged with communication of this information to the PRC or any other foreign entity.

[b]On average, one page of typed text holds 2 kilobytes (KB) of data; thus, 250,000 pages x 2 KB/page = 500,000 KB, or 488 megabytes (MB). A data CD with a capacity of 700 MB retails for $0.75, and a flashdrive with a capacity of 4 gigabytes costs about $13.00.

Extra-territoriality. In addition to the problem of attribution, it often is difficult to establish the geographic location of an act of economic espionage that takes place in cyberspace. Uncertainty about the physical location of the act provides cover for the perpetrators and complicates efforts by US Government law enforcement or intelligence agencies to respond.

Non-Cyber Methods of Economic Espionage

Although this assessment focuses on the use of cyber tools and the cyber environment in foreign efforts to collect sensitive US economic information and technologies, a variety of other methods also remain in use.

Requests for Information (RFI). *Foreign collectors make unsolicited direct and indirect requests for information via personal contacts, telephone, e-mail, fax, and other forms of communication and often seek classified, sensitive, or export-controlled information.*

Solicitation or Marketing of Services. *Foreign companies seek entrée into US firms and other targeted institutions by pursuing business relationships that provide access to sensitive or classified information, technologies, or projects.*

Conferences, Conventions, and Trade Shows. *These public venues offer opportunities for foreign adversaries to gain access to US information and experts in dual-use and sensitive technologies.*

Official Foreign Visitors and Exploitation of Joint Research. *Foreign government organizations, including intelligence services, use official visits to US Government and cleared defense contractor facilities, as well as joint research projects between foreign and US entities, to target and collect information.*

Foreign Targeting of US Visitors Overseas. *Whether traveling for business or personal reasons, US travelers overseas—businesspeople, US Government employees, and contractors—are routinely targeted by foreign collectors, especially if they are assessed*

as having access to some sensitive information. Some US allies engage in this practice, as do less friendly powers such as Russia and China. Targeting takes many forms: exploitation of electronic media and devices, surreptitious entry into hotel rooms, aggressive surveillance, and attempts to set up sexual or romantic entanglements.

Open Source Information. *Foreign collectors are aware that much US economic and technological information is available in professional journals, social networking and other public websites, and the media.*

Large but Uncertain Costs

Losses of sensitive economic information and technologies to foreign entities represent significant costs to US national security. The illicit transfer of technology with military applications to a hostile state such as Iran or North Korea could endanger the lives of US and allied military personnel. The collection of confidential US Government economic information—whether by a potential adversary or a current ally—could undercut US ability to develop and enact policies in areas ranging from climate change negotiations to reform of financial market regulations. The theft of trade secrets from US companies by foreign economic rivals undermines the corporate sector's ability to create jobs, generate revenues, foster innovation, and lay the economic foundation for prosperity and national security.

Data on the effects of the theft of trade secrets and other sensitive information are incomplete, however, according to an ONCIX-sponsored survey of academic literature on the costs of economic espionage.

- Many victims of economic espionage are unaware of the crime until years after loss of the information.
- Even when a company knows its sensitive information has been stolen by an insider or that its computer networks have been penetrated, it may choose not to report the event to the FBI or other law enforcement agencies. No legal requirement to report a loss of sensitive information or a remote computer intrusion exists, and announcing a security breach of this kind could tarnish a company's reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders.
- A company also may not want to publicly accuse a corporate rival or foreign government of stealing its secrets from fear of offending potential customers or business partners.
- Finally, it is inherently difficult to assign an economic value to some types of information that are subject to theft. It would, for example, be nearly impossible to estimate the monetary value of talking points for a meeting between officials from a US company and foreign counterparts.

The Cost of Economic Espionage to One Company

Data exist in some specific cases on the damage that economic espionage or theft of trade secrets has inflicted on individual companies. For example, an employee of Valspar Corporation unlawfully downloaded proprietary paint formulas valued at $20 million, which he intended to take to a new job in China, according to press reports. This theft represented about one-eighth of Valspar's reported profits in 2009, the year the employee was arrested.

Even in those cases where a company recognizes it has been victimized by economic espionage and reports the incident, calculation of losses is challenging and can produce ambiguous results. Different methods can be used that yield divergent estimates, which adds to the difficulty of meaningfully comparing cases or aggregating estimated losses.

- An executive from a major industrial company told ONCIX representatives in late 2010 that his company has used historical costs—tallying salaries, supplies, utilities, and similar direct expenses—to estimate losses from cases of attempted theft of its trade secrets. This method has the advantage of using known and objective

data, but it underestimates the extent of losses in many cases because it does not capture the effect of lost intellectual property on future sales and profits.

- Harm is calculated in US civil court cases involving the theft of trade secrets by measuring the "lost profits" or "reasonable royalty" that a company is unable to earn because of the theft. Although this method requires subjective assumptions about market share, profitability, and similar factors, it does offer a more complete calculation of the cost than relying strictly on historical accounting data.
- Estimates from academic literature on the losses from economic espionage range so widely as to be meaningless—from $2 billion to $400 billion or more a year—reflecting the scarcity of data and the variety of methods used to calculate losses.

A Possible Proxy Measure of the Costs of Economic Espionage to the United States

New ideas are often a company's or an agency's most valuable information and are usually of greatest interest to foreign collectors. Corporate and government spending on research and development (R&D) is one measure of the cost of developing new ideas, and hence is an indicator of the value of the information that is most vulnerable to economic espionage. R&D spending has been tracked by the National Science Foundation (NSF) since 1953. For 2008, the most recent year available, the NSF calculated that US industry, the Federal Government, universities, and other nonprofit organizations expended $398 billion on R&D, or 2.8 percent of the US Gross Domestic Product.

Pervasive Threat from Intelligence Adversaries and Partners

Many states view economic espionage as an essential tool in achieving national security and economic prosperity. Their economic espionage programs combine collection of open source information, HUMINT, signals intelligence (SIGINT), and cyber operations—to include computer network intrusions and exploitation of insider access to corporate and proprietary networks—to develop information that could give these states a competitive edge over the United States and other rivals.

- China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of US economic information and technology.
- Other countries with closer ties to the United States have conducted CNE and other forms of intelligence collection to obtain US economic and technology data, often taking advantage of the access they enjoy as allies or partners to collect sensitive military data and information on other programs.

Recent Insider Thefts of Corporate Trade Secrets with a Link to China

David Yen Lee…chemist with Valspar Corporation…between late 2008 and early 2009 used access to internal computer network to download about 160 secret formulas for paints and coatings to his own storage media…intended to take this proprietary information to a new job with Nippon Paint in Shanghai, China…arrested March 2009…pleaded guilty to one count of theft of trade secrets; sentenced in December 2010 to 15 months in prison.

Meng Hong…DuPont Corporation research chemist...in mid-2009 downloaded proprietary information on organic light-emitting diodes (OLED) to personal e-mail account and thumb drive…intended to transfer this information to Peking University, where he had accepted a faculty position; sought Chinese Government funding to commercialize OLED research…arrested October 2009…pleaded guilty to one count of theft of trade secrets; sentenced in October 2010 to 14 months in prison.

Yu Xiang Dong (aka Mike Yu)…product engineer wjth Ford Motor Company who in December 2006 accepted a job at Ford's China branch…copied approximately 4,000 Ford documents onto an external hard drive to help obtain a job with a Chinese automotive company…arrested in October 2009…pleaded guilty to two counts of theft of trade secrets; sentenced in April 2011 to 70 months in prison.

China: Persistent Collector

Chinese leaders consider the first two decades of the 21st century to be a window of strategic opportunity for their country to focus on economic growth, independent innovation, scientific and technical advancement, and growth of the renewable energy sector.

China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to corporate networks to steal trade secrets using removable media devices or e-mail. Of the seven cases that were adjudicated under the Economic Espionage Act—both Title 18 USC § 1831 and § 1832—in Fiscal Year 2010, six involved a link to China.

US corporations and cyber security specialists also have reported an onslaught of computer network intrusions originating from Internet Protocol (IP) addresses in China, which private sector specialists call "advanced persistent threats." Some of these reports have alleged a Chinese corporate or government sponsor of the activity, but the IC has not been able to attribute many of these private sector data breaches to a state sponsor. Attribution is especially difficult when the event occurs weeks or months before the victims request IC or law enforcement help.

- In a February 2011 study, McAfee attributed an intrusion set they labeled "Night Dragon" to an IP address located in China and indicated the intruders had exfiltrated data from the computer systems of global oil, energy, and petrochemical companies. Starting in November 2009, employees of targeted companies were subjected to social engineering, spear-phishing e-mails, and network exploitation. The goal of the intrusions was to obtain information on sensitive competitive proprietary operations and on financing of oil and gas field bids and operations.
- In January 2010, VeriSign iDefense identified the Chinese Government as the sponsor of intrusions into Google's networks. Google subsequently made accusations that its source code had been taken—a charge that Beijing continues to deny.
- Mandiant reported in 2010 that information was pilfered from the corporate networks of a US Fortune 500 manufacturing company during business negotiations in which that company was looking to acquire a Chinese firm. Mandiant's report indicated that the US manufacturing company lost sensitive data on a weekly basis and that this may have helped the Chinese firm attain a better negotiating and pricing position.
- Participants at an ONCIX conference in November 2010 from a range of US private sector industries reported that client lists, merger and acquisition data, company information on pricing, and financial data were being extracted from company networks—especially those doing business with China.

Russia: Extensive, Sophisticated Operations

Motivated by Russia's high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward US and other Western interests at the expense of Russia, Moscow's highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia's economic development and security.

- For example, the 10 Russian Foreign Intelligence Service (SVR) "illegals" arrested in June 2010 were tasked to collect economic and technology information, highlighting the importance of these issues to Moscow.[c]

[c] An illegal is an officer or employee of an intelligence organization who is dispatched abroad and who has no overt connection with the intelligence organization with which he or she is connected or with the government operating that intelligence organization.

Russian Leaders Link Intelligence Operations and Economic Interests

The SVR "must be able to swiftly and adequately evaluate changes in the international economic situation, understand the consequences for the domestic economy and…more actively protect the economic interests of our companies abroad."
—Vladimir Putin, President, Russian Federation, October 2007

"Intelligence…aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology."
—Mikhail Fradkov, Director, SVR, December 2010

Source: Russian press reports.

US Partners: Leveraging Access

Certain allies and other countries that enjoy broad access to US Government agencies and the private sector conduct economic espionage to acquire sensitive US information and technologies. Some of these states have advanced cyber capabilities.

Outlook

Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will remain at high levels and continue to threaten US economic security. The nature of these attempts will be shaped by the accelerating evolution of cyberspace, policy choices made by the economic and political rivals of the United States, and broad economic and technological developments.

Near Certainties

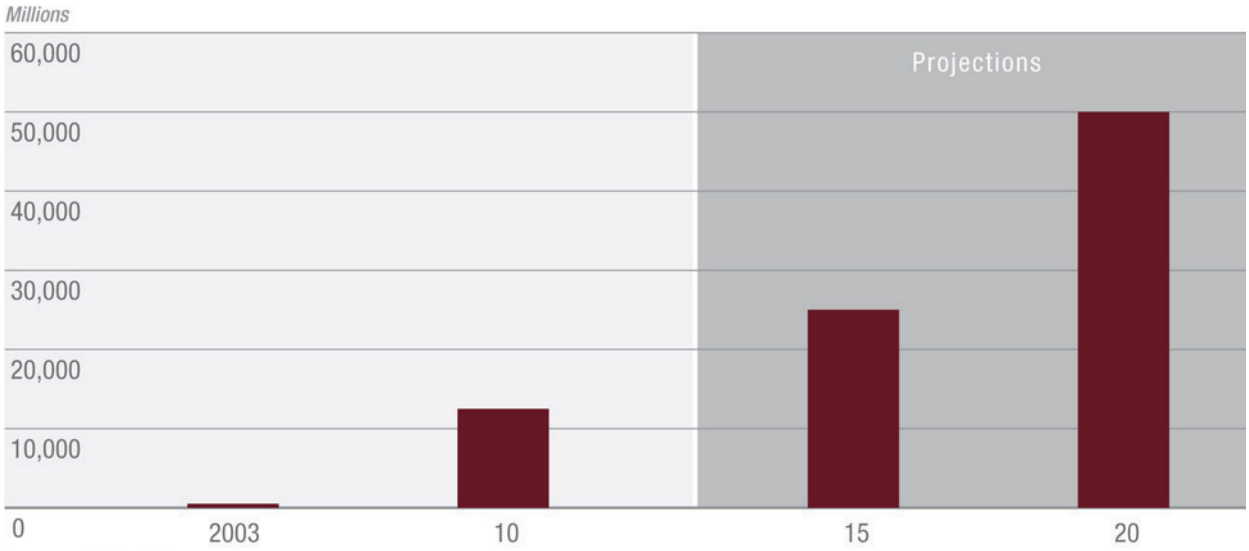
Evolving cyber environment. Over the next three to five years, we expect that four broad factors will accelerate the rate of change in information technology and communications technology in ways that are likely to disrupt security procedures and provide new openings for collection of sensitive US economic and technology information. These were identified in studies conducted by Cisco Systems and discussed at the ONCIX conference in November 2010. At the same time, the growing complexity and density of cyberspace will provide more cover for remote cyber intruders and make it even harder than today to establish attribution for these incidents.

The first factor is a *technological shift*. According to a Cisco Systems study, the number of devices such as smartphones and laptops in operation worldwide that can connect to the Internet and other networks is expected to increase from about 12.5 billion in 2010 to 25 billion in 2015. This will cause a proliferation in the number of operating systems and endpoints that malicious actors such as foreign intelligence services or corrupt insiders can exploit to obtain sensitive information. Meanwhile, the underlying hardware and software of information systems will become more complex.

- Marketing and revenue imperatives will continue to lead IT product vendors to release products with less than exhaustive testing, which will also create opportunities for remote exploitation.

An *economic shift* will change the way that corporations, government agencies, and other organizations share storage, computing, network, and application resources. The move to a "cloud computing" paradigm—which is much cheaper for companies than hosting computer services in-

Projected Growth in Number of IT Devices Connected to Networks and the Internet, 2003-2020



Source: CISCO Systems

house—will mean that employees will be able to work and access data anywhere and at any time, and not just while they are at the office, laboratory, or factory. Although cloud computing offers some security advantages, such as robust backup in the event of a systems disruption, the movement of data among multiple locations will increase the opportunities for theft or manipulation by malicious actors.

The *cultural shift* involves the rise in the US workforce of different expectations regarding work, privacy, and collaboration. Workers will tend to draw few distinctions between their home and work lives, and they will expect free access to any information they want—whether personal or professional—from any location.

- Current technology already enables many US workers to conduct business from remote locations and on-the-go at any time of day. This alteration relies on the ability of workers to connect to one another and their companies through the Internet—increasing their flexibility and corporate productivity but potentially increasing the risk of theft.

Finally, a *geopolitical shift* will continue the globalization of economic activities and knowledge creation. National boundaries will deter economic espionage less than ever as more business is conducted from wherever workers can access the Internet. The globalization of the supply chain for new—and increasingly interconnected—IT products will offer more opportunities for malicious actors to compromise the integrity and security of these devices.

Little change in principal threats. The IC anticipates that China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace. Both will almost certainly continue to deploy significant resources and a wide array of tactics to acquire this information from US sources, motivated by the desire to achieve economic, strategic, and military parity with the United States.

China will continue to be driven by its longstanding policy of "catching up fast and surpassing" Western powers. An emblematic program in this drive is Project 863, which provides funding and guidance for efforts to clandestinely acquire US technology and sensitive economic information. The project

was launched in 1986 to enhance China's economic competitiveness and narrow the science and technology gap between China and the West in areas such as nanotechnology, computers, and biotechnology.

- The growing interrelationships between Chinese and US companies—such as the employment of Chinese-national technical experts at US facilities and the off-shoring of US production and R&D to facilities in China—will offer Chinese Government agencies and businesses increasing opportunities to collect sensitive US economic information.
- Chinese actors will continue conducting CNE against US targets.

Two trends may increase the threat from Russian collection against US economic information and technology over the next several years.

- The many Russian immigrants with advanced technical skills who work for leading US companies may be increasingly targeted for recruitment by the Russian intelligence services.
- Russia's increasing economic integration with the West is likely to lead to a greater number of Russian companies affiliated with the intelligence services—often through their employment of ostensibly retired intelligence officers—doing business in the United States.

Technologies likely to be of greatest interest. Although all aspects of US economic activity and technology are of potential interest to foreign intelligence collectors, we judge that the highest interest may be in the following areas.

Information and communications technology (ICT). ICT is a sector likely to remain one of the highest priorities of foreign collectors. The computerization of manufacturing and the push for connectedness mean that ICT forms the backbone of nearly every other technology used in both civilian and military applications.

- Beijing's Project 863, for example, lists the development of "key technologies for the construction of China's information infrastructure" as the first of four priorities.

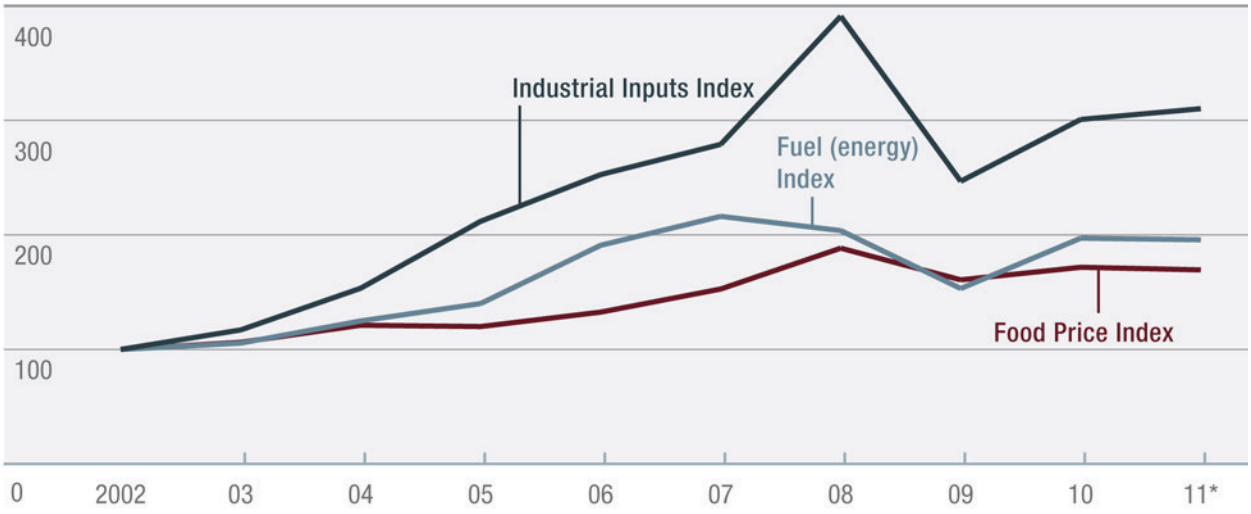
Military technologies. We expect foreign entities will continue efforts to collect information on the full array of US military technologies in use or under development. Two areas are likely to be of particular interest:

- *Marine systems.* China's desire to jump-start development of a blue-water navy—to project power in the Taiwan Strait and defend maritime trade routes—will drive efforts to obtain sensitive US marine systems technologies.
- *Aerospace/aeronautics.* The air supremacy demonstrated by US military operations in recent decades will remain a driver of foreign efforts to collect US aerospace and aeronautics technologies. The greatest interest may be in UAVs because of their recent successful use for both intelligence gathering and kinetic operations in Afghanistan, Iraq, and elsewhere.

Civilian and dual-use technologies. We expect that foreign collection on US civilian and dual-use technologies will follow overall patterns of investment and trade. The following sectors—which are expected to experience surges in investment and are priorities for China—may be targeted more aggressively.

- *Clean technologies.* Energy-generating technologies that produce reduced carbon dioxide and other emissions will be the fastest growing investment sectors in nine of 11 countries recently surveyed by a US consulting company—a survey that included China, France, and India.
- *Advanced materials and manufacturing techniques.* One focus of China's 863 program is achieving mastery of key new materials and advanced manufacturing technologies to boost industrial competitiveness, particularly in the aviation and high-speed rail sectors. Russia and Iran have aggressive programs for developing and collecting on one specific area of advanced materials development: nanotechnology.

Rising Prices Increase Value of Commodity Information to Foreign Collectors (Index, 2002=100)



*2011 values as of April.

Source: International Monetary Fund, World Economic Outlook Database.

- *Healthcare, pharmaceuticals, and related technologies.* Healthcare services and medical devices/equipment will be two of the five fastest growing international investment sectors, according to a US consulting firm. The massive R&D costs for new products in these sectors—up to $1 billion for a single drug—the possibility of earning monopoly profits from a popular new pharmaceutical, and the growing need for medical care by aging populations in China, Russia, and elsewhere are likely to drive interest in collecting valuable US healthcare, pharmaceutical, and related information.
- *Agricultural technology.* Surging prices for food—which have increased by 70 percent since 2002, according to the food price index published by the International Monetary Fund (IMF)—and for other agricultural products may increase the value of and interest in collecting on US technologies related to crop production, such as genetic engineering, improved seeds, and fertilizer.[d]

Business information. As with technologies, we assess that nearly all categories of sensitive US economic information will be targeted by foreign entities, but the following sectors may be of greatest interest:

Energy and other natural resources. Surging prices for energy and industrial commodities—which have increased by 210 percent and 96 percent, respectively, since 2002 according to IMF indices—may make US company information on these resources priority targets for intelligence services and other collectors.[e]

- As noted earlier, cyber intrusions originating in China, but not necessarily attributed to the Chinese Government, since at least 2009 have targeted sensitive operational and project-financing information of US and other international oil, energy, and petrochemical companies, according to reports published by McAfee.

[d]The IMF's Food Price Index is a weighted index that includes the spot prices of cereal grains, vegetable oils and protein meals, meat, seafood, sugar, bananas, and oranges.

[e]The Fuel (energy) index published by the IMF is a weighted index that includes the spot prices of crude oil, natural gas, and coal. The Industrial Inputs Index is a weighted index that includes the spot price of agricultural raw materials (timber, fibers, rubber and hides) and non-precious metals (such as copper, aluminum, and iron ore).

Business deals. Some foreign companies—at times helped by their home countries' intelligence services—will collect sensitive information from US economic actors that are negotiating contracts with or competing against them.

Macroeconomic information. In the wake of the global financial crisis of 2008-2009 and related volatility in the values of currencies and commodities, sensitive macroeconomic information held by the US private sector and government agencies is likely to remain a prime collection target for both intelligence services and foreign corporations. Chinese and Russian intelligence collectors may pursue, for example, non-public data on topics such as interest rate policy to support their policymakers' efforts to advance the role of their currencies and displace the dollar in international trade and finance. Such information also could help boost the performance of sovereign wealth funds controlled by governments like China's, whose China Investment Corporation managed more than $300 billion in investments as of late 2010.[f]

Possible Game Changers

Any of a range of less-likely developments over the next several years could increase the threat from economic espionage against US interests.

Emergence of new state threats. The relative threat to sensitive US economic information and technologies from different countries is likely to evolve as a function of international economic and political developments.

One or more fast-growing regional powers may judge that changes in its economic and political interests merit the risk of an aggressive program of espionage against US technologies and sensitive economic information.

Growing role of non-state and non-corporate actors. The migration of most business and technology development activities to cyberspace is making it easier for actors without the resources of a nation-state or a large corporation to become players in economic espionage. Such new actors may act as surrogates or contractors for intelligence services or major companies, or they could conduct espionage against sensitive US economic information and technology in pursuit of their own objectives.

Hackers for hire. Some intelligence services with less-developed cyber programs already use relationships with nominally independent hackers to augment their capabilities to target political and military information or to carry out operations against regime enemies. For example, the Iranian Cyber Army, a hacker group with links to the Iranian Government, has used social engineering techniques to obtain control over Internet domains and disrupt the political opposition, according to research conducted under an ONCIX contract.

No evidence of involvement by independent hackers in economic espionage has been found in intelligence or academic reporting to date, in large part due to the absence of a profitable market for the resale of stolen information. This "cyber underground" could, however, become a fruitful recruiting ground for the tools and talents needed to support economic espionage. Following the model used by some intelligence services in exploiting the cyber environment for political or military espionage, a foreign government or corporation could build relationships with hackers for the development of customized malware or remote access exploits for the exfiltration of sensitive US economic or technology information.

Hacktivists. Political or social activists also may use the tools of economic espionage against US companies, agencies, or other entities. The self-styled whistleblowing group WikiLeaks has already published computer files provided by corporate insiders indicating allegedly illegal or unethical behavior at a Swiss bank, a Netherlands-based commodities company, and an international pharmaceutical trade association. LulzSec—another hacktivist group—has exfiltrated data from several businesses that it posted for public viewing on its website.

[f] A sovereign wealth fund is a government investment fund, funded by foreign currency reserves but managed separately from official currency reserves. In other words, it is a pool of money that a government invests for profit.

Corporate trade secrets or information about critical US technology may be at similar risk of disclosure to activist groups by disgruntled insiders.

- Antipoverty activists, for instance, could seek to publish the details of a new medicine under development by a US pharmaceutical company, with the goal of ending the firm's "monopoly" profits and making the product more widely available.
- Antiwar groups could disclose information about a new weapons system in the hope of dissuading the United States from deploying it.

Annex A

Intelligence Community and Private Sector Measures to Counter Economic Espionage and Manage Collection in Cyberspace

The IC is working closely with all segments of the public and private sectors to try to counter espionage activities that target our sensitive economic data and technology. We cannot expect to stop entirely or prevent hostile activity to collect US public and private sector information, but we can work to minimize the activity and mitigate its effects.

Intelligence Community Responses

The IC and especially counterintelligence (CI) officers have already taken a number of steps to improve collaboration, collection, and analysis across the CI, economics, and cyber disciplines.

Improved collaboration. Over the past few years, the IC has established multiple organizations and working groups to better understand the cyber espionage threat. These have contributed to a better understanding of the use of cyber in economic espionage.

- The National Cyber Counterintelligence Working Group established in 2011 is composed of 16 IC and other federal agencies and is creating a coordinated response to the cyber intelligence threat.
- The FBI is leading the National Cyber Investigative Joint Task Force, which brings together multiple agencies to collaborate on intrusions into US systems.

CI officers are considering an expansion of collaboration to include enhanced information sharing with Department of Justice attorneys. CI officers could introduce questions for attorneys to pose to offenders during the investigation process. They might also look at ways to tie plea bargains and sentencing decisions to suspects' willingness to cooperate with the CI Community during damage assessments.

Improved analysis and collection. The IC has made great strides over the past few years in understanding the cyber espionage threat to US Government systems, but our knowledge of cyber-enabled economic espionage threats to the US private sector remains limited.

Defense Model Shows Limits to Mandatory Reporting Requirements

DoD's partnership with cleared defense contractors (CDCs) highlights difficulties in establishing an effective framework to improve the IC's understanding of foreign cyber threats and promote threat awareness in industry. The defense industrial base conducts $400 billion in business with the Pentagon each year and maintains a growing repository of government information and intellectual property on unclassified networks. CDCs are required to file reports of suspicious contacts indicative of foreign threats—including cyber—to their personnel, information, and technologies.

- *Despite stringent reporting requirements for CDCs, DSS reports that only 10 percent of CDCs actually provide any sort of reporting in a given year.*
- *Another shortcoming of the defense model is that contractors do not always report theft of intellectual property unless it relates specifically to Pentagon contracts, according to outreach discussions with corporate officers.*
- *Corporate security officers also have noted that US Government reporting procedures are often cumbersome and redundant, with military services and agencies such as DSS and the FBI often seeking the same information but in different formats.*

Operations. CI professionals are adapting how they detect, deter, and disrupt collection activity in cyberspace because of the challenges in detecting the traditional indicators of collection activity—spotting, assessing, and recruiting.

It is imperative that we improve our ability to attribute technical and human activity in the cyber environment so that we can improve our understanding of the threat and our ability to generate a greater number of offensive CI responses.

Training and awareness. Expanding our national education and awareness campaign aimed at individuals and corporations is an essential defensive strategy for countering threats from cyber-enabled economic collection and espionage. We are building on current outreach initiatives that the FBI and ONCIX have already initiated.

- IC outreach to all US Government agencies, state and local governments, academia, nongovernmental organizations, industry associations, and companies is critical for promoting threat awareness, as well as for a better understanding of nongovernmental perspectives. Partners outside the IC are becoming aware of the wide range of potentially sensitive information in their possession and the extent of foreign efforts to acquire it.
- Outreach efforts include awareness and mitigation strategies for insider threat issues. The unique access of insiders to information technology systems and organizational processes makes this the most dangerous approach to cyber economic collection and espionage, as insiders can act alone to guide CNE or to download sensitive data to portable media.

ONCIX already engages in dialogue with ASIS International—an industry association for security professionals—and the Department of State's Overseas Security Advisory Council on the challenges facing both the public and private sectors with regard to cyber-enabled economic collection and espionage.

Finally, IC outreach efforts to the private sector on economic espionage need to fully engage corporate and other partners in order to be credible. We can facilitate partnerships to share best practices, threat updates and analysis, and data on intrusions. One company security officer has suggested that the IC must speak to industry in language geared to the private sector's needs and experience and emphasize, for example, that the protection of trade secrets is critical to corporate profitability and growth.

As a follow-up to the public/private sector Workshop on Cyber-Enabled Economic Espionage held in 2010, ONCIX should consider sponsoring another conference with Department of Justice and private sector stakeholders on lessons learned regarding successful convictions under Section 1831 of the Economic Espionage Act.

Corporate Responses

The private sector already has a fiduciary duty to account for corporate risk and the bottom-line effects of data breaches, economic espionage, and loss or degradation of services. A key responsibility of chief executive officers and boards of directors is to ensure that the protection of trade secrets and computer networks is an integral part of all corporate decisions and processes and that all managers—not just security and information systems officials—have a stake in the outcome.[a] Viewing network security and data protection as a business matter that has a significant impact on profitability will lead to more effective risk management and ensure that adequate resources are allocated to address cyber threats to companies.

- Only 5 percent of corporate chief financial officers are involved in network security matters, and just 13 percent of companies have a cross-functional cyber risk team that bridges the technical, financial, and other elements of a company, according to a 2010 study.

Judicial Mandate for Boards of Directors To Secure Corporate Information

Delaware's Court of Chancery ruled in the 1996 Caremark *case that a director's good faith duty includes a duty to attempt to ensure that a corporate*

[a]Legal and human resources officers are two sets of key stakeholders given the role that corporate insiders have historically played in contributing to economic espionage and the theft of trade secrets.

information and reporting system exists and that failure to do so may render a director liable for losses caused by the illegal conduct of employees. The Delaware Supreme Court clarified this language in the 2006 Stone v. Ritter *case—deciding that directors may be liable for the damages resulting from legal violations committed by the employees of a corporation, if directors fail to implement a reporting system or controls or fail to monitor such systems.*

Companies that successfully manage the economic espionage threat realize and convey to their employees that threats to corporate data extend beyond company firewalls to include other locations where company data is moved or stored. These include cloud sites, home computers, laptops, portable electronic devices, portable data assistants, and social networking sites.

- A survey of 200 information technology and security professionals in February 2011 revealed that 65 percent do not know what files and data leave their enterprise.
- According to a March 2011 press report, 57 percent of employees save work files to external devices on a weekly basis.
- E-mail systems are often less protected than databases yet contain vast quantities of stored data. E-mail remains one of the quickest and easiest ways for individuals to collaborate—and for intruders to enter a company's network and steal data.

Cyber threats to company information are compounded when employees access data through portable devices or network connections while traveling overseas. Many FIS co-opt hotel staffs to allow access to portable devices left unattended in rooms. It is also much easier for FIS to monitor and exploit network connections within their own borders.

- Foreign collectors engage in virtual methods to collect sensitive corporate data and take advantage of victims' reluctance to report digital penetrations and low awareness of foreign targeting, according to legal academic research.

Corporate security officers have told ONCIX that US Government reporting procedures on economic espionage and cyber intrusions are often cumbersome and redundant. Agencies such as DSS and the FBI often seek the same information but in different formats.

Best Practices in Data Protection Strategies and Due Diligence for Corporations

Information Strategy
• Develop a "transparency strategy" that determines how closed or open the company needs to be based on the services provided.
Insider Threat Programs and Awareness
• Institute security training and awareness campaigns; convey threats to company information accessed through portable devices and when traveling abroad.
• Establish an insider threat program that consists of information technology-enabled threat detection, foreign travel and contact notifications, personnel security and evaluation, insider threat awareness and training, and reporting and analysis.
• Conduct background checks that vet users before providing them company information.
• Implement non-disclosure agreements with employees and business partners.
• Establish employee exit procedures; most employees who steal intellectual property commit the theft within one month of resignation.
Effective Data Management
• Get a handle on company data—not just in databases but also in e-mail messages, on individual computers, and as data objects in web portals; categorize and classify the data, and choose the most appropriate set of controls and markings for each class of data; identify which data should be kept and for how long. Understand that it is impossible to protect everything.
• Establish compartmentalized access programs to protect unique trade secrets and proprietary information; centralize intellectual property data—which will make for better security and facilitate information sharing.
• Restrict distribution of sensitive data; establish a shared data infrastructure to reduce the quantity of data held by the organization and discourage unnecessary printing and reproduction.
Network Security, Auditing, and Monitoring
• Conduct real-time monitoring/auditing of the networks; maintain thorough records of who is accessing servers, and modifying, copying, deleting, or downloading files.
• Install software tools—content management, data loss prevention, network forensics—on individual computer workstations to protect files.

- Encrypt data on servers and password-protect company information.
- Incorporate multi-factor authentication measures—biometrics, PINs, and passwords combined with knowledge-based questions—to help verify users of information and computer systems.
- Create a formal corporate policy for mobility—develop measures for centrally controlling and monitoring which devices can be attached to corporate networks and systems and what data can be downloaded, uploaded, and stored on them.
- Formalize a social media policy for the company and implement strategies for minimizing data loss from on-line social networking.

Contingency Planning

- Establish a continuity of operations plan—back up data and systems; create disaster recovery plans; and plan for data breach contingencies.
- Conduct regular penetration testing of company infrastructure as well as of third-party shared service provider systems.
- Establish document creation, retention, and destruction policies.

Resources for Help

- Contact ONCIX or the FBI for assistance in developing effective data protection strategies. If a data breach is suspected, contact the FBI or other law enforcement/organizations for help in identifying and neutralizing the threat.

Annex B

West and East Accuse China and Russia of Economic Espionage

Other advanced industrial countries principally blame China and Russia for economic espionage that results in large but uncertain monetary costs and job losses. They perceive that China and Russia continue to use traditional human and technical collection methods—particularly against small- and medium-sized businesses—to gather economic information and technologies that save them research and development (R&D) resources and provide entrepreneurial and marketing advantage for their corporate sectors.

- Germany's Federal Office for the Protection of the Constitution (BfV) estimates that German companies lose $28 billion-$71 billion and 30,000-70,000 jobs per year from foreign economic espionage. Approximately 70 percent of all cases involve insiders.
- South Korea says that the costs from foreign economic espionage in 2008 were $82 billion, up from $26 billion in 2004. The South Koreans report that 60 percent of victims are small- and medium-sized businesses and that half of all economic espionage comes from China.[a]
- Japan's Ministry of Economy, Trade, and Industry conducted a survey of 625 manufacturing firms in late 2007 and found that more than 35 percent of those responding reported some form of technology loss. More than 60 percent of those leaks involved China.

France's Renault Affair Highlights Tendency to Blame China

Broad French concerns with Chinese economic espionage formed the background of the hasty—and subsequently retracted—accusations by corporate and political leaders in January 2011 that three top executives with the Renault automobile company had taken bribes from China in exchange for divulging technology.

- *An investigation by the French internal security service revealed that the accusations against China lacked substance and may have stemmed from a corrupt corporate security officer's attempts to generate investigative work for a friend's consulting business.*

Past Chinese economic espionage against the French automotive industry—including the parts manufacturer Valeo—probably made the French willing to give credence to any accusation of similar malfeasance against China.

Countries acknowledge the growing use of cyber tools for foreign economic collection and espionage and often note difficulties in understanding losses associated with these cyber collection methods. A 2010 survey of 200 industry executives from the power, oil, gas, and water sectors in 12 Western countries, China, and Russia indicates that 85 percent of respondents experienced network intrusions and that government-sponsored sabotage and espionage was the most often cited cyber threat.

- A 2010 Canadian Government report claimed that 86 percent of large Canadian corporations had been hit and that cyber espionage against the private sector had doubled in two years, according to a press report.
- The German BfV offers no reliable figures on the number of cases and amount of damage caused by cyber-enabled economic espionage, adding that their intelligence services are "groping in the dark." The German Government has noted the use of CNE tools and removable media devices, claiming that $99 million are spent annually for IT security.
- UK officials note that the cost of an information security incident averages between $16,000 and $32,000 for a small company and between

[a]We have no information on the methodologies that the Germans and South Koreans used to calculate their losses.

$1.6 million and $3.2 million for firms with more than 500 employees. The United Kingdom estimates that attacks on computer systems, including industrial espionage and theft of company trade secrets, cost the private sector $34 billion annually, of which more than 40 percent represents theft of intellectual property such as designs, formulas, and company secrets.

- Germany and South Korea judge that China, in particular, increasingly uses cyber tools to steal trade secrets and achieve plausible deniability, according to press reporting.[b]
- Unidentified CNE operators have accessed more than 150 computers at France's Finance Ministry since late 2010, exfiltrating and redirecting documents relating to the French G-20 presidency to Chinese sites, according to a press report.
- The British Security Service's Center for the Protection of National Infrastructure warned hundreds of UK business leaders in 2010 of Chinese economic espionage practices, including giving gifts of cameras and memory sticks equipped with cyber implants at trade fairs and exhibitions. This followed similar notification sent to 300 UK business leaders in 2007 warning them of a coordinated cyber espionage campaign against the British economy.
- German officials also noted that business travelers' laptops are often stolen during trips to China. The Germans in 2009 highlighted an insider case in which a Chinese citizen downloaded highly sensitive product data from the unidentified German company where he worked to 170 CDs.

China's Response to Allegations of Economic Espionage

China usually responds to public allegations of economic espionage with outright denial and counteraccusations. In 2009 China claimed the Australian mining giant Rio Tinto engaged in six years of espionage activities—bribery and information gathering—that resulted in a loss of iron ore imports for the Chinese steel industry as large as $107 billion. This loss was more than twice the total profits generated by the Chinese steel industry over that same six-year period, according to the Chinese Government.

Russia also is seen as an important actor in cyber-enabled economic collection and espionage against other countries, albeit a distant second to China. Germany's BfV notes that Russia uses CNE and e-mail interception to save billions of dollars on R&D in the energy, information technology, telecommunications, aerospace, and security sectors.

- The Director-General of the British Security Service publicly stated that Russia, as well as China, is targeting the UK's financial system.
- A Russian automotive company bribed executives at South Korea's GM-Daewoo Auto and Technology to pass thousands of computer files on car engine and component designs in 2009, according to a press report.
- A German insider was convicted of economic espionage in 2008 for passing helicopter technology to the Russian SVR in exchange for $10,000. The insider communicated with his Russian handler through anonymous e-mail addresses.

Countries Suspect Each Other of Committing Economic Espionage

Allies often suspect each other of economic espionage—underlining how countries can be partners in traditional security matters yet competitors in business and trade. Foreign corporate leaders may make accusations that are not publicly endorsed by their governments.

- *According to a 2010 press report, the Germans view France and the United States as the primary perpetrators of economic espionage "among friends."*
- *France's Central Directorate for Domestic Intelligence has called China and the United States the leading "hackers" of French businesses, according to a 2011 press report.*

[b] We lack insight on the processes that the Germans and South Koreans used to attribute cyber activities to China.

Some countries exercise various legislative, intelligence, and diplomatic options to respond to the threat of cyber-enabled economic collection and espionage.

- France and South Korea have proposed new legislation or changes to existing laws to help mitigate the effects of economic espionage. France also is considering a public economic intelligence policy and a classification system for business information.
- France, the United Kingdom, and Australia have issued strategies and revamped bureaucracies to better align resources against cyber and economic espionage threats. France created a 12-person Economic Intelligence Office in 2009 to coordinate French corporate intelligence efforts. The United Kingdom established an Office of Cyber Security to coordinate Whitehall policy under a senior official and a Cyber Security Operations Centre within the Government Communications Headquarters (GCHQ) SIGINT unit. Australia created a cyber espionage branch within its Security Intelligence Organization in 2010.
- The United Kingdom is mobilizing its intelligence services to gather intelligence on potential threats and for operations against economic collection and espionage in cyberspace, according to press reports.

German Espionage Legislation Has Limited Results

Germany's Federal Prosecutor General initiated 31 preliminary proceedings on espionage in 2007, resulting in just one arrest and one conviction. German authorities note that espionage cases are often hindered by diplomatic immunity protections and by attribution issues from operating abroad through cyberspace.

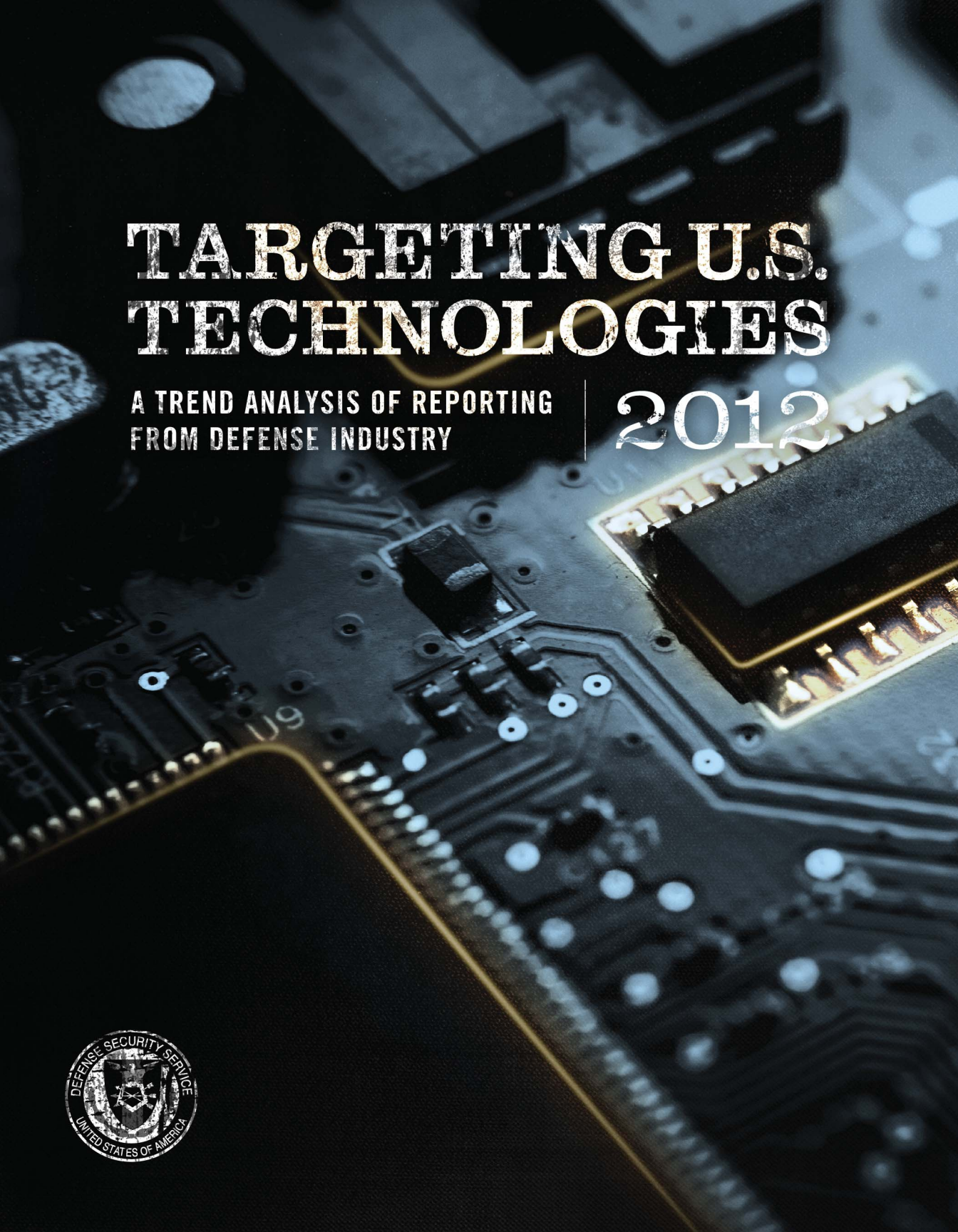
Nearly all countries realize that public and private partnerships are crucial to managing the effects of cyber-enabled economic collection and espionage. The United Kingdom notes that 80 percent of its critical national infrastructure is owned and operated by the private sector. German authorities would like more corporate feedback and say that most enterprises either do not know when they are victims of cyber espionage or do not want to publicly admit their weaknesses. Most countries engage in some form of corporate outreach.

- The French intelligence services offer regular threat briefings to private companies, according to press reports.
- German authorities regularly exchange information with corporate security officers through a private/public working group that includes Daimler AG, Volkswagen, Porsche, Bayer, the German post office, and the railroad industry.

Corporate Leaders Speak Out on Chinese Espionage

Some foreign corporate executives have singled out Chinese espionage as a threat to their companies.

- *British entrepreneur James Dyson—inventor of the bagless vacuum cleaner—warned in 2011 that Chinese students were stealing technological and scientific secrets from UK universities, according to a press report. He noted that Chinese students were also planting software bugs that would relay information to China even after their departure from the universities.*
- *The CEO of an Australian mining firm said that worries over Chinese and other corporate espionage drove him to adopt a more transparent quarterly pricing mechanism for commodities such as iron ore. He claimed that selling products at market-clearing prices visible to all would minimize the impact of differential information that one party may hold, according to a press article.*



TARGETING U.S. TECHNOLOGIES

A TREND ANALYSIS OF REPORTING FROM DEFENSE INDUSTRY

2012

DEFENSE SECURITY SERVICE
UNITED STATES OF AMERICA

DSS MISSION

DSS supports national security and the warfighter, secures the nation's technological base, and oversees the protection of sensitive and classified information and technology in the hands of industry.

We accomplish this mission by: clearing industrial facilities, personnel, and associated information systems; collecting, analyzing, and providing threat information to industry and government partners; managing foreign ownership control and influence in cleared industry; providing advice and oversight to industry; delivering security education and training; and, providing information technology services that support the industrial security mission of the Department of Defense and its partner agencies.

THIS PRODUCT WAS COORDINATED WITH: ACIC, AFOSI, DIA, & NGA

Produced by the Defense Security Service
Counterintelligence Directorate
www.DSS.mil

TARGETING U.S. TECHNOLOGIES

A TREND ANALYSIS OF REPORTING FROM DEFENSE INDUSTRY | 2012

TABLE OF CONTENTS

FIGURES

IN THE INTERESTS OF READABILITY AND COMPREHENSION, THE EDITORS HAVE DEFERRED THE CONVENTIONAL STYLISTIC USE OF REPEATED ACRONYMS IN FAVOR OF A FULL EXPOSITION OF TERMS AS THEY ARE FIRST USED WITHIN EACH SECTION.

PREFACE

The stakes are high in the battle against foreign collection efforts and espionage that target U.S. technology, intellectual property, trade secrets, and proprietary information. Our national security relies on our collective success at thwarting these persistent attacks. Every time our adversaries gain access to sensitive or classified information and technology, it jeopardizes the lives of our warfighters, since these adversaries can exploit the information and technology to develop more lethal weapons or countermeasures to our systems. Our national security is also at risk in the potential loss of our technological edge, which is closely tied to the economic success of the cleared contractor community and the well-being of our economy.

Preventing such losses takes a team effort. The Defense Security Service (DSS) builds on the information contained in reports from industry to develop analytical assessments that articulate the threat to U.S. information and technology resident in cleared industry. This annual publication, *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry*, presents DSS' analysis of those industry reports. Like any analysis, this one is only as good as the information that goes into it. Timely and accurate initial reports of illicit collection attempts are the foundation upon which this process rests, and it is cleared contractor employees who originate those suspicious contact reports.

When this process works well, our national security, warfighters, cleared industry partners, and local communities all benefit. The information contained in this report helps employees, companies, and intelligence and law enforcement professionals better understand the continuing yet changing nature of the threats we face. Increased awareness of the U.S. technologies being targeted by foreign entities and the methods of operation they use in their efforts to acquire those technologies can only make us better at identifying and thwarting illicit collection attempts. In fiscal year 2011, our combined efforts produced 485 operations or investigations based on information that industry provided. Over three-quarters of these are still undergoing significant action, with many foreign collectors already identified, isolated, diverted, or otherwise thwarted.

But these combined efforts face a threat that is growing, persistent, pervasive, and insidious. Cleared industry, DSS, and the intelligence and law enforcement communities continue their efforts to further expand, develop, and refine their methods of defending our national security. Yet the response by foreign collectors who seek to illicitly acquire U.S. information and technology despite those efforts also continues to undergo expansion, development, and refinement.

During fiscal year 2011, the persistent, pervasive, and insidious nature of that threat became particularly noteworthy, and the pattern became even more firmly established. Foreign collectors seek to elude the protective efforts of industry, DSS, the Intelligence Community, and law enforcement by concealing their activities behind various covers, such as third countries, front companies, and cyber identities. This report will present various examples of such activities.

Increasingly, the result of all this foreign collection activity is like malignant plants with multiple interlocking roots and branches. These noxious weeds root in unexpected places, then send out shoots and tendrils that encroach through any crack or gap into the nurseries and gardens of our industrial base. We may pull out some parts of a plant by the roots and lop off the leaves of others, but the pervasive, penetrating weeds remain.

It is only by the continued vigilance and focused and unstinting effort of those of you in cleared industry—by "tending your garden" assiduously and reporting incursions of "weeds" promptly and fully—that the rest of the nation's defenders can help protect its security.

Stanley L. Sims

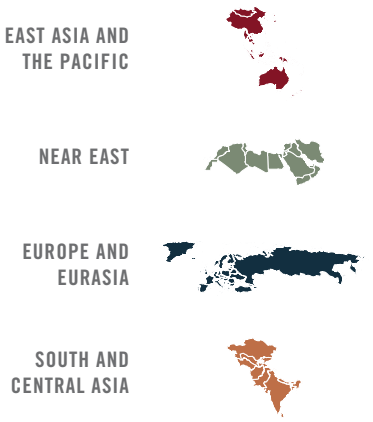
DIRECTOR
DEFENSE SECURITY SERVICE

EXECUTIVE SUMMARY

In one way, the data concerning industry reports of foreign attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base remained very consistent between fiscal year 2010 (FY10) and FY11. The East Asia and the Pacific region accounted for 43 percent of the total in both years; the Near East accounted for 18 percent in both years; Europe and Eurasia dropped only slightly, from 15 percent to 13 percent; and South and Central Asia was reasonably stable, rising from nine percent to twelve percent.

REGIONAL TRENDS

FIGURE 1



But this seeming stability in the data does not reflect the overall phenomena in the past year. The total number of reports received from industry increased over 75 percent from FY10. In the past year, reports from the East Asia and the Pacific and Near East regions increased by around 75 percent, from Europe and Eurasia by over 60 percent, and from South and Central Asia by a steep 129 percent. All other regions increased in number of reports as well. Thus, the only stability in the data is the relentless upward trend.

Considerable diversity exists within each region. Countries vary in size, resources, economic development, political system, degree of militarization, and foreign policy orientation and goals. And the situation is not static; change continues in these variables as well. Some countries are on the way "up," others "down," however defined. Some are satisfied with their place and role in the world; others aspire to change them, and work aggressively to do so. Any of these factors can lead to attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base.

Despite the diversity between regions and countries discussed above, collectors continue to expand the degree of interaction between them in their attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. Whether working with each other, working through each other, buying from each other, or attempting to throw suspicion on each other, these convoluted pathways make it more difficult to ascribe collection attempts to a particular country, region, or collector affiliation.

KEY FINDINGS

The order of the regions linked to the most prolific collectors of U.S. information and technology remained unchanged from fiscal year 2010 (FY10); commercial remained the most common collector affiliation; and the top four most targeted technology categories remained the same.

Constancy of the order of the regions represents the most enduring trend. Over the past five years, East Asia and the Pacific and the Near East have remained the first and second most prolific collector regions, responsible for at least 56 percent of all reported collection attempts each year, including 61 percent in FY11. However, industry reports of collection attempts originating from South and Central Asia increased by 129 percent, reflecting aggressive collection efforts.

Commercial entities constituted the most common affiliation in FY11 industry reporting, residing at the top of the ranking in five of the six regions.

Collectors' most frequently applied methods of operation (MO) sought information or technology directly, whether by attempted acquisition of technology or request for information (RFI). Combined, these MOs accounted for 43 percent of reported collection attempts in FY11. A DSS redefinition of attempted acquisition led to different apportionment of cases in FY11 than in previous years, but taken together these two MOs represent direct overt contact with cleared industry in an attempt to receive information or acquire technology—by simply asking for it.

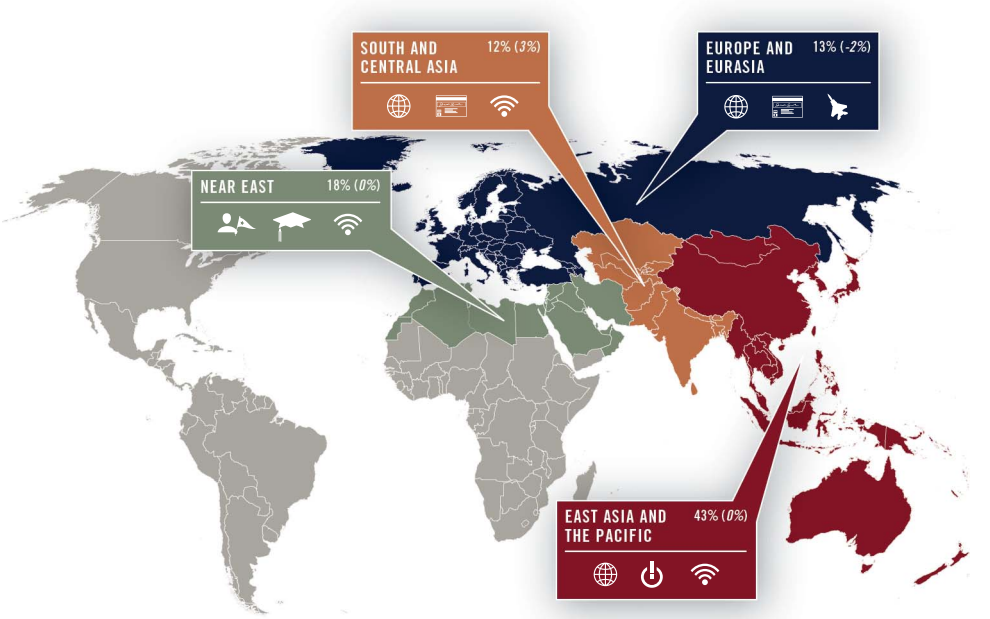
In FY11, suspicious network activity (SNA) was the most prevalent collection MO for entities originating from East Asia and the Pacific; SNA figured no more prominently than fifth in any other region. Due to the nature of SNA, it remains difficult to attribute such collection attempts to an entity or even to a region of origin.

The top four most targeted technology categories in FY11—information systems (IS); lasers, optics, and sensors (LO&S); aeronautics systems; and electronics—remained unchanged. Armaments and energetic materials replaced marine systems as the fifth most targeted category of the Militarily Critical Technologies List (MCTL). But there was a broadening of reported interest in technology to space systems, processing and manufacturing, and directed energy systems in FY11.

Foreign governments are beginning to move into space for commercial telecommunications, increased command and control, and intelligence, surveillance, and reconnaissance (ISR), and the demand for radiation-hardened (rad-hard) microelectronics is likely to dramatically rise over the coming years. Foreign entities' interest in these technologies rose over the past year, and collectors will likely increase their targeting of cleared contractors' design, manufacturing, and packaging of rad-hard microelectronics.

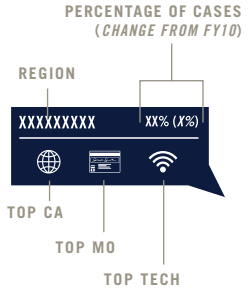
FISCAL YEAR 2011 COLLECTION TRENDS

FIGURE 2



COLLECTOR AFFILIATIONS*

- COMMERCIAL
- INDIVIDUAL
- GOVERNMENT AFFILIATED
- GOVERNMENT
- UNKNOWN



METHODS OF OPERATION*

- ATTEMPTED ACQUISITION OF TECHNOLOGY
- REQUESTS FOR INFORMATION
- SUSPICIOUS NETWORK ACTIVITY
- ACADEMIC SOLICITATION
- SOLICITATION OR MARKETING
- OFFICIAL FOREIGN VISITS AND TARGETING
- CONFERENCES, CONVENTIONS, AND TRADE SHOWS
- EXPLOITATION OF RELATIONSHIPS
- SEEKING EMPLOYMENT
- CRIMINAL ACTIVITIES
- TARGETING U.S. TRAVELERS OVERSEAS

TOP TARGETED TECHNOLOGIES*

- INFORMATION SYSTEMS
- LASERS, OPTICS, AND SENSORS
- AERONAUTICS SYSTEMS
- ELECTRONICS
- ARMAMENTS AND ENERGETIC MATERIALS
- SPACE SYSTEMS
- MARINE SYSTEMS
- POSITIONING, NAVIGATION, AND TIME
- MATERIALS AND PROCESSES
- GROUND SYSTEMS
- INFORMATION SECURITY
- PROCESSING AND MANUFACTURING

*Categories of affiliations, methods, and technologies listed above appear in order of prevalence in overall FY11 reporting statistics.

BACKGROUND

THE ROLE OF THE DEFENSE SECURITY SERVICE

DSS supports national security and the warfighter, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information and technology in the hands of industry. The DSS Counterintelligence (CI) Directorate seeks to identify unlawful penetrators of cleared U.S. industry and stop foreign collection attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. DSS CI articulates the threat for industry and U.S. Government leaders.

THE ROLE OF INDUSTRY

In carrying out its mission, DSS relies on the support of cleared contractor employees and the U.S. intelligence and law enforcement communities. Chapter 1, Section 3 of Department of Defense (DoD) Instruction 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, dated February 28, 2006, requires cleared contractors to remain vigilant and report suspicious contacts. The process that begins with initial industry reporting and continues with ongoing and collective analysis reaches its ultimate stage in successful investigations or operations by federal investigative or intelligence agencies.

In accordance with the reporting requirements laid out in the *NISPOM*, DSS receives and analyzes reports from cleared contractors and categorizes them as suspicious, unsubstantiated, or of no value. For each reported collection attempt, DSS data aggregation and analysis methodologies seek to gather as much information as possible. The analysis of this information forms the basis for this report.

Such cleared contractor reporting provides information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversion activities to DSS and the Federal Bureau of Investigation. When indicated, DSS refers cases of CI concern to its partners in the law enforcement and intelligence communities for potential exploitation or neutralization. DSS follows up with remedial actions for industry to decrease the threat in the future. This builds awareness and understanding of the individual and collective threats and actions and informs our defenses.

THE REPORT

DoD Instruction 5200.39, *Critical Program Information (CPI) Protection within the Department of Defense*, dated July 16, 2008, requires DSS to publish a report that details suspicious contacts occurring within the cleared contractor community. The focus of the report is on efforts to compromise or exploit cleared personnel or to obtain illegal or unauthorized access to classified information and technology resident in the U.S. cleared industrial base.

Each year DSS publishes *Targeting U.S. Technologies: A Trend Analysis of Reporting*

from Defense Industry. In this report, the 14th annual *Targeting U.S. Technologies*, DSS provides a snapshot of its findings on foreign collection attempts. It provides a statistical and trend analysis that covers the most prolific foreign collectors targeting the cleared contractor community during fiscal year 2011 (FY11), compares that information to the previous year's report, and places that comparison into a larger context.

DoD Instruction 5200.39 requires DSS to provide its reports to the DoD CI community, national entities, and the cleared contractor community. This unclassified version of the report constitutes part of DSS' ongoing effort to assist in better protecting the U.S. cleared industrial base by raising general threat awareness, encouraging the reporting of incidents as they occur, identifying specific technologies at risk, and applying appropriate countermeasures. DSS intends the report to be a ready reference tool for security professionals in their efforts to detect, deter, mitigate, or neutralize the effects of foreign targeting. DSS released a classified version of this report earlier this year.

SCOPE/METHODOLOGY

DSS bases this report primarily on SCRs collected from the cleared contractor community. It also includes references to all-source Intelligence Community (IC) reporting.

DSS considers all SCRs received from cleared industry. It then applies analytical processes to them, including the DSS foreign intelligence threat assessment methodology. This publication is organized first by targeting region, then by collector affiliation, methodologies employed, and technologies, including the specific technology sectors targeted. It incorporates statistical and trend analyses on each of these areas. Each section also contains a forecast of potential future collection attempts against the cleared contractor community, based on analytical assessments.

COLLECTOR AFFILIATION DEFINITIONS

FIGURE 3

COMMERCIAL
Entities whose span of business includes the defense sector

GOVERNMENT AFFILIATED
Research institutes, laboratories, universities, or contractors funded by, representing, or otherwise operating in cooperation with a foreign government agency, whose shared purposes may include acquiring access to U.S. sensitive, classified, or export-controlled information

GOVERNMENT
Ministries of Defense and branches of the military, as well as foreign military attachés, foreign liaison officers, and the like

INDIVIDUAL
Persons who, for financial gain or ostensibly for academic or research purposes, seek to acquire access to U.S. sensitive, classified, or export-controlled information or technology, or the means of transferring it out of the country

UNKNOWN
Instances in which no attribution of a contact to a specific end user could be directly made

METHOD OF OPERATION DEFINITIONS

FIGURE 4

ACADEMIC SOLICITATION

Via requests for or arrangement of peer or scientific board reviews of academic papers or presentations, or requests to study or consult with faculty members, or applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees

ATTEMPTED ACQUISITION OF TECHNOLOGY

Via direct purchase of firms or the agency of front companies or third countries, these are attempts to acquire protected information in the form of controlled technologies, whether the equipment itself or diagrams, schematics, plans, spec sheets, or the like

CONFERENCES, CONVENTIONS, AND TRADE SHOWS

This refers to suspicious activity at such events—especially those involving dual-use or sensitive technologies that involve protected information—such as taking of photographs, making sketches, or asking of detailed technical questions

CRIMINAL ACTIVITIES

Via theft, these are attempts to acquire protected information with no pretense or plausibility of legitimate acquisition

EXPLOITATION OF RELATIONSHIPS

Via establishing connections such as joint ventures, official agreements, foreign military sales, business arrangements, or cultural commonality, these are attempts to play upon existing legitimate or ostensibly innocuous relationships to gain unauthorized access

OFFICIAL FOREIGN VISITS AND TARGETING

Via visits to cleared contractor facilities that are either pre-arranged by foreign contingents or unannounced, these are attempts to gain access to and collect protected information that goes beyond that permitted and intended for sharing

REQUESTS FOR INFORMATION

Via phone, email, or webcard approaches, these are attempts to collect protected information under the guise of price quote, marketing surveys, or other direct and indirect efforts

SEEKING EMPLOYMENT

Via résumé submissions, applications, and references, these are attempts to introduce persons who, wittingly or unwittingly, will thereby gain access to protected information which could prove useful to agencies of a foreign government

SOLICITATION OR MARKETING

Via sales, representation, or agency offers, or response to tenders for technical or business services, these are attempts by foreign entities to establish a connection with a cleared contractor vulnerable to the extraction of protected information

SUSPICIOUS NETWORK ACTIVITY

Via cyber intrusion, viruses, malware, backdoor attacks, acquisition of user names and passwords, and similar targeting, these are attempts to carry out intrusions into cleared contractor networks and exfiltrate protected information

TARGETING U.S. TRAVELERS OVERSEAS

Via airport searches, hotel room incursions, computer/device accessing, telephone monitoring, personal interchange, and the like, these are attempts to gain access to protected information through the presence of cleared contractor employees traveling abroad as a result of invitations and/or payment to attend seminars, provide training, deliver speeches, and the like

Pending a transition in technology categorization schemes, DSS continues to analyze foreign interest in U.S. defense technology in terms of the 20 sections in the Militarily Critical Technologies List (MCTL). The MCTL is a compendium of the science and technology capabilities under development worldwide that have the potential to significantly enhance or degrade U.S. military capabilities in the future. It provides categories and subcategories for DSS to use in identifying and defining targeted technologies.

This publication also makes reference to the Department of Commerce's Entity List. This list provides public notice that certain exports, re-exports, and transfers (in-country) to entities included on the Entity List require a license from the Bureau of Industry and Security. An End-User Review Committee (ERC) annually examines and makes changes to the list, as required. The ERC includes representatives from the Departments of Commerce, Defense, Energy, State, and, when appropriate, Treasury.

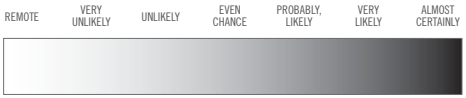
For FY11, the categories DSS used to identify methods of operation remained unchanged from the previous year. However, improved industry reporting and a refinement in DSS methodology resulted in more cases falling into the attempted acquisition of technology category that might previously have been labeled requests for information.

ESTIMATIVE LANGUAGE AND ANALYTIC CONFIDENCE

DSS uses the IC estimative language standard. The phrases used, such as *we judge*, *we assess*, or *we estimate*, and terms such as *likely* or *indicate* represent the agency's effort to convey a particular analytical assessment or judgment.

Because DSS bases these assessments on incomplete and at times fragmentary information, they do not constitute facts nor provide proof, nor do they represent empirically based certainty or knowledge. Some analytical judgments are based directly on collected information, others rest on previous judgments, and both types serve as building blocks. In either variety of judgment, the agency may not have evidence showing something to be a fact or that definitively links two items or issues.

Intelligence judgments pertaining to likelihood are intended to reflect the approximate level of probability of a development, event, or trend. Assigning precise numerical ratings to such judgments would imply more rigor than the agency intends. The chart below provides a depiction of the relationship of terms to each other.



The report uses *probably* and *likely* to indicate that there is a greater than even chance of an event happening. However, even when the authors use terms such as *remote* and *unlikely*, they do not intend to imply that an event will not happen. The report uses phrases such as *we cannot dismiss*, *we cannot rule out*, and *we cannot discount* to reflect that, while some events are unlikely or even remote, their consequences would be such that they warrant mentioning.

DSS uses words such as *may* and *suggest* to reflect situations in which DSS is unable to assess the likelihood of an event, generally because relevant information is sketchy, fragmented, or nonexistent.

In addition to using words within a judgment to convey degrees of likelihood, DSS also assigns analytic confidence levels based on the scope and quality of information supporting DSS judgments:

HIGH CONFIDENCE

- Well-corroborated information from proven sources, minimal assumptions, and/or strong logical inferences
- Generally indicates that DSS based judgments on high-quality information, and/or that the nature of the issue made it possible to render a solid judgment

MODERATE CONFIDENCE

- Partially corroborated information from good sources, several assumptions, and/or a mix of strong and weak inferences
- Generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence

LOW CONFIDENCE

- Uncorroborated information from good or marginal sources, many assumptions, and/or mostly weak inferences
- Generally means that the information's credibility or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that we have significant concerns or problems with the sources

SPECIAL FOCUS AREA:

RADIATION-HARDENED MICROELECTRONICS

OVERVIEW

Ionizing radiation affects microelectronics and electronic systems during high-altitude flights and space operations, in particle accelerators, and in the proximity of fission or fusion reactions. In environments of high ionizing radiation, non radiation-hardened (rad-hard) microelectronics or insufficiently rad-hard microelectronics operationally degrade or fail due to single-event effects (SEEs).

Radiation hardening, by process or design, protects microelectronics and electronic systems from the effects of ionizing radiation. The Defense Security Service (DSS) produced this Special Focus Area assessment to alert cleared industry to the increasing foreign threat to rad-hard microelectronics and facilitate the implementation of mitigation strategies to counter that threat.

RADIATION HARDENING BY PROCESS – This method requires a foundry dedicated to hardened microelectronics. Recipe steps are the proprietary information of the manufacturer or classified by the U.S. Government. Radiation hardening by process can consist of proprietary steps added to a standard process of manufacturing a wafer so as to make it rad-hard. In such a case, there is no distinction between standard wafers and rad-hard wafers during much of the process.

RADIATION HARDENING BY DESIGN – This method relies solely on integrated circuit design and layout techniques to mitigate damage caused by ionizing radiation. Manufacturers design custom circuits for optimal performance in a targeted radiation environment, then fabricate them separately in a high-volume commercial approach. Radiation hardening by design presumes no access or visibility into the manufacturing process to enhance radiation tolerance reliability.

Foreign entities' interest in rad-hard microelectronics has risen over the past year, a trend reflected in industry reporting from fiscal year 2011 (FY11), which saw a 17 percent rise in reported targeting of rad-hard microelectronics from FY10. When analyzed collectively, these reports show a particularly strong interest in these technologies from regions with active or maturing space programs. Acquisition of a relatively small number of rad-hard microelectronics would likely assist foreign governments in developing their own radiation hardening processes or increase the reliability and effectiveness of their indigenous technologies already in use. Foreign entities focused collection activities on cleared contractors producing rad-hard memory whose resistance to the effects of ionizing radiation make them suitable for supporting manned and unmanned space activities.

Foreign governments are beginning to move to space for commercial telecommunications, increased command and control, and intelligence, surveillance and reconnaissance (ISR). Failure of microelectronics in space is costly. Whether SEEs are non-destructive or destructive, they can result in the total abandonment of a space system versus spending the time and money to fix the problem.

DSS analysis of industry documentation reveals that reported foreign collection attempts directed at cleared contractors that design, manufacture, and package rad-hard microelectronics increased 17 percent from FY10 to FY11. Near East and Europe and Eurasia collectors targeting rad-hard microelectronics, who were frequently noted in reporting in previous years, emerged as the most active collectors, with each region accounting for 26 percent of FY11 reports. Entities connected to East Asia and the Pacific, however, remained the top collectors, as represented by their 40 percent of total industry reporting.

Foreign entities appear to rely on three methods of operation (MOs) when targeting rad-hard designers, manufacturers, and packers: requests for information (RFIs); attempted acquisitions of technology; and academic solicitations. These MOs account for 97 percent of FY11 collection attempts reported by industry.

SINGLE-EVENT EFFECTS

SOFT ERRORS (non-destructive)

- SINGLE-EVENT TRANSIENT – Discharge of collected charges from an ionizing event
- SINGLE-EVENT UPSET – Changes of memory or register bits caused by a single ion interaction on the chip
- SINGLE-EVENT FUNCTIONAL INTERRUPTION – Ionizing events cause temporary loss of device functionality

HARD ERRORS (destructive)

- SINGLE-EVENT LATCHUP – Ionizing events cause circuit lockup and/or catastrophic device failure
- SINGLE-EVENT BURNOUT – Destructive burnout due to high current conditions
- SINGLE-EVENT GATE RUPTURE – Rupture of gate dielectric due to high electrical field conditions
- STUCK BITS – Unalterable change of state in a memory element

The packaging of microelectronics is as important as the design and manufacturing of integrated circuitry. Timothy May of Intel Corporation noted the first packaging-induced soft errors in 1979. In an article entitled "Alpha-Particle-Induced Soft Errors in Dynamic Memories," first published in *IEEE Transactions on Electron Devices*, May analyzed single-event upsets occurring due to uranium and thorium decay in microelectronics packaging.

REGIONS OF ORIGIN

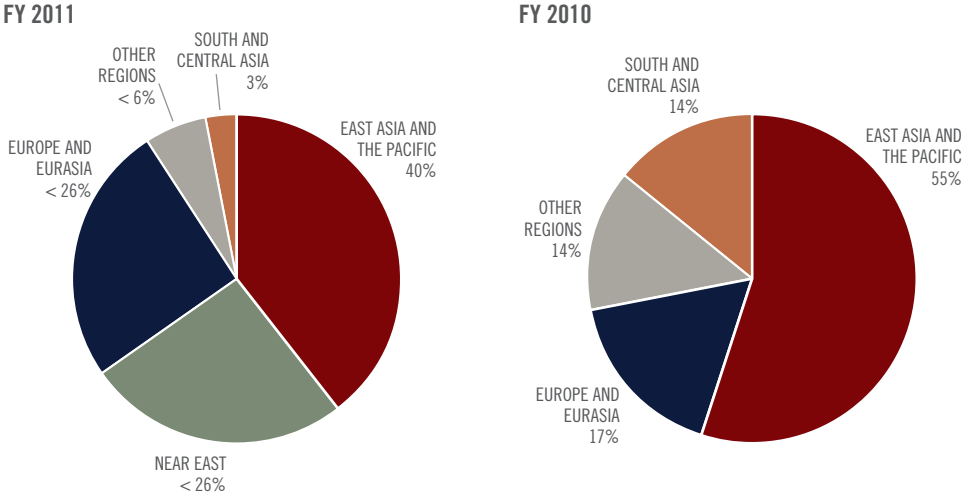
- East Asia and the Pacific
  - Requested specific quantities of rad-hard static random-access memory (SRAM), optical transceivers, and databus controllers
  - Primarily used commercial entities with RFI as MO
- Near East
  - Primarily used student requests to attempt to elicit information from leading experts
- Europe and Eurasia
  - Attempted to acquire specific quantities of rad-hard SRAM and optical transceivers
  - Primarily attempted acquisition by commercial entities

EAST ASIA AND THE PACIFIC

East Asia and the Pacific entities accounted for 40 percent of FY11 industry reporting on the targeting of rad-hard microelectronics. In many requests for rad-hard microelectronics from entities in this region, the requestor solicited the U.S. cleared manufacturer for a specific quantity of the product, implying that there was an immediate need from a customer for the microelectronics.

Twelve East Asia and the Pacific countries have active or planned space programs. Three with the most active space programs are spending $4 billion annually for launching space platforms, controlling satellites, and observing space. Expanding East Asia and the Pacific economies are using space-based technologies to communicate, command, and control across growing land and sea lines of communications.

REGIONS OF ORIGIN
FIGURE 5



However, many of these countries do not possess the technical proficiency to design, manufacture, and rad-hard microelectronics capable of withstanding sustained cosmic radiation. These countries seek Western Hemisphere and Europe and Eurasia rad-hard microelectronic suppliers to enable them to assemble space-worthy systems that will withstand high radiation for a sustained period.

Analyst Comment: Based on reporting from cleared industry, it is likely that East Asia and the Pacific collectors have immediate needs for rad-hard microelectronics for various commercial and military programs. The lack of East Asia and the Pacific technical proficiency to design and manufacture space-worthy rad-hard microelectronics coupled with East Asia and the Pacific commercial entities' specific requests for the technology from cleared industry likely signify that the microelectronics markets in East Asia and the Pacific are unable to meet the strategic goals of included countries. (Confidence Level: Moderate)

NEAR EAST

Near East entities were the second most active FY11 collectors of rad-hard microelectronics information, as reflected in attempts reported by industry. Near East entities are consistently among the most active collectors of U.S. technology overall, but this is the first year in which industry reporting portrayed a particular and deliberate effort to obtain restricted rad-hard information from U.S. universities researching radiation hardening. To do so, Near East entities relied on academic solicitation, in the form of student requests seeking restricted rad-hard information

CASE STUDY

On November 11, 2010, a Colorado-based cleared contractor received a request from an individual representing an East Asia and the Pacific commercial entity for rad-hard SRAM. The individual did not specify the end use or end user of the rad-hard SRAM; however, according to the commercial entity's website, an East Asia and the Pacific military is a customer of the company.

On November 17, 2010, the same Colorado-based cleared contractor reported receiving an almost identical request from another individual representing a separate East Asia and the Pacific commercial entity. In an email, the individual requested to purchase a large number of the company's rad-hard microelectronics for an East Asia and the Pacific customer. The individual did not further identify the intended end use or end user of the requested products. The quantities and specifications of the requested rad-hard microelectronics follow:

- 2000 pieces of 512K rad-hard SRAMs with a standard microcircuit drawing
- 2000 pieces of 256K rad-hard SRAMs with a standard microcircuit drawing

These commercial entities' collection activities demonstrate the aggressive nature of the attempts to acquire U.S. rad-hard microelectronics from cleared contractors.

Analyst Comment: Although a connection between these commercial entities cannot be confirmed, given the similarity of the requests over a relatively short period, it is likely that the end user of the rad-hard SRAM would have been customers within the same East Asia and the Pacific country. East Asia and the Pacific commercial entities and their proxies will likely continue to employ these MOs in attempts to circumvent U.S. export laws covering this restricted technology. (Confidence Level: High)

from cleared contractors and research and employment opportunities at facilities specializing in radiation hardening.

Analyst Comment: Near East governments' association with universities likely provides an avenue for procurement of restricted rad-hard microelectronics research and development under the guise of academic cooperation for the advancement of sciences and technologies. Rad-hard microelectronic information garnered through academic cooperation with U.S. universities would almost certainly advance current Near East space capabilities and provide a foundation for long-term space and military advancements in hardening of microelectronics. (Confidence Level: High)

EUROPE AND EURASIA

Europe and Eurasia entities' targeting of rad-hard microelectronics increased from the previous year, now representing 26 percent of the FY11 reported total. Although collectors connected to Europe and Eurasia are consistently among the top foreign entities attempting to collect U.S. technology, this is the first year that reporting suggested a concerted effort by Europe and Eurasia collectors to acquire rad-hard microelectronics from cleared contractors. In almost every reported incident, Europe and Eurasia commercial entities attempted to acquire specific numbers of rad-hard microelectronics.

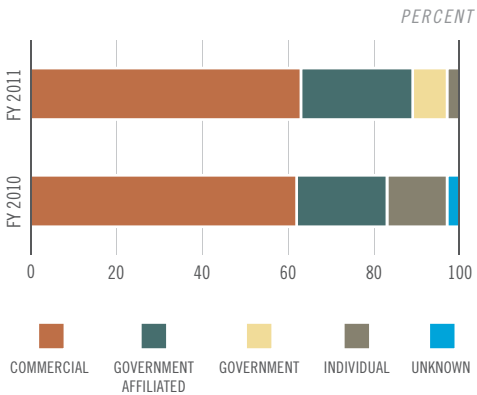
Europe and Eurasia leaders have stated their beliefs that national defensive capabilities are directly related to strong microelectronics design and manufacturing processes. For over ten years, Europe and Eurasia leaders have discussed the need to end reliance on foreign microelectronics. In some countries, over 90 percent of the microelectronics used in defense systems are imported.

Analyst Comment: Although indigenous microelectronics design and manufacturing and radiation hardening research appear to be a priority among Europe and Eurasia strategic technology pursuits, regional producers almost certainly cannot provide U.S.-quality and -quantity rad-hard microelectronics. The attempted acquisition of specific numbers of rad-hard microelectronics probably means there is a specific Europe or Eurasia program requiring certain capabilities to be found only in U.S. cleared contractor-manufactured rad-hard microelectronics.
(Confidence Level: Moderate)

AFFILIATIONS AND METHODS OF OPERATION

Once DSS established the collecting entity's country of origin, it identified its affiliation and the MO used. The following paragraphs detail the top affiliations and MOs identified in FY11 reporting from cleared industry.

COLLECTOR AFFILIATIONS
FIGURE 6



DSS analysis of industry reporting shows that collectors affiliated with East Asia and the Pacific primarily relied on commercial entities to obtain sensitive or classified U.S. information and technology in FY11. They did so using two MOs. The RFI was used most often, employing email to seek price quotes and technical information regarding rad-hard technology. At 45 percent, attempted acquisition of technology via email was the other MO East Asia and the Pacific commercial entities used to attempt

to circumvent U.S. laws restricting the export of rad-hard microelectronics. In emails, when individuals representing commercial entities were notified that the U.S. cleared contractor would need an export determination prior to a transaction, the U.S. manufacturer either did not receive a response or the suspicious entity provided a U.S. address and reiterated the same request.

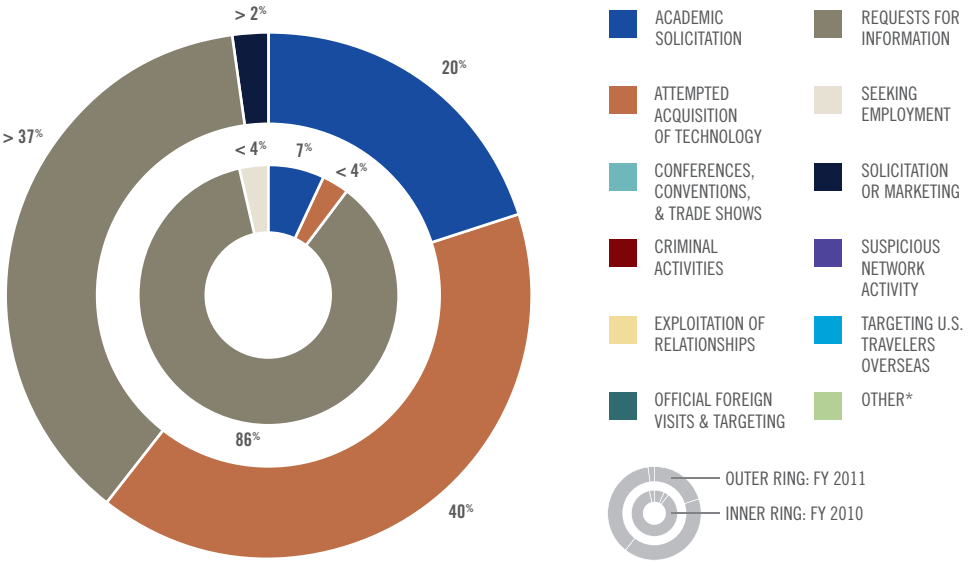
In contrast, Near East entities' efforts, as reflected in industry reporting, relied solely on government-affiliated university students who made academic solicitations to rad-hard research facilities. Radiation reliability experts at a cleared U.S. university received numerous emails and curricula vitae (CVs) from Near East university students expressing interest in obtaining research positions under their supervision. Often the résumé or CV demonstrated a history of research in microelectronics and radiation effects on microelectronics. In one email, the collector cited experience working in a laboratory studying space radiation effects on satellite systems.

Europe and Eurasia entities, like East Asia and the Pacific entities, relied on RFIs and the attempted acquisition of technology through commercial collectors in attempting to acquire sensitive rad-hard technology in FY11. RFIs ranged from requesting data sheets for a U.S. contractor's rad-hard technology to requesting a list of a U.S. company's distributors in a particular foreign country.

TARGETING RAD-HARD SRAM

Reporting from cleared industry pointed to SRAM being the most sought after rad-hard microelectronics technology. SRAM is a type of memory that is faster and more reliable than the more common dynamic random-access memory (DRAM). While DRAM supports access times of about 60 nanoseconds, SRAM can support

METHODS OF OPERATION
FIGURE 7



*Includes potential espionage indicators and cases not otherwise listed

access times as low as 10 nanoseconds. In addition, its cycle time is much shorter than that of DRAM because it does not need to pause between accesses. It is also much more expensive to produce, so SRAM is usually employed only as a memory cache.

The following table shows the number and type of rad-hard SRAMs that entities from East Asia and the Pacific and Europe and Eurasia requested, according to reporting from cleared industry in FY11.

TARGETED STATIC RANDOM ACCESS MEMORY

COUNTRY	TYPE	QUANTITY
EAST ASIA AND THE PACIFIC	128K, 256K, 512K	> 4338
EUROPE AND EURASIA	128K, 512K	> 6640

Analyst Comment: Although previous assessments found that these requests for rad-hard microelectronics were likely intended to fill immediate requirements in commercial and military programs, there is an even chance that the requestor could divert rad-hard microelectronics to commercial or government organizations specializing in reverse-engineering. (Confidence Level: Moderate)

According to IC reporting, multiple foreign companies and government labs conduct failure and vulnerability analysis and reverse-engineering (FAVA-RE) to validate microelectronics design. Although the FAVA-RE process is legal in the United States to discover and analyze circuit designs, it can reveal sensitive information contained in microelectronics and proprietary fabrication processes.[1,2]

Analyst Comment: Success by East Asia and the Pacific and Europe and Eurasia companies in the illegal acquisition of U.S. rad-hard SRAM would probably result in the revelation of sensitive information and proprietary fabrication processes. The likely diversion of these items to university or government labs capable of conducting FAVA-RE analysis would probably spur indigenous development of rad-hard microelectronics. This would likely decrease the funding that entities in these regions would have to dedicate to researching radiation hardening techniques and increase world-wide competition to supply rad-hard microelectronics, potentially impacting U.S. companies' sales. (Confidence Level: Moderate)

OUTLOOK

Reporting from industry confirms that U.S. rad-hard microelectronics are of significant interest to collecting entities in several regions. They are likely to use a variety of MOs by commercial, government-affiliated, government, and individual entities to attempt to collect rad-hard microelectronics information or technology. **(Confidence Level: High)**

DSS assesses that agents from East Asia and the Pacific, the Near East, and Europe and Eurasia in particular will likely continue their efforts to collect U.S. rad-hard microelectronics in the immediate future, largely reliant on the RFI and attempted acquisition of technology MOs. **(Confidence Level: High)**

With more countries moving toward conducting space activities and operations, DSS assesses that it is likely the demand for rad-hard microelectronics will dramatically rise over the coming years, especially as once-torpid economies grow and outdated militaries modernize and move terrestrial communication and ISR activities into space. As U.S. companies continue to increase rad-hard microelectronics' speed and decrease their susceptibility to ionizing radiation, foreign entities will likely increase their targeting of cleared contractors' design, manufacturing, and packaging of rad-hard microelectronics. **(Confidence Level: Moderate)**

CASE STUDY: A DATE FOR THE PROM

On September 30, 2011, two Chinese nationals were sentenced to 24 months in prison for participating in a conspiracy to violate the Arms Export Control Act. Hong Wei Xian, also known as Harry Zan, and co-conspirator Li Li, also known as Lea Li, attempted to acquire and smuggle rad-hard microchips out of the United States for an agency controlled by the Chinese government.

Xian and Li, representing Beijing Starcreates Space Science and Technology Development Company Limited, engaged in the importing and selling of programmable read-only memory (PROM) to China Aerospace Science and Technology Corporation. Between April 2009 and September 2010, they contacted a company in the Eastern District of Virginia requesting to purchase thousands of rad-hard PROMs. China Aerospace is controlled by the government of China and researches, designs, develops, and produces strategic and tactical missiles and exo-atmospheric launch vehicles.

Xian and Li sought PROMs specifically designed to withstand sustained radiation bombardment in space. The conspirators knew the PROMs were export-controlled, but they did not seek licenses because doing so would have revealed the ultimate end user of the rad-hard microelectronics—China Aerospace. Xian and Li conspired to break up orders into multiple shipments in an attempt to circumvent U.S. export-control restrictions on the sale of U.S. Munitions List technology to China.[3]

Analyst Comment: This collection attempt and thwarted scheme demonstrate an approach used by collectors to illegally acquire rad-hard microelectronics. Based on investigations, it is almost certain that China Aerospace is driving its commercial suppliers to collect U.S.-manufactured rad-hard microelectronics. (Confidence Level: High)

EAST ASIA AND THE PACIFIC

OVERVIEW

Foreign collectors connected to this region remain dominant among those attempting to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. The East Asia and the Pacific region maintained the same 43 percent share of the total in fiscal year 2011 (FY11) as in FY10. This steady share represented an increase in the number of reported cases of more than 75 percent from FY10 to FY11.

Despite this continuity in East Asia and the Pacific's portion of the year's total reports from industry, some interesting shifts occurred from FY10 to FY11 within the data applicable to the region. The most significant overall trend within industry reporting was the increased clustering in the data among collector affiliations as well as methods of operation (MOs).

There was also increased quality of industry reporting, especially of the new top MO, suspicious network activity (SNA), which resulted in improved attribution by the Defense Security Service (DSS) Counterintelligence (CI) Directorate.

Commercial entities, in their 31 percent of total reported attempts in FY11, were probably attempting to gain opportunistic access to sensitive technologies for subsequent resale to other East Asia and the Pacific actors.

Additionally, industry reporting reflects a large number of cases (a combined 27 percent of the year's total) in which East Asia and the Pacific-connected entities reportedly attempted to establish a relationship with a cleared contractor, either through academic exchange, commercial deals, or individual employment. While these incidents did not suggest specific targeting of technology, they remain of interest due to the possibility that such relationships could lead to future opportunities for exploitation.

Multiple countries within East Asia and the Pacific perceive themselves as being surrounded by threats, including from each other. This leads them to believe that they must significantly upgrade their military capabilities, building their capacity for deterrence. Many of those countries also desire to make their militaries more self-reliant, although at present they remain significantly dependent on the acquisition of military technology from abroad.

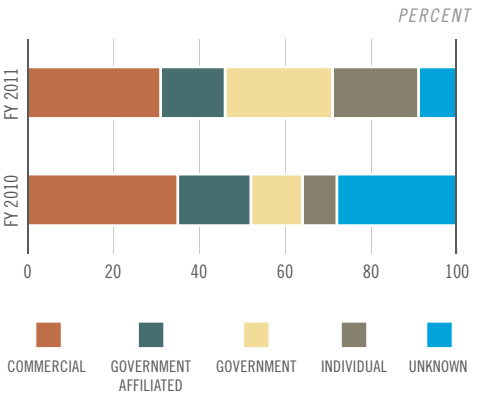
Reflecting the significant scope of these military modernization efforts ongoing in the region, requests originating in East Asia and the Pacific sought technologies found in nearly every section of the Militarily Critical Technologies List (MCTL). As in FY10, information systems (IS) was the single most targeted technology category, although reduced from FY10's 25 percent to 13 percent. However, the majority of those incidents were attributed to cyber actors and were non-specific in nature. In addition to IS technology, lasers, optics, and sensors (LO&S) technology remained a top identifiable targeting priority.

Despite the aforementioned frictions that exist between some countries in the East Asia and the Pacific region, unique relationships continue to exist between some of its geopolitical entities. Close economic ties between some of these entities continue to make third-party technology transfers a possibility. Some locations within the region are not governed by enforcement regimes that are sufficiently robust to adequately implement transit/transshipment license controls, creating popular diversion points for third-party transfers. Some East Asia and the Pacific collectors attempt to obtain U.S. technology to sell to third countries hostile to U.S. interests.

COLLECTOR AFFILIATIONS

East Asia and the Pacific entities targeting cleared industry were characterized by significantly variegated affiliations. Of the five categories of collector affiliation, four increased in number of reports from industry concerning East Asia and the Pacific, while the unknown category decreased in number of reports, and its share of all FY11 reports went from 28 to nine percent. Two categories—the top category, commercial, and government-affiliated—increased in number of reports, but fell slightly in percentage of the total, commercial from 35 to 31 percent and government-affiliated

COLLECTOR AFFILIATIONS
FIGURE 8



from 17 to 15 percent. The final two categories increased both in number of reports and share of the total, government from 12 to 25 percent and individual from eight to 20 percent.

Analyst Comment: The pattern revealed in industry reporting is that some East Asia and the Pacific collection entities use a diversified and persistent approach, often employing multiple collector types and MOs at the same time. When one entity fails, a second entity, often with a different affiliation, reengages the cleared contractor in pursuit of the same technology. DSS assesses that some East Asia and the Pacific collection campaigns probably represent coordinated national strategies. (Confidence Level: Moderate)

In particular, increased attribution of cyber incidents highlights the multifaceted nature of the threat to U.S. information and technology originating in East Asia and the Pacific. Overt collection efforts by commercial entities run in parallel with aggressive cyber collection activities, which target cleared contractor networks in attempts to exfiltrate data relating to sensitive U.S. information and technologies and the companies that produce them.

In some cases within East Asia and the Pacific, commercial entities are known to be tightly interwoven with other East Asia and the Pacific actors, relationships that cleared industry reporting and subsequent DSS analysis confirmed in FY11. This is especially so with regard to attempted technology collection and defense sales, as other collectors often use commercial entities to collect information on U.S. technology and programs. Commercial entities involved ran the gamut from large international corporations to small, privately owned companies with ten or fewer employees.

Analyst Comment: In many cases involving commercial entities, requestors failed to identify intended end users or uses. However, cleared industry reported frequent demonstrations of interest in a very specific system or capability from multiple separate entities, making it likely that they were acting on behalf of a common end user. (Confidence Level: Moderate)

While some requests for information (RFIs) from or attempts to purchase components by commercial entities resolved to innocuous entities, industry reporting cited a significant number of instances in which the companies and individuals behind these requests had appeared in previous industry or Intelligence Community (IC) reporting. Many of these entities were based in third countries, including the United States, Canada, and European nations, but could be attributed to East Asia and the Pacific end users.

Analyst Comment: Some collectors were likely attempting to circumvent U.S. export laws that apply different regulations to different locations within East Asia and the Pacific. It is likely that many of these collectors were acting as illicit technology brokers for other East Asia and the Pacific actors. DSS assessed that most requests made by entities identified in IC reporting as illicit technology brokers very likely reflected tasking by end users to acquire specific components, systems, or technologies. Additionally, inquiries from technology brokers associated with particular East Asia and the Pacific entities which mirrored otherwise innocuous requests can identify otherwise unidentified or intentionally misidentified end users. (Confidence Level: High)

A substantial minority of the commercial cases consisted of interest from companies in establishing business relationships with cleared contractors, either as distributors in the East Asia and the Pacific market or as suppliers of components for integration into systems under development by the contractors.

Analyst Comment: Integration of foreign-manufactured components into U.S. defense systems is a growing concern within the

IC and U.S. cleared industrial base. While the majority of cases in which companies attempted to establish supply chain relationships with cleared contractors appear unlikely to be directed efforts to infiltrate the contractors, DSS CI deemed these cases likely to be of intelligence value due to the identity of the companies interested in establishing connections with cleared contractors. (Confidence Level: Moderate)

In many other cases the acquisition mechanisms employed by East Asia and the Pacific militaries are manifestations of complex and very opaque systems of competing interests sharing common goals and end users. There are many unknowns concerning commercial entities, other collectors, and the varying nature of the relationships between them. This frequently makes specific attribution of commercially originated requests to the ultimate requestors and end users uncertain at best, and concrete findings of any kind difficult to establish.

Overt requests usually come from non-traditional collectors, such as commercial and academic entities. In the majority of cases associated with commercial entities, East Asia and the Pacific companies contacted cleared contractors and attempted to acquire sensitive, export-controlled, or dual-use components and systems by overt means.

Analyst Comment: Most separate incidents appeared to be innocuous, involving entities which did not appear to be acting in a duplicitous manner and which had not been cited in classified reporting for previous suspicious activities. Most of the commercial collectors involved maintain no apparent ties to intelligence services, and in many instances are likely motivated by financial gain. (Confidence Level: Moderate)

Additionally, the sharp rise from FY10 to FY11 in the number of reported cases attributed to government entities and the doubling of their share of the total, while noteworthy, should not be viewed as reflecting new entry into attempted technology collection by governments from East Asia and the Pacific, but rather as the result of refined attribution by DSS and increased quality of reporting from industry. Through security education and other means of generating increased awareness, cleared contractors increasingly recognized the threat posed by seemingly innocuous contacts and reported these incidents with greater frequency and attention to technical indicators. As a result of this increased fidelity, DSS attributed a large number of cases to government entities which would likely have been designated with the unknown affiliation in FY10.

Industry-reported cases attributed to individuals provided 20 percent of the FY11 total. Students attempting to obtain postdoctoral positions or other employment opportunities with cleared contractors dominated reported attempts, and the majority of these reports came from cleared contractors associated with U.S. universities. While available information can seldom establish a direct connection between foreign intelligence services and most, if any, of the students and academics who contacted cleared contractors, IC and law enforcement reporting provides numerous instances in which East Asia and the Pacific students have exploited access to sensitive or classified technologies to support parallel research and development (R&D) efforts in their home countries.

Analyst Comment: While most or all of these individuals are likely legitimately interested in obtaining positions with cleared contractors, placement within those facilities would likely offer academics the opportunity to exploit their access to personnel, information, and technologies resident in those facilities. Moreover, some individuals have used the bona fides of U.S. universities to acquire otherwise inaccessible components, materials, and systems for end users in their home countries. Review of industry and IC reporting leads DSS to assess that many

academics and their sponsoring institutions very likely view placement in U.S. facilities as supporting national technology collection goals. (Confidence Level: High)

METHODS OF OPERATION

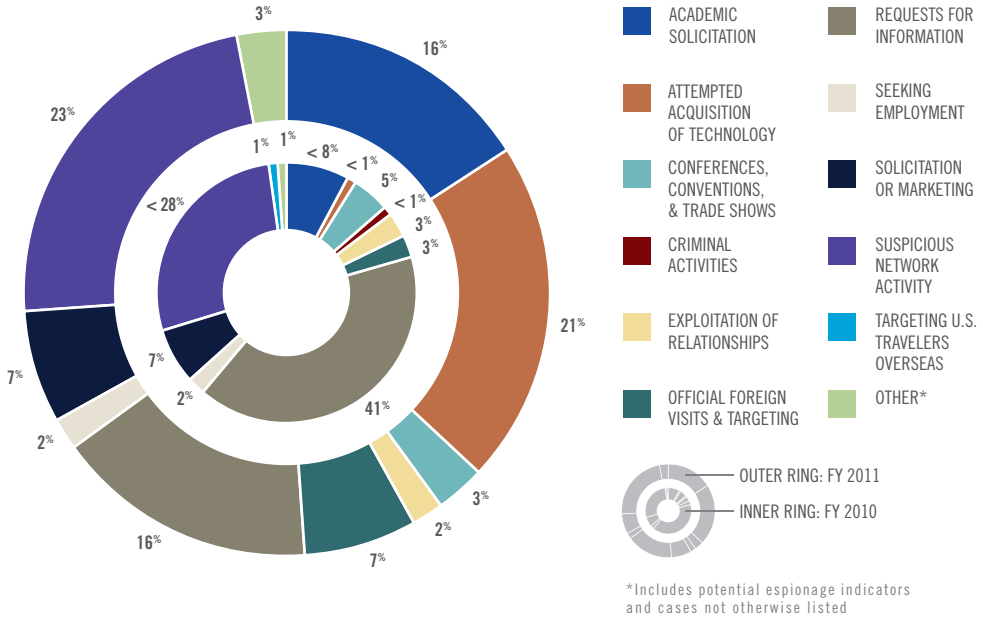
The data on frequency of use of different MOs by collectors from East Asia and the Pacific fell into two tiers. SNA, attempted acquisition of technology, RFI, and academic solicitation each accounted for 16 percent of the total or more, whereas the portion that all other MOs accounted for individually remained in the single digits.

A major change in the DSS categorization method led to many reports that in previous years would have been labeled RFI being listed as attempted acquisition of technology, moving the latter category from low in the second tier in FY10 to the second highest category in FY11, at 21 percent. Within the upper tier, this dropped RFI from the top position in FY10 at 41 percent down to third in FY11 at 16 percent. It was joined at 16 percent by academic solicitation, up from eight percent in FY10. Partly as a result of the accounting change but also due to a continued increase in illicit cyber activity, SNA surged to the top of the region's MO list in FY11 at 23 percent of the total.

Together these four MOs accounted for over three-quarters of the East Asia and Pacific total. The next most common MOs, as measured by reports from industry, were official foreign visits and targeting and solicitation or marketing services, at only seven percent apiece.

The new top MO practiced by East Asia and the Pacific collectors, SNA, experienced increased quality of reporting from industry, which led to significant refinement in attribution. Increased clarity allowed DSS analysts to discard most reports of unsophisticated attempts to access cleared

METHODS OF OPERATION
FIGURE 9



*Includes potential espionage indicators and cases not otherwise listed

contractor networks through tactics such as brute-force attacks, attributing these actions to criminal rather than intelligence actors. Notably, almost all of the SNA reporting deemed to be of intelligence value resulted from spear phishing emails with malicious attachments received by cleared contractors.

Analyst Comment: While FY11 industry reporting of spear phishing emails significantly increased over FY10, this probably does not represent greater use of that vector, or delivery mechanism, but rather increased cleared contractor awareness, recognition, and acknowledgement of such collection attempts. In those instances in which a compromise occurred but no vector was identified, DSS CI assessed that the initial intrusion was likely achieved through an unidentified spear phishing email. (Confidence Level: Moderate)

Although attempted acquisition of technology and RFIs (accounting for 21 and 16 percent, respectively, of the total collection attempts reported by industry in FY11) are separated into different reporting categories, these MOs are employed very similarly, and both are associated very closely with commercial entities. Typically, reports of either type resulted from commercial entities requesting sensitive components or specifications through the cleared contractor's sales department, with many initial contacts failing to disclose the intended end user and use.

In most instances of attempted acquisition of technology, the entity sent an email with a purchase order for the cleared contractor's products. The second most common MO reported was RFI, again most commonly executed via email, web-card submission, or telephone call. RFIs often begin with general questions whose answers, if supplied, could be used to confirm or deny information on the technology or system, opening the way to more pointed and sensitive questions.

Both attempted acquisition and RFI represent a low-risk, high-reward approach to collection. If the request is questioned or deemed inappropriate, the entity can claim it was made in good faith with no knowledge of restrictions. If the request goes unchallenged, it provides immediate reward as well as building a potential relationship that can be exploited in the future. If the acquisition attempt is successful, it provides opportunity for reverse-engineering and significant savings in R&D costs.

Some requests initially appear innocuous, but gradually reveal themselves as apparent attempts to acquire sensitive or controlled technology for East Asia and the Pacific end users. In a handful of reports, entities openly or implicitly stated their intention to circumvent export controls by transshipping purchased components through third countries.

Analyst Comment: While U.S. export controls prevent many collection entities from purchasing sensitive, dual-use components and systems, it is likely that unauthorized East Asia and the Pacific end users have acquired components through entities located in countries without such restrictions and the falsification of end-use documents. (Confidence Level: High)

Academic solicitations jumped significantly as a percentage of industry reports, from eight percent in FY10 to 16 percent in FY11, and more than tripled in the number of reported approaches. This largely resulted from increased industry reporting of attempts by students and postdoctoral researchers to obtain positions with cleared contractors. U.S. universities reported receiving by far the greatest number of academic solicitations noted in DSS reporting. Reporting also reflected a significant number of solicitations in which individuals affiliated with East Asia and the Pacific universities and institutes requested research and other academic information produced by cleared contractor employees.

Analyst Comment: While much of the requested research material was both publicly available and basic in nature, attempts to acquire information directly from the author present the opportunity to expand conversations into areas outside the scope of the initial paper and into more sensitive areas of the cleared contractor employee's current research. Taking advantage of the academic predilection to share information in this way almost certainly presents an excellent avenue to support military research.
(Confidence Level: Moderate)

TARGETED TECHNOLOGIES

In FY11, the four most common targeted technologies by collectors connected to East Asia and the Pacific were IS; LO&S; electronics; and aeronautics systems, just as they were in FY10. However, the top technology, IS, actually fell slightly in number of reports and by almost half in share, from 25 to 13 percent. Technologies in the next three sections of the MCTL all increased in number of reports, but LO&S decreased in percentage from 13 to ten percent, electronics increased slightly from seven to eight percent, and aeronautics maintained its share unchanged at eight percent.

Even more interesting variation occurred in the second tier of technologies. The next four most commonly targeted technologies all increased in number of reports from industry. But while positioning, navigation, and time merely maintained its five percent share of the total and marine systems declined to five percent, two categories, armaments and energetic materials and space systems, doubled in the number of reports year over year and increased in proportional share; the former actually doubled its share to six percent.

East Asia and the Pacific's increased practice of the SNA MO meant that there were more incidents in which the specific data targeted could not be determined; in such cases, DSS analysts frequently

TARGETED TECHNOLOGY
FIGURE 10

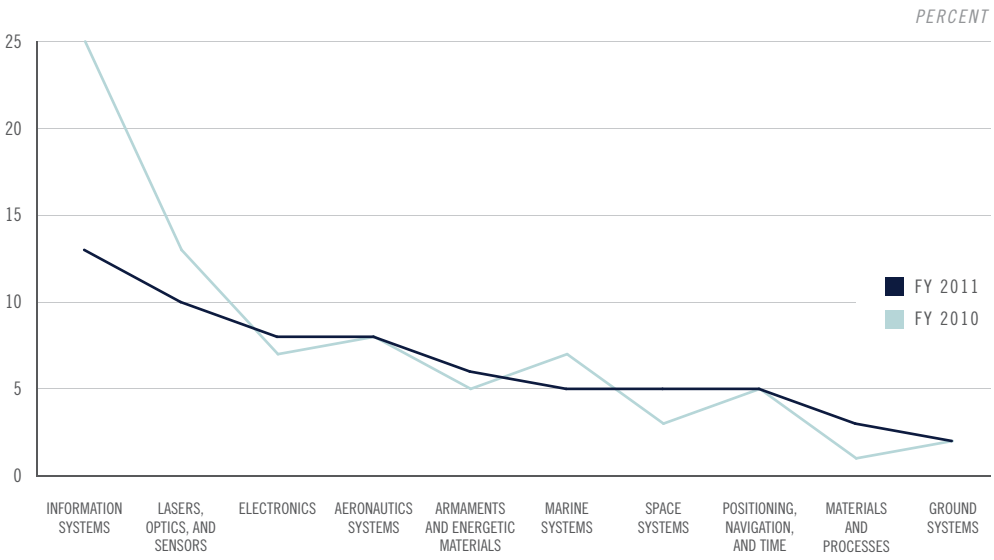


Figure illustrates the top ten most targeted technology categories in FY11 compared with the reporting statistics for the same categories from FY10.

identified attempts with the primary technologies affiliated with the subject facility. However, this determination was made on a case-by-case basis, and in many instances it was not possible to associate a cyber incident with a specific MCTL section. In instances in which entities contacted a facility more directly but still did not mention a specific product or technology, such as the case with many student requests and business solicitations, analysts regarded the request as undefined with regard to MCTL category.

Despite the fall in the number of cases attributed to IS technology in both numbers and share of the total, it remained the most commonly targeted section. Most cases involving IS as well as aeronautics technology originated from cyber actors and were nonspecific in nature. In the non-cyber cases in which entities expressed interest in specific IS technologies, software programs were the most common targets, particularly those supporting satellites, radar, and signals.

Analyst Comment: Whereas in FY10 DSS analysts frequently assessed the targeted technologies based on incomplete information regarding the incident or targeted facility, the improvement in the quality of industry reporting allowed for better identification of targeted technologies. DSS analysts did not designate a targeted MCTL category in those incidents which suggested multiple targeted technologies or targeting of non-MCTL information. The sharp decrease in reporting regarding IS compared to the previous year is almost certainly due to improved attribution techniques and results. (Confidence Level: Moderate)

Requests from East Asia and the Pacific that fell within the category of LO&S encompassed a wide range of technologies. Some of the most commonly targeted were advanced radar and sonar systems suitable for upgrading and modernizing the region's sometimes antiquated missile, air, and maritime defense networks and improving command and control capabilities. Similarly, interest in unmanned aerial systems within the aeronautics category is consistent with a need to survey and monitor against neighbors' infiltration and attack. The geographical, topographical, and geopolitical landscape of the East Asia and the Pacific region makes such technologies a matter of high priority to regimes and militaries within the region.

Among the most targeted LO&S technologies were shortwave infrared optical systems, which are useful for measurements imaging for a variety of civilian and military purposes, ranging from agricultural to battlefield targeting applications. While some of the requests received were ostensibly civilian in nature, others made specific reference to military hardening and specifications exceeding those required for civilian use. Collection entities also sought a variety of laser technologies.

Requests for electronics technology accounted for eight percent of the total, slightly more than the previous year. This section also encompassed a wide range of sub-technologies. Many requests targeted a variety of antenna systems as well as space-qualified equipment. Based on the specifications requested, the items were appropriate for use in satellite communications, but could also be applied to a number of other end uses. Of additional note, industry reporting concerning attempts by East Asia and the Pacific students to obtain placement with cleared contractors showed that a large number of requests were sent to professors and employees working in areas of study that have both commercial and military uses, including sensors, positioning, and detection technologies.

Analyst Comment: Many East Asia and the Pacific universities and research institutes have associations with their nations' militaries. Reported interest by such institutions in the study of the

technologies and applications discussed above is noteworthy, as many of the requesting academics and students are likely to contribute to military R&D following completion of their studies. (Confidence Level: Moderate)

The noted increase in industry reports concerning the attempted collection of armaments and energetic materials and space systems technology involved integrated circuits, switches, amplifiers, and other electronic components with applications to a variety of systems, which could include missile systems or weapons countermeasure systems.

Analyst Comment: It is not apparent what, if any, specific requirements have driven these increases. They are likely a result, at least in part, of general modernization and upgrade efforts and/or attempts to reverse-engineer any technology obtained to produce indigenous variants for domestic use and foreign sales. (Confidence Level: Moderate)

OUTLOOK

As anticipated in previous years' versions of this publication, industry awareness of the threat posed by entities from East Asia and the Pacific has consistently increased year over year, and will likely lead to greater numbers of reports from cleared contractors and further identification of entities of concern. However, even as this awareness has grown, DSS has not observed any discontinuities from the reported MOs that entities from the region have used over preceding years, providing evidence that those methods continue to be useful in acquiring U.S. technologies. Therefore, DSS CI assesses that East Asia and the Pacific entities will continue to aggressively target cleared contractors through both computer network exploitation activities and the overt means used predominantly by non-cyber actors. **(Confidence Level: High)**

East Asia and the Pacific commercial entities continued to lead all other collector affiliations. This points to some degree of success by those entities, so their collection efforts are likely to continue. The opaque but arguably close relationship between governments and industry within East Asia and the Pacific often manifests itself in collection patterns characteristic of coordinated collection strategies. DSS assesses it is very likely that commercial entities will lead the accounting of the East Asia and the Pacific collection effort in FY12, but may receive significant support from government, government-affiliated, and individual entities. **(Confidence Level: High)**

This year's industry reporting does not suggest any single, common, driving goal behind technology collection efforts beyond the continuing frictions in relations between countries within the region and between countries within the region and those from outside. It is likely that these general concerns will continue to drive the great scope of efforts to modernize and upgrade the somewhat backward and antiquated existing militaries of countries within East Asia and the Pacific, and thus collection attempts related to them. **(Confidence Level: High)**

The breadth of systems, components, and capabilities that East Asia and the Pacific collection entities target underscores these frictions and the dangers to which various regimes consider themselves subject. The immediacy of the perceived threats calls for a high priority on border surveillance and air and maritime defenses. Consequently, LO&S, particularly sensor technologies, will almost certainly remain a high priority. **(Confidence Level: High)**

Multiple regimes within East Asia and the Pacific seek advanced technology to transform their militaries from quantitative to qualitative forces. Technology can be a force multiplier crucial to success in that transformation. In pursuit of this, collection

entities will almost certainly continue to place a high priority on IS technologies and aeronautics systems technologies. However, the broadness of the goals pursued will likely drive collection entities, whether tasked or not, to target a very wide array of technology categories across nearly the entire MCTL. **(Confidence Level: High)**

Requests for sensitive or classified information and technology resident in the U.S. cleared industrial base, if successful, would likely directly support development of new military systems or upgrades to existing capabilities. Such requests also emphasize the degree to which indigenous research capabilities in the region, while improving, continue to rely on acquisition of foreign technology to further ongoing development efforts and will likely continue to do so in the foreseeable future. **(Confidence Level: High)**

Similarly, based on industry reporting, East Asia and the Pacific collection entities practice a diverse suite of collection methodologies, with significant effort exerted in SNA, attempted acquisition of technology, RFIs, and academic solicitation. These MOs are either "stand-off" methods practiced from a distance or arguably innocuous, and the use of this combination of methods is very likely to continue. **(Confidence Level: High)**

CASE STUDY: "IF AT FIRST YOU DON'T SUCCEED..."

In September 2011, a Massachusetts-based cleared contractor received a request for an export-controlled amplifier from a company based in East Asia and the Pacific. The company did not state the intended end user or end use in the initial contact.

Reporting from the same cleared contractor indicated that the model of amplifier requested had been the subject of numerous previous requests, including several from companies located in the U.S. and third countries. Several of these requests listed other East Asia and the Pacific actors as the intended end users.

Reporting from other cleared contractors cited several of the entities requesting the equipment as having contacted separate facilities seeking other particular items of sensitive, dual-use technologies. IC reporting identified several of those entities as suspected technology brokers for East Asia and the Pacific actors and enterprises associated with multiple military development projects.

Analyst Comment: Requests such as this one were typical of overt attempts by East Asia and the Pacific entities to acquire sensitive or classified information and technology resident in the U.S. cleared industrial base. While the contacting entities were likely unaware of each others' requests, viewing the requests together allowed DSS CI to establish a likely connection between the soliciting entities and end users associated with the national military in question. (Confidence Level: Low)

NEAR EAST

OVERVIEW

The Near East accounted for 18 percent of the worldwide total of industry reports to the Defense Security Service (DSS) for fiscal year 2011 (FY11), just as it did in FY10. The aggressive efforts of collectors associated with this region to obtain illegal or unauthorized access to sensitive or classified information and technology resulted in almost 75 percent more reports in FY11 than FY10.

Near Eastern collectors' steadily increasing volume of suspicious contacts over the last several years signifies a continued high value placed on the acquisition of U.S. defense technology and technological know-how. This is despite national goals, in several cases, of achieving greater self-sufficiency in the production of defense equipment. While the region produces some of its own defense equipment, the technology remains foreign-influenced, and rapid advances in defense technology mean the Near East continues to rely on accessing foreign sources.

At present, increased perceived threats from regional neighbors and/or the United States may have temporarily taken precedence over longer-term goals of self-sufficiency. Near East short-term collection efforts may be driven by the perceived need to quickly improve national defense infrastructures, particularly air defense-related technologies.

DSS continues to receive reports of Near Eastern entities' attempts to acquire U.S. technology by subterfuge. Near Eastern collectors have become exceptionally adept at using complex networks of front companies, shell companies, brokers, and procurement agents in their efforts to acquire U.S. technology. These collectors continue their attempts to acquire U.S.-origin technology through third countries, leveraging relaxed export-control laws.

Sometimes the subterfuge is somewhat more direct. Some Near East collectors attempt to exploit established trade assistance agreements (TAAs) with U.S. cleared contractors. Official visits and targeting was also prevalent in reporting as collectors sought to leverage official facility visits to gain unauthorized access to U.S. technology information.

Other frequently attempted MOs manifested themselves in FY11 when Near Eastern commercial entities sought to acquire U.S. technology, requested sensitive information, or solicited marketing relationships. Although not as prevalent as in FY10, targeting by Near East government agents of U.S. travelers on official business overseas, usually as cleared contractor personnel were departing the region, remained a threat.

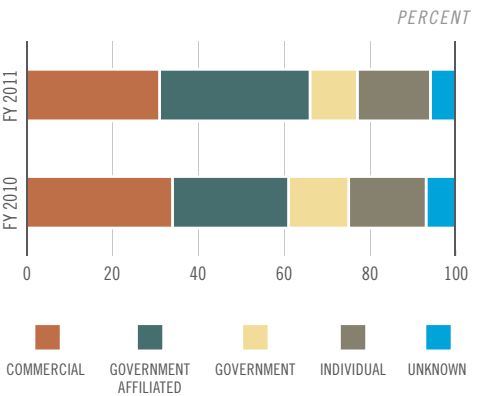
In FY11, Near Eastern collectors targeted a wide array of defense technologies, ranging from antiquated U.S. military hardware to new, state-of–the-art military technologies. Consistent with previous years' reporting, Near East collection targets spanned nearly all the sections of the Militarily Critical Technologies List (MCTL).

Students from the Near East continue to show interest in conducting postgraduate-level research in emerging technologies. Reporting received from industry shows evidence of an increase in academic solicitations from students seeking to conduct postgraduate research in cleared university-affiliated research centers. Near East student enrollment in these programs poses a technology transfer risk when students return home equipped with the knowledge and technological know-how to design and develop new defense technologies necessary to help their countries achieve self-sufficiency.

COLLECTOR AFFILIATIONS

All five collector affiliations increased year over year in number of reports from industry. The top two affiliations swapped places in the ranking from FY10 to FY11, while the remaining three maintained their positions. The interesting changes were in the percentages of the total each category accounted for. The new most common identification, government-affiliated, increased in percentage from 27 to 35 percent, while all four other categories, including the former top category, commercial, declined in share, by one to three percentage points each.

COLLECTOR AFFILIATIONS
FIGURE 11



Within the government-affiliated category for the Near East, the two main models involved affiliations between the government and either academics or commercial firms. Government-affiliated academics, purporting to be students and professors, tended to be associated with major universities; government-affiliated firms tended to

be major commercial companies. The academics typically requested access to cleared contractors' postgraduate research, placements for sabbaticals, assistance with or collaboration on research and scientific publications, and/or employment; government-affiliated firms tended to attempt to exploit established relationships with cleared contractors and leverage official cleared facility visits.

Analyst Comment: Near Eastern countries desiring to maintain or enhance their status as regional powers likely seek to establish technological autonomy and gain recognition as scientific and technological achievers, which requires the ability to independently develop advanced and innovative technologies. Currently, their education systems, scientific establishments, industrial bases, and/or forces of skilled workers probably lack the resources, equipment, and technical expertise to achieve such goals. Therefore they likely continue to rely on collections against western countries' industrial bases to cultivate the necessary knowledge and technical abilities and keep current on technology advances. (Confidence Level: Moderate)

Although industry reports identified with the commercial affiliation declined in their share of the Near East total and the affiliation fell from the top spot, it still accounted for nearly a third of all reports. During FY11, commercial entities maintained a consistent targeting of cleared contractors by seeking dual-use technologies. Sometimes the same individual attempted to acquire the same technology while purportedly representing multiple companies; sometimes multiple companies from the same country attempted to acquire the same technology.

Using commercial firms for collection attempts can constitute an effort to obscure government involvement in attempted collection against U.S. information and technology. Near East companies sometimes contacted cleared contractors in an attempt to either procure an export-controlled technology or solicit an opportunity to market the cleared contractor's technology within the country or region.

Various industry reports recounted incidents in which Near East commercial distributors requested U.S. technology in what would nominally be a legal and permitted acquisition. However, the purchases sometimes were on behalf of end users from other regions, after multiple attempts by entities in those regions to procure the same technology themselves had failed. In such cases, any subsequent transfers of defense technology violated signed agreements requiring U.S. approval. In other cases, regimes' acquisition of U.S. technology itself was illicit, and was then followed by a sharing of U.S. technology with the third parties that sought it indirectly.

Analyst Comment: DSS assesses that aggressive collectors from other regions likely exploit Near East relations with the United States to acquire U.S. defense technology for misrepresented end uses, as well as employ other successful MOs. When Near Eastern states obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base, it is likely to undergo further illicit transfer. (Confidence Level: Moderate)

FY11 industry reporting attributed to individual collectors represented 17 percent of suspicious contacts to cleared industry, remaining proportionally consistent with last year's results. These collectors continue to provide little to no information to indicate ties to commercial or government entities. Individual collectors typically employed the academic solicitation, the request for information (RFI), and seeking employment MOs.

Analyst Comment: Individual collectors likely attempt to increase their chances of successfully obtaining U.S. sensitive or classified information and technology

by obscuring ties to governments and commercial firms known to the United States. (Confidence Level: High)

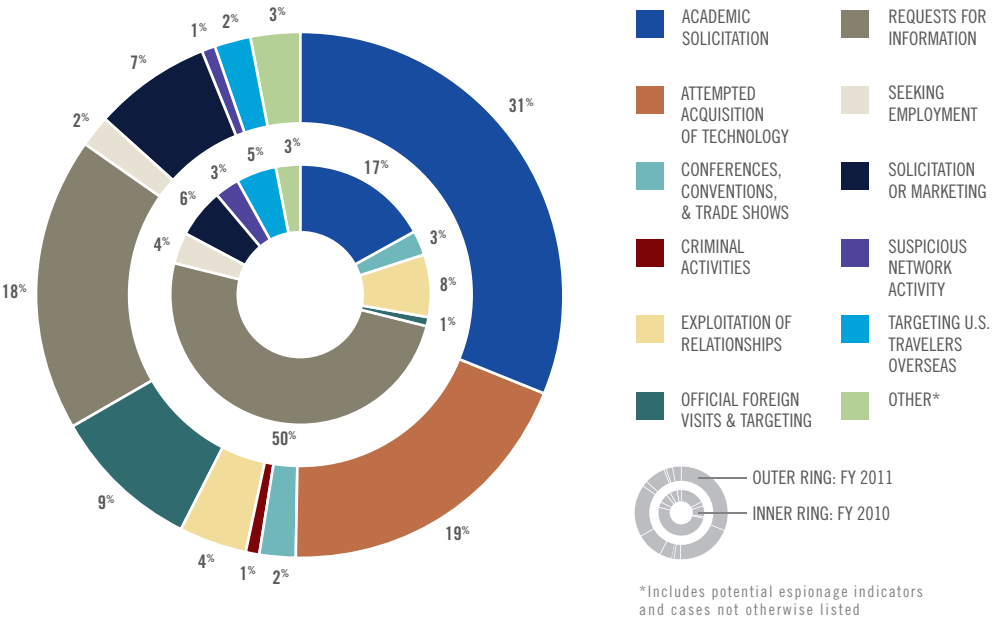
Reported collection attempts associated with Near Eastern government entities declined slightly in proportion of the whole, from 14 percent in FY10 to 11 percent in FY11, even as the number of industry reports in that category increased by over 40 percent. In FY11, governments with access to cleared contractor facilities via established TAAs continued to attempt to leverage them to collect against U.S. information and technology. Known or suspected intelligence officers (IOs) supplemented official delegations in visits to cleared facilities, typically under the guise of official representation. Also, in conformance with a FY10 trend, in some countries airport security continued targeting cleared contractor personnel while on official business in-country. Industry reporting documented multiple incidents of cleared contractor personnel receiving intense scrutiny from airport security elements when attempting to depart the country.

METHODS OF OPERATION

An adjustment in the DSS accounting system for MOs resulted in many FY11 cases that would previously have been categorized as RFIs being labeled instead as attempted acquisitions of technology. This had a major effect on the top of the listing of MOs used by Near East collectors, as represented by industry reporting. The RFI, which had been at the top of the FY10 listing by accounting for half of that year's reports, fell to third at 18 percent of the total in FY11. The corresponding rise in attempted acquisition of technology reports was from no reports in FY10 to 19 percent of the total in FY11.

The most notable change, however, occurred with regard to reports on academic solicitation. The number of such reports

METHODS OF OPERATION
FIGURE 12



*Includes potential espionage indicators and cases not otherwise listed

more than tripled, an increase of 220 percent. Academic solicitation accounted for 31 percent of this year's larger total.

Recent changes in U.S. visa requirements loosened restrictions on foreign students, allowing more to remain in the United States after graduation, and available statistics verify that the number of such students staying has increased in recent years.

Analyst Comment: Some of the statistical shift can be attributed to the recategorization of many reports from RFIs to the attempted acquisition of technology. However, it is likely that a greater part of the explanation for the diversion of Near Eastern collection efforts into solicitations aimed at exploiting U.S. academia lies in loosened visa requirements. (Confidence Level: Moderate)

Of the lower tier of MOs, as measured by the number of industry reports, none individually accounted for more than nine percent of reports. Some increased in number of reports, some declined, and there were resultant adjustments in proportional share. Two of these lesser MOs deserve specific comment, however. There were 11 times as many reports of targeting during official foreign visits to cleared contractors in FY11 than in FY10. In contrast, the suspicious network activity that represents such a noted threat from other regions actually declined in number of reports related to the Near East, measured year over year, and in FY11 accounted for only one percent of reports.

As noted in the previous section, academics, both students and professors, constituted a major bloc of Near Eastern government-affiliated collectors. Students sent emails to cleared U.S. professors requesting to join research programs in technology areas related to energy, materials, electronics, and mechanical and aerospace engineering.

Analyst Comment: The levels at which students from the Near East are contacting U.S. professors engaged in classified research are alarming. Almost exclusively, such programs are classified because the research they conduct is defense-related. It is noteworthy that the U.S. universities targeted are not commensurate with the top universities attended by Near Eastern students in the United States or located in areas with large home-country expatriate communities where foreign students typically seek to live. It is likely that many of the approaches to particular U.S. professors by Near Eastern students are intended to gain illicit access to sensitive or classified information and technology in targeted technology areas. (Confidence Level: Moderate)

Although no available evidence corroborates that Near Eastern government agencies are presently tasking student placement at cleared contractor facilities, some intelligence reporting suggests that the practice has occurred in the recent past. Students may be recruited, trained, and tasked as sources, and receive financial aid and support.

Analyst Comment: Some Near Eastern students seeking placement at cleared contractor facilities receive financial support from their governments. Government-sponsored students would likely attempt to collect technical information on behalf of their government in return for its sponsorship. (Confidence Level: Moderate)

Although attempted acquisition of technology was the second most prevalent MO practiced by Near Eastern collectors as represented by industry reporting, at 19 percent of the total it fell far behind academic solicitation. Intelligence Community (IC) reporting showed that some countries' collectors attempted to purchase sensitive or classified U.S. technology directly, usually via email or telephone, whereas others made their approaches indirectly, using front companies or third-country entities to make contact with U.S. companies. Industry reporting during FY11 corroborates IC reporting, with requests for

export-controlled technology linked to the Near East originating from at least a dozen foreign countries.

Analyst Comment: Because of the nature of clandestine attempts to acquire sensitive or classified U.S. technology, DSS assesses that FY11 industry reporting almost certainly does not provide a complete representation of this aspect of Near Eastern collection activities. Some companies in other regions have a documented history of providing Near Eastern collectors with U.S. technology, and during FY11 DSS analysis found a substantial increase in such links. DSS assesses it as very likely that some portion of the reported attempts to acquire U.S. technology that DSS attributed to collectors from other regions had intended Near Eastern end users. (Confidence Level: Moderate)

Direct attempts to acquire sensitive or classified U.S. technology via purchase, usually requested via email or telephone, were most often made by commercial firms overtly requesting to purchase export-controlled technology. When commercial entities target U.S. technology, it is often for competitive advantage, with the export of defense production in mind. Most often, such Near Eastern collection entities attempted to procure U.S. technology in a seemingly innocuous and legitimate manner. Similarly, commercial firms constitute the affiliation of Near Eastern collectors predominantly employing the relatively similar and seemingly straightforward MOs of the RFI and solicitation and marketing.

As noted earlier, however, such seemingly innocuous, legitimate, and straightforward requests can be the result of deliberate efforts to minimize the signature of government involvement. DSS evaluation of information concerning certain Near Eastern firms reveals the likelihood that the government in question had a hand in certain requests, such as requests to market a cleared contractor's global positioning system or act as an intermediary for brokering aerospace and defense deals with the United States.

As represented by FY11 industry reporting, the RFI was Near Eastern collectors' third most frequently used MO, representing 18 percent of reported cases. These contacts consisted of web-card submissions that requested the cleared contractor to provide more information regarding its products and emails to cleared contractor employees to obtain additional information. For example, in May 2011, a California-based cleared contractor facility received an unsolicited email request for information regarding ship technology. The sender stated that he was studying naval architecture and drafting an article about such technology for a home-country newspaper.

Analyst Comment: The email to the cleared employee was likely an attempt to obtain specific information about such ships under the guise of drafting an article. Any information provided to the sender probably would have been used to determine specifications and aid in reverse-engineering a ship for home-country use. (Confidence Level: Moderate)

Although FY11 industry reporting registered official visits and targeting at only nine percent of the year's total, that represented a noteworthy increase in both number of cases and percentage share from FY10. This MO is typically employed by governments or defense firms that maintain defense relationships with cleared contractors. In FY11, under the auspices of official delegation visits, Near Eastern entities made numerous attempts, in multiple variants, to leverage their admission to cleared contractor facilities to gain illegal or unauthorized access to sensitive or classified U.S. information and technology. For example, some visitors, typically through casual conversation, persistently queried cleared contractor personnel for sensitive information that fell outside the agreed-upon topic or scope of discussion. Additionally,

delegations attempted to make last-minute revisions to the approved list of individuals visiting the facility so as to insert known or suspected IOs into their delegations.

In FY11, some Near Eastern entities employed additional methods to exploit established trade agreements. Typically, employees of privileged firms would contact cleared contractor personnel via email and attempt to leverage an established relationship by inquiring about sensitive information beyond the scope of the TAA. The pattern in previous incidents using this approach has been for foreign personnel to deliberately solicit multiple cleared contractor personnel through casual conversation in pursuit of the same information.

Analyst Comment: DSS assesses that some Near Eastern entities likely prefer using the official foreign visit MO over email contact to target cleared industry because in-person requests appear less premeditated. (Confidence Level: Moderate)

Although constituting only two percent of industry reports, the targeting of cleared contractor personnel traveling overseas on official business did still occur in the Near East in FY11. Industry reported multiple instances of airport security personnel selecting cleared contractor employees for enhanced scrutiny as they attempted to depart for home. Actions included invasive questioning regarding classified and proprietary information and occasional seizure and exploitation of contractor-issued laptops and electronic devices.

Of collection activity ascribed to Near Eastern entities in FY11, suspicious network activity remained at a low level. Reported Near East-originating cyber activity directed against cleared contractors included brute-force password attacks against internet-accessible servers and spear phishing emails that sent back information on recipients but contained no malware in attachments or links. Some Near Eastern actors conducted an intelligence campaign that consisted of relatively innocuous but extensive collection efforts, including on social network sites. Directed against the Department of Defense and its personnel as well as some cleared contractors, they sought to gather email contact lists and similar information. Such tracking and reconnaissance-type activities posed a low threat and did not result in any confirmed intrusions into cleared contractor networks in FY11.

Analyst Comment: While limited in number, the recent Near East-originating spear phishing campaigns likely served to collect information about the recipients so as to check the accuracy of target lists and the effectiveness of the messages in getting recipients to open them. Collection agents almost certainly sought this data in order to more effectively target particular employees when conducting future spear phishing operations against cleared contractors. (Confidence Level: Moderate)

TARGETED TECHNOLOGIES

The top six technology categories targeted by collectors from the Near East, as measured by FY11 reports from cleared industry, were the same as in FY10. The numbers of reports relating to all six sectors of the MCTL increased in FY11, by percentages ranging from 45 to 210 percent. However, while four of these technologies (lasers, optics, and sensors [LO&S]; space systems; armaments and energetic materials; and electronics) also increased their share of the total, two sectors (including the top category, information systems [IS], as well as aeronautics systems) declined in share. The result was that these top six targeted technologies became more tightly bunched, ranging from eight to 14 percent apiece in FY11 in contrast to five to 16 percent in FY10.

Thus, reporting showed that Near East entities' technology interests became more evenly spread across the field, with collectors seeking more U.S. information

TARGETED TECHNOLOGY
FIGURE 13

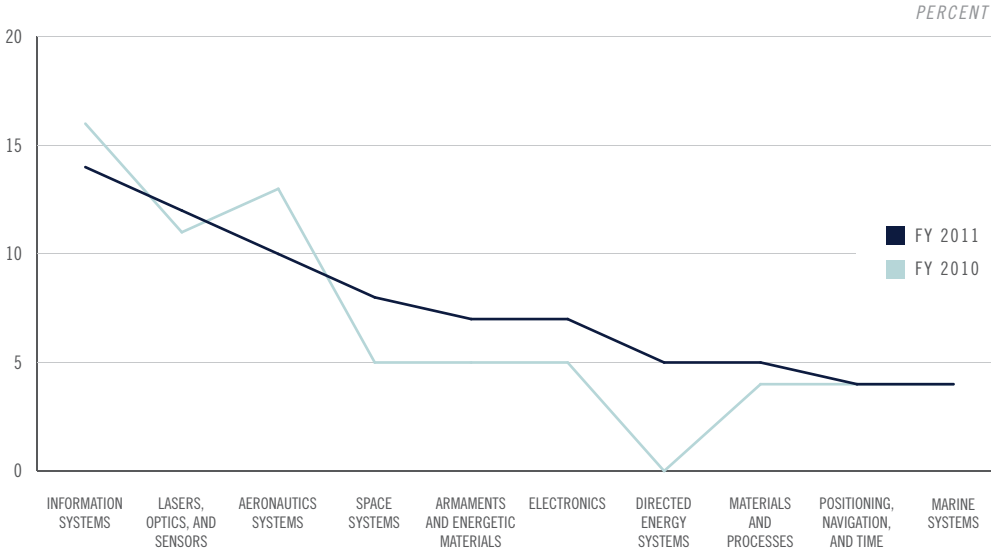


Figure illustrates the top ten most targeted technology categories in FY11 compared with the reporting statistics for the same categories from FY10.

and technology almost impartially. Within this wide range of technology sectors, some particular technologies came to the fore, including unmanned aerial vehicles, underwater autonomous vehicles, night vision devices, modeling and simulation (M&S) software, radiation-hardened (rad-hard) electronics, commercial aircraft, missile technology, and radar components. On the other hand, while a particular technology, an inertial navigation system, was absent from this year's industry reporting on the Near East, it should be noted that some requests for the technology resolved to companies from other regions which have a history of conducting business with Near Eastern entities and which failed to identify an end user.

Analyst Comment: It is likely that some of the third-country requests for the system were intended to supply Near Eastern end users. (Confidence Level: Moderate)

The IS technology sector received the most attention from Near Eastern collectors, as reflected in FY11 industry reporting. The number of reported collection attempts from this region rose 75 percent from FY10, representing 14 percent of the total in FY11.

Potential Near Eastern collectors practicing the longer-term MO of academic solicitation showed a high level of interest in academic programs addressing radar, communications, antenna, and radio technologies. Other Near Eastern collectors attempted to acquire IS technologies more directly. They specifically targeted U.S.-developed command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems technology, and requested to purchase dual-use telecommunications equipment.

Analyst Comment: The courses of academic study in question are likely targeted for their defense applications that support advances in wireless networking and communication. Those who sought C4ISR technology probably did so to enhance battle space awareness, airborne electronic warfare systems, and naval electronic support measures systems. (Confidence Level: Moderate)

LO&S technology, at 12 percent of the total, was the second highest Near Eastern collection priority in FY11, based on industry reports that doubled year over year. The attention was attributable largely to interest in U.S.-developed radar technologies associated with naval and ground vehicle applications.

Examples of attempts against LO&S include a Near Eastern research company contacting multiple cleared contractors in FY11, requesting detailed technical information regarding U.S. naval radar platforms. In other cases, Near Eastern delegations visiting cleared contractors conducted entire facility visits in a mode of aggressive attempts to gain unauthorized access to particular technology assembly processes.

Analyst Comment: Near Eastern delegation personnel were likely attempting to acquire the schematics and learn about the assembly processes to provide insight into the functioning of the specified technology. Collecting entities likely sought to obtain such technical know-how to strengthen their country's indigenous development and production capability and decrease the vulnerabilities inherent in relying on foreign sources for military equipment. (Confidence Level: Moderate)

In FY11, aeronautics systems technology remained a noteworthy Near Eastern collection target, accounting for 10 percent of industry-reported incidents, even though the category experienced a relatively "low" 45 percent increase in number of reports. Unmanned aerial systems were a primary target, including associated technologies and short-range unmanned aerial vehicles (UAVs) normally used for surveillance purposes.

Analyst Comment: Border security and terrorist threat concerns have likely heightened Near Eastern nations' interest in enhanced surveillance capability, leading to attempts to acquire U.S.-developed mini-UAVs to strengthen their security presence along their borders. (Confidence Level: Moderate)

Based on industry reporting, Near Eastern entities targeted space systems technology in FY11 at eight percent of the total, but with a 210 percent increase in number of cases. Powers within the region that are investing heavily in space programs have plans to launch several indigenous satellites for military and civilian use over the next several years.

In a space systems-related trend, Near Eastern students also demonstrated significant interest in conducting research related to rad-hard electronics, which are necessary to withstand the high levels of radiation encountered during space flight (see the Special Focus Area section). In one case, a national of a Near Eastern country attempted to acquire a free trial of a cleared contractor's version of M&S software (which satellite programs require) by creating a fictitious web-based email account using the name of a U.S. cleared employee. The attempt failed only because an employee of the cleared contractor recognized the name and asked the cleared employee whether he had sent the email.

Analyst Comment: For any country within the Near East, having a successful space program would be a substantial source not only of military benefit but also of national pride. Interested collectors likely target U.S. space technology through a variety of means. Collector attempts to acquire satellite and M&S software are likely linked to aspiring national satellite programs. (Confidence Level: Moderate)

Armaments and energetic materials technology increased from being the subject of five percent of total industry reports related to the Near East in FY10 to seven percent in FY11, representing an increase of over 152 percent in number of reports. Near Eastern government and government-affiliated entities attempted to leverage official facility visits to gain access to U.S. classified or export-restricted technology information and data, including U.S. missile defense technology and technical data and source codes of missile defense systems.

Analyst Comment: Near Eastern governments are likely concerned with countering missile attacks. They probably sought to enhance their missile defense platforms' capability to withstand rocket and missile threats by correcting deficiencies in missile defense capabilities, leading to their active attempts to address these deficiencies through system upgrades. (Confidence Level: Moderate)

Electronics technology also received substantial interest from Near Eastern collectors, representing seven percent of the year's reports, a rise in number of over 150 percent. Near Eastern collectors focused their efforts on various microwave, radar, antenna, and other specialized electronics systems and components.

OUTLOOK

The Near East contains several countries that harbor hostility toward each other, and perceive threats against their safety and security to be immediate. Some are on good terms with the United States, others are not. These countries strive not only to counter any regional attack by one another and in some cases from the United States as well, but also to achieve regional dominance in the Middle East. All Near Eastern collectors will likely remain reliant on acquiring U.S. information and technology to enhance their defensive and offensive capabilities and support their own military industrial bases, so will almost certainly continue to target U.S. technology. **(Confidence Level: Moderate)**

The Near East includes countries that are or strive to be technologically competitive with U.S. defense industries, and even to establish and maintain a global economic advantage in the field of defense exports. Stable economic success can come to rely heavily on indigenous manufacturing entities successfully collecting against equivalent, rival U.S. technologies. Technologies targeted by Near Eastern interests in FY12 will likely include a wide variety of U.S. systems and equipment in pursuit of modernization and enhancement of their own forces, as well as their likely goal, moving forward, of dominating specific defense markets for economic gain. **(Confidence Level: Moderate)**

Near Eastern collector affiliations will likely settle into the new pattern established in FY11. Government-affiliated entities will likely remain the top category, largely due to the number of Near Eastern students and professors requesting some sort of association with cleared contractors, which requires them to provide some identifying information. In contrast, individual and unknown collectors will likely remain noteworthy as some near Eastern entities strive to provide minimal or no information linking them to their home countries. **(Confidence Level: High)**

Commercial firms will very likely contribute a noteworthy share of overall reported Near Eastern collection attempts again in FY12. Governments will likely continue to attempt to exploit official facility visits so as to gain unauthorized access to U.S. information and technology. Perceptions of success in employing this tactic will likely result in the continuation of its use from FY11 into FY12. Other Near Eastern commercial entities

will very likely continue to use companies located outside of the region to request U.S. technology. **(Confidence Level: High)**

Near Eastern MOs will also likely remain stable in the near future. Numbers of reported academic solicitations will almost certainly remain at high levels as students continue to seek entry into cleared research programs and request technology under the guise of academic cooperation. Recent changes in U.S. visa requirements will very likely continue to make U.S. research programs a prime target for Near Eastern collection activity. **(Confidence Level: High)**

In their attempted acquisition of U.S. technology and information from cleared contractors, some Near Eastern collectors will probably take very direct approaches, combining this MO with RFIs; official foreign visits; solicitation or marketing; exploitation of relationships; conferences, conventions, and trade shows; and targeting U.S. travelers overseas. Other collectors will likely continue to use a variety of circuitous methods to procure technologies, relying heavily on front companies, procurement agents, and brokers located abroad. As more of these procurement networks are exposed, Near Eastern acquisition methods will likely evolve even further in the direction of advanced techniques to attempt to delude U.S. companies, such as the use of western-style aliases and company names from non-threatening countries.
(Confidence Level: High)

Current events and the need to defend their countries against the aforementioned perceived threat of military strikes within the region or by the United States will almost certainly continue to focus Near Eastern technology collection efforts in FY12. These would likely be aimed, first, toward addressing any previously identified limitations in indigenously produced missile defense systems, then on further enhancing missile defense platforms' capability against rocket and missile threats. Collection attempts against cleared contractors will likely target missile technologies and radar components. **(Confidence Level: High)**

Given various Near Eastern governments' desires to strengthen their border security, a revived focus on aerial and underwater autonomous vehicles for surveillance purposes will likely reemerge in FY12, leading to continued targeting of U.S.-manufactured unmanned systems.
(Confidence Level: Moderate)

Any country within the Near East desiring to launch indigenously produced satellites will likely continue to target U.S.-derived rad-hard electronics.
(Confidence Level: Moderate)

CASE STUDY: PERMUTATIONS

The following case demonstrates the convoluted mechanisms by which some Near Eastern entities seek to acquire U.S. export-controlled technology. During FY11, a suspected procurement agent for a Near Eastern regime was seeking various radar, microwave, and electronic components. He contacted several cleared contractor facilities and U.S. businesses, using various company names and email addresses in his requests.

In June 2011, the agent, purportedly representing a Near Eastern company, contacted a New York-based cleared contractor facility seeking the price and availability of two items of an export-controlled technology. On the same day, another individual, representing a commercial entity in another region, contacted the cleared contractor facility regarding the acquisition of two items of the export-controlled technology as well as other electronic components. The items requested by both procurement agents had the same specifications. According to the cleared contractor, specifications for the items were uncommon, as none with those specifications had been sold before.

Analyst Comment: Considering the unusual specifications of the requested items, combined with the similarity of the two requests, DSS assesses that the two suspicious contacts were likely related. The out-of-region firm was probably seeking to procure export-controlled items on behalf of Near Eastern entities.
(Confidence Level: Moderate)

In December 2010, the same Near Eastern procurement agent contacted the same cleared contractor facility, this time claiming to represent a company located in a different Near Eastern country. He requested a quote for six amplifiers of an advanced type. IC reporting revealed that he had made multiple previous solicitations as well. In December 2010, the agent—purportedly representing both the same company and yet another company in yet another Near Eastern country—contacted U.S. businesses seeking a variety of export-controlled advanced amplifiers.

An available business directory classifies the procurement agent's company as trading in textiles, clothing, and footwear. However, DSS records reveal it is linked to multiple requests for U.S. electronic components with warfare applications.

Analyst Comment: Reporting from cleared industry continues to illustrate Near Eastern collectors' use of complicated networks consisting of third-party intermediaries, front companies, brokers, and procurement agents to attempt to illicitly acquire U.S. technology. DSS assesses that the individual in question is almost certainly a procurement agent for his government, specializing in radar and microwave components that could be used for electronic warfare operations. He probably uses various company names, email addresses, and locations to facilitate attempts to illegally acquire U.S. export-controlled technology. It is likely that Near Eastern entities also use brokers or intermediaries based in other regions to further their acquisition of U.S. technology.
(Confidence Level: High)

EUROPE AND EURASIA

OVERVIEW

Europe and Eurasia was the third most active region in fiscal year 2011 (FY11) in terms of reports from industry concerning collectors attempting to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. Yet as significant as that is, it might seem less consequential when compared to the approximately 75 percent increases by the two most active regions, East Asia and the Pacific and the Near East, and a 129 percent increase by the fourth-ranking South and Central Asia. In this context, industry reports on collection attempts originating in Europe and Eurasia increased by "only" 60 percent in FY11.

Yet some factors serve to heighten concerns about Europe and Eurasia. The region contains some of the most advanced technological and economic competitors to the United States, as well as some of the most skillful and clever human and cyber intelligence collectors. It is likely that even industry reporting and other counterintelligence contributions combined underestimate the totality of the ongoing Europe and Eurasia efforts to gain illicit access to U.S. industrial secrets.

In industry reporting, commercial entities and government-affiliated institutions (often involved in research and education) were the top two Europe and Eurasia collector affiliations, at 45 and 19 percent of the total, with individuals and government following. From FY10, the number of reported contacts by entities with unknown affiliation decreased and the proportion of the total accounted for by that category went from second position at 28 percent to fifth position at ten percent. This could reflect collectors' greater willingness to disclose association with government-affiliated research organizations due to deepening economic ties between the United States and Europe and Eurasia.

Attempted acquisition of technology was the method of operation (MO) Europe and Eurasia entities used most, as reflected in industry reporting, accounting for over a third of the FY11 total, followed by the request for information (RFI) at 29 percent. The relative prominence of these categories is consistent with the previous year's data. New Defense Security Service (DSS) categorization guidelines require that a contact formerly considered an RFI now be identified as an attempted acquisition of technology if it solely sought to purchase the technology.

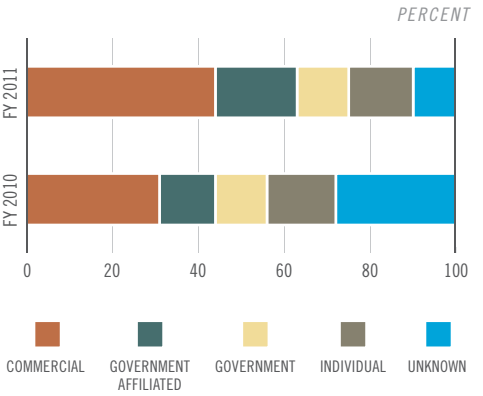
Based on industry reporting, Europe and Eurasia collectors targeted aeronautics systems and lasers, optics, and sensors (LO&S) almost equally, followed closely by information systems (IS) technology and electronics technology. They were all clustered within a narrow range, each accounting for 10 to 16 percent of the FY11 total.

The implied continuity in Europe and Eurasia collection emphases is attributable to the ongoing efforts to upgrade military technology. Europe and Eurasia countries seek to accomplish a variety of goals, whether reducing dependence on natural resource exports, decreasing dependence on foreign supply sources and thus foreign influence, boosting domestic production of military goods for both domestic use and export, and/or creating indigenous high-technology sectors.

COLLECTOR AFFILIATIONS

Collector affiliations reflected in industry reporting linked to Europe and Eurasia became ever more concentrated in FY11 on commercial collectors. Whereas in FY10 reports were fairly well distributed between the five categories, from 31 percent for commercial down into the teens, in FY11 the commercial category accounted for 45 percent of the total, with no other category exceeding 19 percent.

COLLECTOR AFFILIATIONS
FIGURE 14



Beyond this basic observation, there was some interesting movement within the statistics. In numbers of reports during the most recent year, the unknown category decreased by 43 percent, while the other four all increased, two of them by around 50 percent and two by over 100 percent. In terms of change from FY10 in percentage of the total, in addition to a decrease in the share accounted for by unknown collectors from 28 to ten percent, the individual collectors' share also decreased, while the government collectors' share was unchanged at 12 percent. This left the government-affiliated collector category to increase from 13 to 19 percent

and the commercial category from 31 to the aforementioned 45 percent.

Consistent with the previous year's reporting, commercial entities remained the primary affiliation of collectors associated with Europe and Eurasia in FY11, with the number of reported cases more than doubling year over year. Many Europe and Eurasia commercial entities identify neither end users nor specific technologies in their requests.

Analyst Comment: Some ostensibly commercial and individual Europe and Eurasia collectors demonstrated a level of knowledge about technologies that was consistent with that of intelligence officers (IOs). DSS assesses that the continued increase in reported activity by Europe and Eurasia commercial collectors likely reflects an effort to upgrade military technology. Certain aspects of the effort to modernize civilian economies likely dovetail with military requirements for improved technology. (Confidence Level: High)

Interest by Europe and Eurasia commercial entities in developing business ties to the United States is increasing, and contacts by collectors affiliated with them are as well. Simultaneous with the 14 percentage point increase in the share of contacts made by commercial collectors, government-affiliated collectors became the second most common category, with the number of such cases in FY11 more than doubling over FY10. The share of contacts from unknown collectors decreased by almost half, and those from individuals slightly.

Analyst Comment: Economic ties between the United States and most countries in Europe and Eurasia are close, and in some cases are growing closer. The significant increase in reports linked to government-affiliated entities likely reflects a greater willingness by collectors to disclose association with government-affiliated research centers in light of these closer economic ties. Simultaneously, multiple countries within Europe and Eurasia almost certainly intend to remain competitive in the world arms market with the United States; Intelligence Community (IC) reporting indicates that such countries view the United States as a market competitor for the sale of military equipment. (Confidence Level: High)

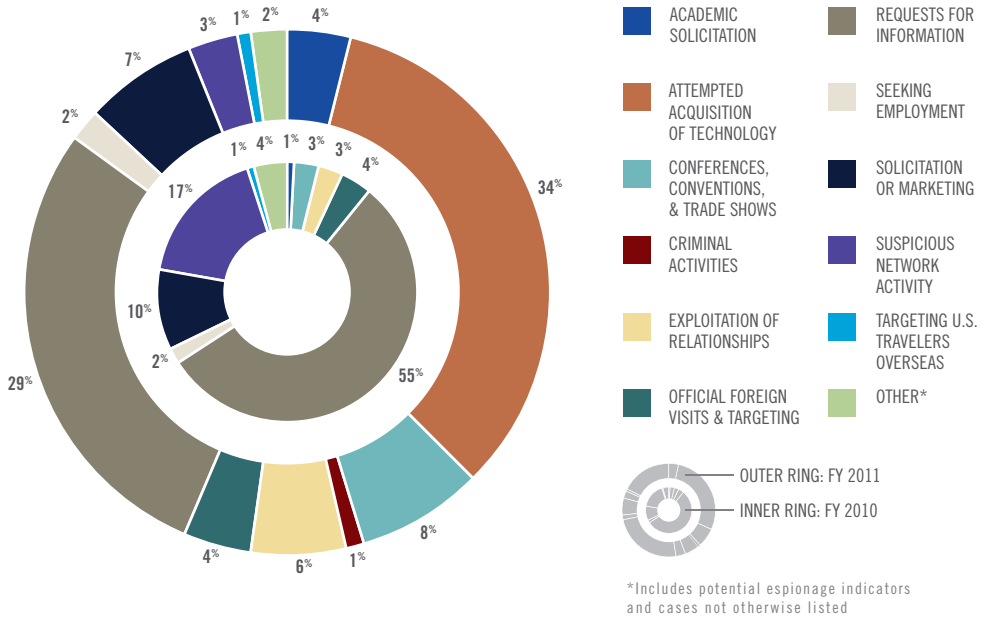
METHODS OF OPERATION

Regarding the MOs that collectors linked to Europe and Eurasia were reported by industry as using, attempted acquisition of technology at 34 percent and RFI at 29 percent combined to account for even more of the total in FY11 (63 percent) than they did in FY10 (55 percent). In the interim, DSS changed its accounting methodology such that many collection attempts that would previously have been labeled as RFIs are now categorized as attempted acquisition of technology.

The increase in these two categories might seem to make all the other MO categories relatively unimportant, with each of them accounting for only one to eight percent of the total. But if the two most common MOs represent the simplest, most straightforward method of attempting to obtain illegal or unauthorized access to sensitive or classified information and technology, it should still be noted that the wide range of other MOs recorded in industry reports represent all the "Plan B" methods. In other words, one may not succeed in gaining the desired information or technology by buying it or asking about it outright. In that case, the next-most-likely-to-succeed method is to somehow get someone close to a cleared contractor, then seek opportunities to gain illegal or unauthorized access to the desired materials. Whether at a conference, convention, or trade show, via a delegation visiting a cleared contractor in the United States, by targeting a U.S. traveler overseas, or by obtaining a job or academic placement or setting up a marketing arrangement, collectors seek to insinuate themselves into a position or relationship they can exploit

METHODS OF OPERATION

FIGURE 15



*Includes potential espionage indicators and cases not otherwise listed

to their benefit. Success for them almost certainly results in harm to the interests of cleared contractors as well as the larger military, technological, and economic well-being of the United States. All of these "lesser" MOs together accounted for a not inconsiderable one-third of the year's reported collection attempts originating in Europe and Eurasia.

The exception to this discussion is the suspicious network activity (SNA) MO. By definition, it involves attempts to work through computers and networks, not human beings directly, and at a distance, not in person. In FY11, industry reports of collection activities categorized as SNA decreased markedly in number from FY10, amounting to a drop of over 70 percent. As a category, SNA went from being the second most common in FY10 at 17 percent to only three percent of the total in FY11. The worrisome possibility is that this change did not occur because industry, DSS, and others in the IC got better at detecting and defeating SNA from Europe and Eurasia, but that the region's cyber collectors, already highly skillful, got even better at concealing their illicit activities.

The MO that Europe and Eurasia collectors were most commonly reported as using in FY11 was the attempted acquisition of technology, accounting for 34 percent of total contacts. Attempted acquisition of technology is defined as expressing interest in purchasing, or actually placing an order for, export-controlled technology.

RFIs comprised 29 percent of FY11 Europe and Eurasia contacts reported by industry. RFIs often target technical specifications of sensitive military systems, but stop short of attempting to purchase an export-controlled item. Receipt of such an RFI could mean that an intelligence service has already obtained a restricted piece of technology and is seeking information on its use.

A possible example occurred in January 2011 when a Europe and Eurasia national contacted a cleared contractor, claimed to possess one of its export-controlled transceivers, and requested the data transfer protocol for use with the module. The transceiver is a component in several military applications, including bombots and other unmanned vehicles. The individual did not reveal how he obtained the transceiver, but it may have been lost or stolen in a combat zone.

Conferences, conventions, and trade shows rose to be the third most used MO in the reporting data for the year. Such venues continued to be used to solicit information and technology in FY11. IC reporting noted that government representatives and civilian journalists from Europe and Eurasia who questioned unmanned aerial system (UAS) industry experts at military expositions and conferences frequently asked questions beyond the scope of their responsibilities and showed an unusual breadth of knowledge.

Together the solicitation or marketing services and the exploitation of relationships MOs accounted for 13 percent of reported Europe and Eurasia collection attempts in FY11. Reporting from cleared contractors suggests that collectors attempt to exploit government cooperation agreements and legitimate business exchanges to collect intelligence. Throughout 2010 and 2011, DSS received several reports that Europe and Eurasia commercial delegations visiting cleared contractors included government IOs.

In their simplest manifestation and deployment, collectors find electronic methods of contact such as unsolicited emails and phone calls to be attractive, as they can be conducted inexpensively, with a low risk of adverse consequences combined with the potential for high gain. Yet the more advanced types of Europe and Eurasia cyber espionage against U.S. cleared contractors essentially represent a current intelligence gap for DSS. In FY11, several cyber attacks against cleared contractor networks, such as those using the Zeus Trojan banking malware, were linked to criminal hacking. Thus, even when contacts are categorized as SNA, incidents cannot necessarily be attributed to foreign intelligence entities.

Analyst Comment: Such cyber espionage may cause malicious activity targeting cleared contractors that is conducted by Europe and Eurasia collectors to be incorrectly attributed to actors in a different country or region. (Confidence Level: Low)

Some Europe and Eurasia countries may attempt insider-enabled network attacks, which prevent the observation of suspicious indicators normally associated with network attacks. Additionally, such attacks may enable the compromise of computer networks that are sufficiently hardened to withstand attacks originating over the Internet, but remain vulnerable to subversion by a malicious employee or contractor, constituting a significant insider threat. (Confidence Level: Low)

TARGETED TECHNOLOGIES

The top four targeted technologies in FY11 industry reports were the same as in FY10: aeronautics systems; LO&S; IS; and electronics. However, they became much more bunched at the top, with the share accounted for by the former top category, IS, cut in half from 26 to 13 percent, leaving aeronautics systems unchanged at 16 percent and tied with LO&S at the top of the list; electronics accounted for ten percent. No other individual technology section accounted for more than five percent of the total.

Aeronautics rose to the top of the list of Europe and Eurasia-targeted technologies at 16 percent of all reports. Some Europe and Eurasia countries that do not have the resources to produce all the weapon systems and technologies they consider vital to their national interest seek out U.S.-developed UASs to support their armed forces

deployed in various spots around the globe. In FY11, there was some focus on long-endurance unmanned aerial vehicles.

LO&S accounted for 16 percent of the reported total. On one occasion, Europe and Eurasia government collectors questioned a cleared contractor employee working at an exhibit booth at the Euronavale Trade Show in Paris about operating frequencies used in tactical missile defense systems.

Last year's top technology category, IS, was FY11's third most targeted sector, accounting for 13 percent of industry reporting. Most of the contacts involved invitations to conferences or foreign visits to cleared contractors specializing in IS; thus, targeting of specific items was difficult to verify. Optical communications technology with civilian and military applications was a specific focus identified in several reports, with one collecting entity withdrawing its request after the cleared contractor insisted on end user information.

Analyst Comment: The consistent collection emphasis on the IS sector probably reflects the priority of Europe and Eurasia militaries to upgrade their communication technologies. (Confidence Level: Moderate)

Radiation-hardened (rad-hard) circuits (see the Special Focus Area section of this publication) for space-based applications have been a consistent target of some Europe and Eurasia collectors for several years. Within the last decade, a company from the region proposed to a cleared contractor a joint venture to create a facility in its country to produce rad-hard circuits, but this did not transpire. Subsequently, Europe and Eurasia entities sought rad-hard circuits from cleared contractors at least 11 times from FY08 to FY11, as reported by industry to DSS. Four of those requests, made to three separate cleared contractors, occurred in FY11. Most of these requests for rad-hard circuits requested between 20 and 42 pieces, although one sought 3,200.

TARGETED TECHNOLOGY

FIGURE 16

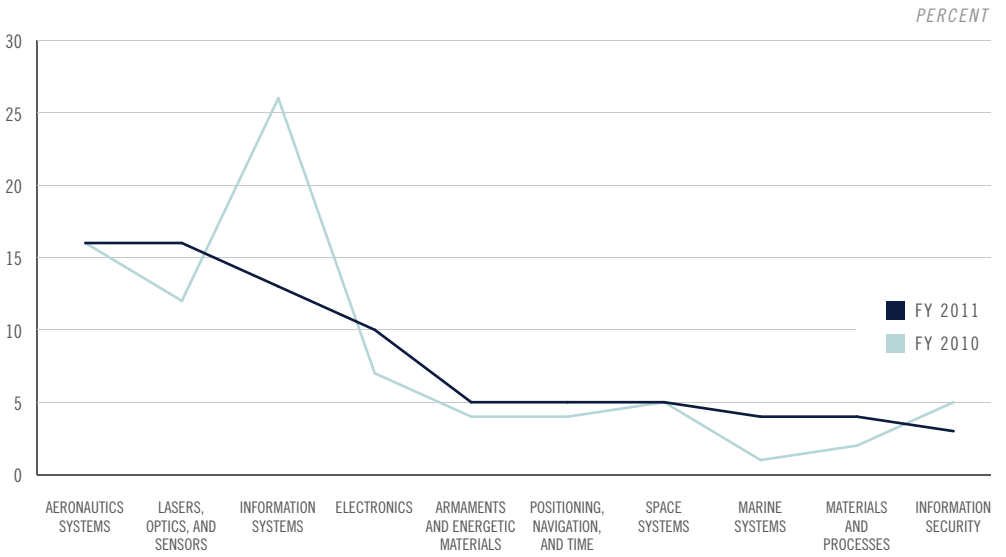


Figure illustrates the top ten most targeted technology categories in FY11 compared with the reporting statistics for the same categories from FY10.

Historical reporting shows that elements within Europe and Eurasia have pursued alternative means to develop or acquire desired technology, including operating facilities to reverse-engineer any Western technology acquired.

Analyst Comment: Those seeking the rad-hard circuits were likely unable to establish an indigenous capability to produce technology that met a desired standard. DSS cannot rule out the possibility that Europe and Eurasia entities are still seeking rad-hard components for reverse-engineering. (Confidence Level: Moderate)

OUTLOOK

DSS assesses that Europe and Eurasia collectors will likely continue to emphasize legitimate commercial exchanges to upgrade their military technology, and those requirements will in turn likely draw upon commercial ties to foreign businesses. Cleared contractors conducting business in Europe and Eurasia will likely be subject to unabated, aggressive collection efforts via all means available. **(Confidence Level: Moderate)**

Several Europe and Eurasia countries view the United States as their foremost economic competitor, and will likely continue to seek information to help them compete politically, economically, and militarily in world affairs. One way in which Europe and Eurasia entities are likely to continue to be a significant threat to U.S. information and technology resident in cleared industry in the coming years is by some companies from the region attempting to purchase U.S. companies. Their likely intent in doing so would be to appropriate U.S. technologies that can then be legally used in Europe and Eurasia exports. **(Confidence Level: Moderate)**

Europe and Eurasia entities' targeting of U.S. information and technology will likely continue to focus on aeronautics systems and IS, with emphasis on UASs and the Joint Tactical Radio System. DSS assesses that additional attention to LO&S will probably continue. Collectors will likely continue to emphasize microelectronics, including the rad-hard variety, due to their importance in bringing militaries in the region into the 21st century. **(Confidence Level: Moderate)**

The U.S. IC will likely face continuing challenges in attempting to attribute cyber attacks against cleared contractors to identifiable Europe and Eurasia entities. Most such SNA will likely appear to support criminal activity, but may occasionally address information falling within the scope of technology requirements set by governments in the region. **(Confidence Level: Moderate)**

CASE STUDY: "WON'T YOU COME INTO MY PARLOR…?"

Between November 2010 and February 2011, a U.S. cleared contractor employee received three email invitations to an international science conference, to be held in Europe and Eurasia. The invitations were sent to the employee's work email address.

IC reporting shows that in 2010, employees from two separate cleared contractors received invitations to the previous conference, held the year before, also in Europe and Eurasia.

Such conferences hosted in Europe and Eurasia may have indirect connections with Europe and Eurasia intelligence services, although the full extent of the relationship is unknown.

Analyst Comment: Scientific conferences present opportunities for foreign intelligence services to spot and assess persons with access to technology intelligence. The successive iterations of this Europe and Eurasia conference may be used to elicit technology information that is responsive to government collection requirements. (Confidence Level: Low)

SOUTH AND CENTRAL ASIA

OVERVIEW

South and Central Asia made the most noteworthy change from fiscal year 2010 (FY10) to FY11—in an unfortunate direction, as far as U.S. cleared contractors are concerned. This region more than doubled year over year in number of reports ascribed to it for attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. In so doing, it increased its share of the world's larger total for FY11 from nine percent to 12 percent.

Increased regional instability and conflicts, counterterrorism efforts, and defense modernization initiatives continue to impact South and Central Asia defense industries, driving efforts to obtain U.S. information and technology. These attempts to maintain and upgrade military capabilities can be accomplished through the purchase of new technologies as well as the upgrading or replacing of older systems. Any sensitive or classified U.S. information and technology acquired could assist greatly with such modernization efforts.

South and Central Asia government entities that experience difficulty in obtaining the licenses and paperwork necessary to purchase dual-use technology are able and willing to exploit their relationships with the U.S. government and commercial entities to circumvent export-restriction laws. South and Central Asia entities still on U.S. export-restriction lists remain a threat to attempt to illicitly acquire U.S. technology.

Commercial companies remained the top South and Central Asia collector category in reported attempts in FY11. The private sector often contacted U.S. cleared contractors in an attempt to win contracts with government agencies in their countries. Intelligence Community (IC) reporting indicates that South and Central Asia intelligence and security services likely work closely with these government agencies on certain matters; however, no evidence suggests that commercial companies have contacted cleared contractors on behalf of or at the urging of intelligence services.

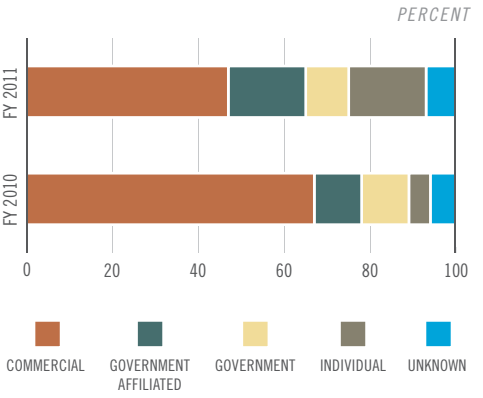
As reflected in FY11 industry reporting on South and Central Asia, the combination of commercial entities using the attempted acquisition of technology and request for information (RFI) methods of operation (MO) accounted for the majority of suspicious contacts. These commercial entities were largely procurement agents who identified military and other government agency end users for the materials sought. In FY11, South and Central Asia commercial companies commonly used direct contact methods, primarily email, to attempt to acquire technology from cleared contractors.

FY11 industry reporting showed that South and Central Asia entities targeted technologies across the Militarily Critical Technologies List (MCTL), most notably in the sections encompassing information systems (IS); lasers, optics, and sensors (LO&S); aeronautics systems; and electronics systems.

COLLECTOR AFFILIATIONS

Given the large overall increase in number of industry reports ascribed to collectors from South and Central Asia, it is not surprising that the number of reports went up in all five affiliation categories from FY10 to FY11. However, the top category in both years, commercial, decreased in share of the total from nearly two-thirds to under one-half. The shares for the government and unknown categories varied by only a percentage point year over year. The significant changes were in the government-affiliated and individual categories, which rose from 11 to 18 percent and from five to 18 percent, respectively, of the more recent year's total, now tying them for a distant second place behind the commercial category's 47 percent.

COLLECTOR AFFILIATIONS
FIGURE 17



Although the percentage share of the year's totals accounted for by commercial entities decreased, the number of reports nonetheless increased by over 60 percent. The majority of the commercial entities making requests for U.S. technology in FY11 were procurement agents acting on behalf of, or in response to requirements from, elements of South and Central Asia governments, including military, security, and intelligence services.

The dominant pattern practiced by governments in South and Central Asia for procuring defense technology consists of state-run organizations issuing tenders to secure military equipment, both systems and subcomponents. Such tenders are often accessible to the public on official government websites and frequently include specifications for the requested technologies. Procurement agents respond to the tenders, attempting to fill the requirements by contacting companies discovered through open-source research that market products matching the tender specifications.

Analyst Comment: The Defense Security Service (DSS) assesses it is very likely that the majority of the suspicious contacts reported by cleared contractors represented efforts to respond to South and Central Asia government tenders and meet government requirements. (Confidence Level: High)

Typically, once a South and Central Asia commercial entity identifies a U.S. company producing technology responsive to the tender requirements, it seeks to contact the company. The commercial agent either attempts to acquire the system outright or requests information on the technology.

Analyst Comment: Queries regarding a technology in question likely constituted attempts to determine whether it could ultimately meet the needs of the South and Central Asia end user; however, DSS cannot rule out that such RFIs represented attempts to obtain sensitive or classified information from the cleared contractor. (Confidence Level: Moderate)

Most South and Central Asia requests for information or technology received by U.S. cleared contractors identified a military service or other government entity as the end user. Several of the commercial collectors that did not identify an end user have ties to the military or are procurement agents with a history of making requests on behalf of the government. Open-source searches provide evidence that in many such cases South and Central Asia companies were referencing tenders put out by specific government agencies, as their requests to U.S. cleared contractors cited specific technologies sought by those tenders.

Analyst Comment: Considering the similarities between the commercial requests and the government tenders, it is likely that South and Central Asia government agencies were the intended end users for the technologies requested in a majority of the cases in the commercial category. (Confidence Level: Moderate)

Some governments within the region are promoting policies to encourage involvement by a wider array of private, commercial companies in defense procurement, including the bidding on government tenders issued by defense agencies.

Analyst Comment: This policy probably contributed to the rise in the number of reported acquisition attempts by South and Central Asia commercial entities. Furthermore, it was also likely responsible for a rise in the overall number of firms and procurement agents that contacted U.S. cleared contractors, as more firms and procurement agents became active in the market. (Confidence Level: Moderate)

Government-affiliated entities followed commercial entities in reported suspicious requests to cleared contractors, constituting 18 percent of the FY11 South and Central Asia total. The number of reports from government-affiliated entities rose by 280 percent over FY10 figures. South and Central Asia collecting entities in this category in FY11 included government-owned companies and government-affiliated technological institutes, other universities, and research organizations.

From such entities, students, researchers, engineers, and others initiated numerous unsolicited contacts to cleared contractors.

They requested jobs, internships, research positions, and other assistance with research; such inquiries often sought information on the pricing or availability of sensitive or classified U.S. technology as well. According to IC reporting, some of the government-affiliated entities in question encourage South and Central Asia students studying in the United States to transfer information and/or technology back to their homelands.

Analyst Comment: Many South and Central Asia students who initiate contacts to cleared contractors likely have a working relationship with defense agencies in their countries, which sometimes fund research and development (R&D) programs at the government-affiliated institutions, then use students and resources from them. (Confidence Level: High)

While the individual category of collector, like government-affiliated, at 18 percent accounted for a considerably smaller share of the total than commercial, the number of reports on individuals soared by over 600 percent since FY10. Entries in the individual category include student requests that DSS counterintelligence analysis connected to independent South and Central Asia universities rather than government-affiliated ones, or cases in which no affiliation with a specific university could be determined. The largest part of these individual requests consisted of résumé submissions to cleared contractors soliciting employment or to U.S. university-affiliated research centers seeking research-related positions.

The small FY11 amount of cyber activity that could be traced to South and Central Asia but no farther is represented in the individual category as well. The remaining individual contacts consisted of RFIs or attempted acquisitions, including requests during which individuals provided no affiliation with a specific company or organization, but their email addresses, mailing addresses, and/or telephone numbers traced back to South and Central Asia. While these requests sought disparate technologies, they tended to mirror requests made by commercial entities.

Analyst Comment: For South and Central Asia collectors in the individual category, DSS could not connect the person to any company. However, there is an even chance that these individuals were independent or new procurement agents responding to government tenders. (Confidence Level: Moderate)

When South and Central Asia government entities themselves contacted cleared contractors, the requests were largely in pursuit of technology systems that are of interest to researchers for space and satellite systems, or consisted of military officers making inquiries about military platforms.

METHODS OF OPERATION

There was a real contrast between FY10 and FY11 in the reported MOs collectors linked to South and Central Asia used in their attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base. Partly this was due to a change in the statistical accounting method used by DSS, which resulted in many contacts that had previously been categorized as RFIs now being labeled attempted acquisitions of technology; the latter category went from no reports in FY10 to ranking first in FY11, with nearly one-third of the total. Mostly this was at the expense of the RFI category, which went from 78 percent of the total in FY10 to 29 percent in FY11.

But the South and Central Asia statistics concerning other MOs experienced change as well. Academic solicitations, which had registered a negligible one percent of the total in FY10, rose to nine percent of the FY11 total, and seeking employment went from three percent to ten percent of the year's total. In comparison, solicitation or

marketing services remained stable within the listing, with only a percentage point increase in share from eight to nine percent.

Attempted acquisition of technology was the most common MO South and Central Asia entities used in FY11, comprising 32 percent of reported collection attempts associated with the region. Generally, South and Central Asia entities sent unsolicited emails to cleared contractors requesting to purchase specific technology, usually in a specific quantity as well. While not all of the unsolicited emails referenced a particular government tender, some cited the exact specifications and quantities listed in such tenders.

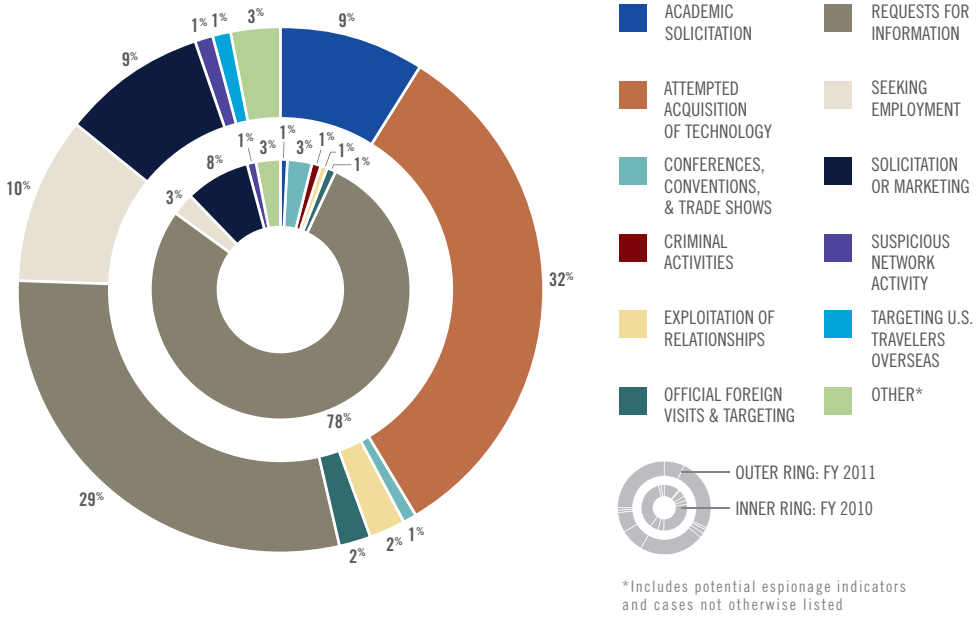
Closely following attempted acquisitions of technology were RFIs, at 29 percent of reported South and Central Asia-originating collection attempts. Commercial entities used unsolicited emails as the primary mechanism to submit purchase requests, ask technical questions, and/or gather information about specific technologies.

Analyst Comment: More South and Central Asia entities are now attempting to develop business relationships with cleared contractors. It is likely that the attempted acquisition of technology MO surpassed reported RFIs in part because of the more amicable relationships between the United States and some South and Central Asia countries, which encourage technology transfer. (Confidence Level: Moderate)

Although the attempted acquisition of technology and RFI categories are separate for the purposes of increasingly discriminating reporting, the means by which these two MOs are employed are very similar. In both methods, an entity contacts a cleared contractor requesting certain sensitive components or platforms, or asking for information such as pricing or technical specifications. The entities

METHODS OF OPERATION

FIGURE 18



*Includes potential espionage indicators and cases not otherwise listed

making these requests mostly appear legitimate; inquiries only occasionally reveal a nefarious or suspicious end user. The difference between the MOs is that in the case of attempted acquisition, the suspicious entity is more likely to be aware that it is not an authorized recipient.

Analyst Comment: Most South and Central Asia procurement agents very likely view RFIs and attempted acquisitions of technology as legitimate and potentially successful means of obtaining sensitive or classified U.S. information and technology. (Confidence Level: Moderate)

FY11 saw the emergence of academic solicitations by South and Central Asia actors, totaling nine percent of reported collection attempts linked to that region in comparison to one percent the year before. Governments within the region are engaged in expanding institutions of higher learning in number and enrollment, to more closely parallel enrollment of students in Western countries. University requirements of an internship for students—a majority of whom seek to fulfill their internship requirement at a U.S. company—contributed to the number of academic solicitations made to cleared contractors.

Analyst Comment: In addition to the creation of additional South and Central Asia universities, better awareness among cleared contractors concerning foreign students likely contributed to the increase in the number of student résumés, job applications, and inquiries reported by cleared industry in FY11. (Confidence Level: Moderate)

While solicitation or marketing was only the fifth most common MO South and Central Asia collectors used in FY11 as reflected in industry reporting, it remains noteworthy. Although it represented eight percent of the reporting last year and nine percent in FY11, due to the overall increase in reporting related to South and Central Asia the number of cases in this category more than doubled year over year. In most suspicious contact incidents reported by cleared industry involving this MO, a South and Central Asia company offered to act as the cleared contractor's agent or distributor in a particular country or the region.

Analyst Comment: While South and Central Asia entities' attempts to form business partnerships may be legitimate, it is likely that they are intended more to promote an additional avenue to access sensitive or classified U.S. information and technology. Were cleared contractors to enter into such agreements, the South and Central Asia entity would likely request an exchange of personnel or even access to controlled U.S. information and technology as a condition of the deal; either situation could result in unauthorized access to sensitive or classified U.S. information and technology. (Confidence Level: Moderate)

TARGETED TECHNOLOGIES

The top of the list of technologies most frequently reported by industry as having been targeted by collectors from South and Central Asia was fairly stable from FY10 to FY11. Just as in FY10, in FY11 the IS and LO&S sections were tied at the top, at 19 percent. Aeronautics, in third place with ten percent, increased only one percentage point from the year before. Last year's fourth-place technology, positioning, navigation, and time, slid to seventh place in the new listing, now at five percent, allowing electronics to move up one spot from last year, with nine percent of the total. Industry reporting shows that South and Central Asia entities continue to seek a wide and diverse range of dual-use technologies from cleared contractors.

The IS technologies South and Central Asia collectors targeted in FY11 included modeling and simulation (M&S) software, used for range-testing of aircraft and missiles. Existing South and Central Asia missile systems may lack radar and testing equipment adequate to track, review, and improve test results

TARGETED TECHNOLOGY
FIGURE 19

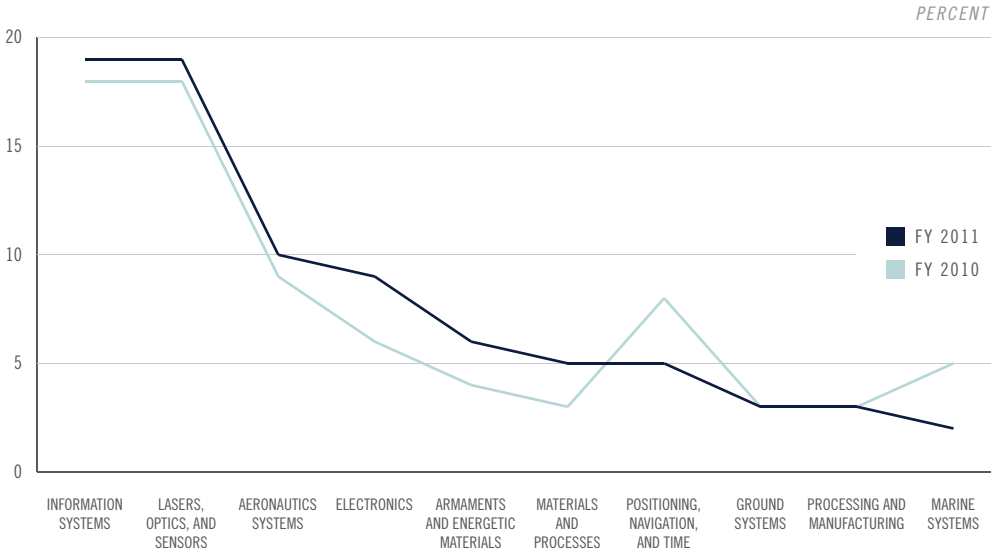


Figure illustrates the top ten most targeted technology categories in FY11 compared with the reporting statistics for the same categories from FY10.

accurately. To achieve a competitive military and economic edge in the region with regard to radar capabilities and products, collectors seek enhanced tracking capability.

Analyst Comment: It is likely that acquisition of more advanced M&S software would improve South and Central Asia entities' radar capabilities, which would likely assist in correcting deficiencies in a multitude of areas, including missiles, surveillance systems, and training programs. (Confidence Level: Moderate)

Additionally, in a large number of cases, South and Central Asia students sent résumés requesting positions in the information technology (IT) field, including programming, software development, and network systems engineering, any of which could facilitate access to cleared contractors' IS-related materials, software, and technologies.

Analyst Comment: While some of the requested positions do not directly involve classified material, they may allow access to proprietary and/or export-controlled information. When students in such positions complete their internships or employment, they possess the potential to either knowingly or unknowingly transfer sensitive information back to their home countries. There is an even chance that relationships opened by such student contacts with U.S. cleared contractors are exploited by the students' home countries. (Confidence Level: Moderate)

Technology areas within the LO&S and electronics systems sections of the MCTL that South and Central Asia entities specifically targeted in FY11 included thermal imaging cameras. South and Central Asia is characterized by security concerns from perceived threats both within and outside the region. Persistent and continuous requests for thermal imaging

systems, considered in the context of IC and open-source reporting, indicate that South and Central Asia actors are probably continuing to build their surveillance technology base for application to border security, and in response to a growing threat of missile deployment along those borders.

Other systems targeted within the LO&S section of the MCTL included fire control radar, airborne warning radar, medium wave infrared cameras, and battlefield surveillance radar (BSR). The volume of requests from South and Central Asia for BSR technology reported by industry, combined with 2010 IC reporting, indicates that some South and Central Asia militaries have a limited BSR capability but are seeking to upgrade it, including to achieve systems networking capability.

Analyst Comment: South and Central Asia nations likely view BSR systems as crucial to protecting their borders. There is an even chance that many South and Central Asia-connected attempts to acquire U.S. BSR systems are a response to similar efforts by their neighbors to improve their own BSR systems. (Confidence Level: Moderate)

To further support goals regarding border security, as well as intelligence, surveillance, and reconnaissance (ISR), weapons mobility/deployment, and the conduct of terrain studies, South and Central Asia companies and agencies targeted unmanned aerial vehicles (UAVs). Entities continued to request not only whole UAV systems but also increased their requests for UAV components, as defense industries and laboratories in the region worked toward self-production of complete UAVs. Some in the region have developed indigenous unmanned aerial systems (UASs), but have experienced difficulties in developing advanced systems.

Analyst Comment: South and Central Asia entities have made multiple attempts to acquire U.S. long-range, ISR-capable UAVs, including those that can be launched from either ship or coastal installations. Their targeting of U.S. UAVs almost certainly reflects an effort to support force modernization plans and upgrades. (Confidence Level: High)

OUTLOOK

DSS assesses that South and Central Asia entities almost certainly perceive an enduring need for foreign, in particular U.S., technology. Ongoing and intensifying conflicts in the region, border issues with neighbors within and outside the region, frictions with the United States, and internal security concerns are likely to motivate South and Central Asia countries. As neighbors and rivals continue efforts to collect and advance upon multiple technology platforms, countries desire to counter with capable technologies of their own. To counter perceived threats, South and Central Asia collectors will almost certainly continue to attempt acquisition of and collection against U.S. information and technology. **(Confidence Level: Moderate)**

Given the perceived imperative to improve military capabilities, there is an even chance that South and Central Asia entities that encounter what they perceive as delays in acquiring desired technology, including dual-use systems, through legitimate avenues will turn to illicit methods. There is an even chance that South and Central Asia agencies' and companies' motivations to protect their own interests will outweigh their inclination to follow U.S. export laws, especially if they risk compromising security within the region, hampering defense industry development, and reducing their own revenue. In order to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base, some South and Central Asia entities will likely attempt to exploit relationships with the United States. **(Confidence Level: Moderate)**

If successful at illicitly acquiring U.S. information and technology from cleared

contractors, some South and Central Asia entities are likely to share such materials with intra- and interregional allies. Such alliance relationships are likely to continue to develop, and the out-of-region parties involved would thereby gain illicit access to U.S. military technology, even that which was legally acquired originally. **(Confidence Level: Moderate)**

There is also an even chance of increased exploitation attempts from South and Central Asia cyber actors. The region's active and growing IT sector produces and employs individuals capable of hacking computer systems. According to industry reporting from FY11, such individuals contacted cleared contractors to establish business relationships with their companies. While no reporting indicates these South and Central Asia IT companies are acting as intelligence collection sources at this time, their capabilities are likely advanced enough for them to be exploited as a collection tool. **(Confidence Level: Moderate)**

The existing and expanding technical institutes that graduate those with such capabilities are likely to produce an increase in student requests to U.S. cleared contractors. Government initiatives will probably enhance R&D partnerships between South and Central Asia training institutes and government agencies, which are then likely to increase their combined outreach to U.S. cleared contractors. **(Confidence Level: Moderate)**

DSS assesses that South and Central Asia collection efforts will probably continue to rely heavily on commercial entities acting as government procurement agents to acquire U.S. technology. These entities will almost certainly continue to use RFIs and attempted acquisitions of technology to obtain sensitive or classified U.S. information and technology for their defense industries. By and large, such requests will very likely continue via email and web card, with occasional in-person contact. While most such approaches will almost certainly be made by legitimate entities, it cannot be discounted that disreputable actors will attempt to obscure the illicit nature of their acquisition attempts amid the increasing volume of reports from commercial entities. **(Confidence Level: High)**

DSS assesses that South and Central Asia entities will very likely continue their collections against U.S. cleared contractors' LO&S systems, software testing materials, infrared and surveillance technologies, and UAS components. Much of this effort will very likely be the result of force modernization requirements and upgrades, but will also likely reflect the perceived need to maintain parity with or even outpace neighbors' capabilities in these areas. **(Confidence Level: Moderate)**

CASE STUDY: GROUND (RADAR) ATTACK

The following is an example of South and Central Asia use of a procurement agent to obtain information regarding a sensitive U.S. technology. This collector has a history of making inquiries on behalf of the military.

In December 2010, a representative of a South and Central Asia company visited the booth of a cleared contractor at the Defence Security and Equipment International conference in London and followed up with an email requesting to market the cleared contractor's ground surveillance radar (GSR) and other technologies to his country.

The individual in question had previously used the same MO at a 2010 Washington, D.C., conference, visiting the booth of the same cleared contractor and following up with an email to inquire about marketing GSR to his country's army. IC reporting indicates that he is a procurement agent for his country's intelligence service and the country's military. Over the last few years, he has attended various defense shows attempting to procure equipment for his country's military.

Analyst Comment: Based on the agent's ties to his government, DSS assesses that he probably conducts his attempts to acquire sensitive or classified information and technology at the behest of his country's military and intelligence establishments. DSS assesses that there is an even chance that his government uses him and his company to leverage the process of legitimate inquiry to obtain information and technologies from U.S. businesses. (Confidence Level: Moderate)

OTHER REGIONS

Entities originating from the Western Hemisphere and Africa accounted for just seven percent of the collection attempts targeting U.S. information and technology reported by cleared industry in fiscal year 2011 (FY11). This was a marginal decrease from previous years in the share of overall reported collection attempts, down from representing eight percent of all attempts in FY10 and ten percent of all attempts in FY09.

DSS attributed a larger number of suspicious reports to entities from both of these regions in FY11 than previously. However, the increase in reports linked to these regions was far lower than the overall increase in reporting from FY10 to FY11, which increased by 75 percent, while reporting attributed to the Western Hemisphere increased by just 49 percent and that from Africa by just six percent.

Commercial entities from both of these regions were the most active at attempting to collect U.S. technologies, as reported by industry. Commercial entities from Africa conducted over half of the collection attempts attributed to this region, while commercial entities accounted for 35 percent of the attempts originating from the Western Hemisphere. Government entities were the second most common affiliation for entities from Africa, accounting for over a fifth of all reported attempts from this region. In contrast, individual was the second most common affiliation for entities from the Western Hemisphere, tallying one-third of all reported collection attempts linked to it.

Entities from both of these regions relied heavily on the request for information followed by attempted acquisition of technology as their primary methods of operation.

Based on industry reporting in FY11, entities from the Western Hemisphere most actively targeted information systems (IS), aeronautics systems, electronics technology, and lasers, optics, and sensors (LO&S), in that order. These four categories accounted for 40 percent of the collection attempts attributed to the region. Similarly, entities from Africa favored information pertaining to aeronautics systems, IS, LO&S, and armaments and energetic materials technology, in that order. Collection attempts targeting those four categories accounted for over two-thirds of those attributed to Africa.

Analyst Comment: The number of attempts to target U.S. technologies originating from these two regions will likely continue to increase, albeit at a slower pace than those from the other four regions. Countries in the Western Hemisphere and Africa largely possess smaller armed forces and less developed defense industrial bases than those in East Asia and the Pacific, the Near East, and Europe and Eurasia. (Confidence Level: Moderate)

CONCLUSION

Technologies resident in U.S. cleared industry remain highly sought after. Foreign intelligence entities (FIEs) continue to expand their collection networks and activities. These networks are growing like a malignant vine. This ongoing theft—FIEs' pilfering of U.S. technologies from cleared industry—could reduce or even end advantages in military capabilities the United States possesses over potential adversaries, thereby adversely affecting U.S. battlefield dominance. It also could strangle U.S economic growth, vitiating the nation's economic health.

The overall number of reports submitted by cleared industry to the Defense Security Service (DSS) in FY11 increased by nearly 65 percent over FY10, and the number that actually became suspicious contact reports (SCRs) increased by 75 percent, likely due in large part to increased awareness and reporting by industry.

Many of the attributes of the entities targeting U.S. technologies remained constant from FY10 through FY11. The order of the regions linked to the most prolific collectors of U.S. information and technology remained unchanged from FY10; commercial remained the most common collector affiliation; and the top four most targeted technology categories remained the same. A modest change in the favored method of operation (MO) occurred, with attempted acquisition of technology becoming the most common MO. This largely reflected a change in terminology, in that DSS would have classified many incidents of attempted acquisition of technology as a request for information (RFI) in previous years. In FY11, RFI became the second most common MO.

Constancy of the order of the regions represents the most enduring trend. Over the past five years, the only change in the order occurred in FY07 and FY09, when South and Central Asia was the third most prolific and Europe and Eurasia the fourth; the other three years, Europe and Eurasia has been the third most prolific. East Asia and the Pacific and the Near East have remained the first and second most prolific collector regions throughout the five years, responsible for at least 56 percent of all reported collection attempts each year.

As previously noted, entities linked to East Asia and the Pacific remained the preeminent attempted collectors of U.S. technology. Over the past five years, entities from this region accounted for 42 percent of all collection attempts reported to DSS. Entities from the Near East consistently represented the second most active collectors, but accounted for just slightly over 18 percent of all reporting.

Analyst comment: East Asia and the Pacific features many areas with a permissive environment in which collectors can operate. In some areas, collection efforts, even those by commercial and individual entities, have government sanction, or at least tacit approval; in some cases, collection is conducted at government direction. In other areas, lax export controls provide collectors a permissive environment from which to acquire technology and subsequently forward

it to entities in other areas of East Asia and the Pacific or beyond to other regions. (Confidence Level: Moderate)

In FY11, foreign entities identified as commercial made that affiliation the most common one in industry reporting for collectors targeting U.S. information and technology. Commercial entities have constituted the most common affiliation in each of the past five years, accounting for over 36 percent of all the reported collection attempts during that period. In FY11, commercial entities were the most common affiliation in five of the six regions, the only exception being government-affiliated entities in the Near East region.

In FY11, the individual affiliation accounted for the second most reported attempts to collect U.S. technology, as reported by industry. This was a significant shift from previous years. Over the five-year period FY07 through FY11, the individual affiliation accounted for just over 13 percent of all collection attempts, the fifth most common. From FY07 through FY09, entities identified as individuals accounted for no more than nine percent of the attempts to collect U.S technologies, and was consistently the fifth most common affiliation. In FY10, the individual affiliation was the fourth most common for attempted collectors and accounted for 12 percent of the collection attempts. In FY11, the number of collection attempts attributed to individuals increased by more than 160 percent over the total from FY10, and accounted for 18 percent of the total collection attempts. This may be related to the increase in academic solicitation.

The third and fourth most common affiliations, government-affiliated and government, both significantly increased in number of reported attempts to target cleared industry. Government-affiliated experienced a 100 percent increase and reported attempts conducted by government entities increased by 165 percent in FY11 over FY10. Much of the increase in attempts attributed to government reflects better reporting and attribution, which reduced the number of attempts credited to unknown entities. Over the past five years, attempts by unknown entities accounted for over 17 percent of all reported collection attempts, and was the second most common affiliation over that period. However, in FY11, unknown was the fifth most common affiliation, accounting for 14 percent of the collection attempts.

Consistently throughout the past five years, the most frequently applied MOs for collectors have been to directly request information or attempt to acquire technology. Attempted acquisition of technology and request for information (RFI) were the two most common MOs. Together in FY11 they accounted for 43 percent of reported collection attempts. A redefinition of attempted acquisitions led to DSS attributing many cases in FY11 to that category that would have been considered RFIs in previous years. Thus, reported efforts via attempted acquisition of technology jumped from less than one percent in FY10 to 23 percent in FY11. Consequently, RFIs plummeted over the same period from representing 48 percent of reported attempted collections to 20

percent. Collectively, these MOs represent direct overt contact with cleared industry in an attempt to receive information or acquire technology by asking for it.

Suspicious network activity (SNA) continued to be a growing phenomenon in FY11. The number of reported SNA collection attempts increased by 36 percent in FY11 over FY10. Better detection and reporting by industry has contributed greatly to improved identification of SNA and the ability to attribute it to particular regions. In FY11, SNA was the most prevalent collection MO for entities originating from East Asia and the Pacific. This is the only region identified as leveraging SNA so heavily; SNA figured no more prominently than fifth in any other region. However, in reports for which the region of origin is unknown, SNA was again the most prominent MO. Due to the nature of SNA, it is difficult to attribute some collection attempts to an entity or even to a region of origin.

The most sought after technologies in FY11 remained largely the same. The top four most targeted technology categories—information systems (IS); lasers, optics, and sensors (LO&S); aeronautics systems; and electronics—remained unchanged. Armaments and energetic materials replaced marine systems as the fifth most targeted category of the Militarily Critical Technologies List (MCTL). The top five in FY11 were the most commonly targeted technologies for the last five years.

A trend for the past three years is an apparent broadening of the targeting of technology: the focus of collectors seems to be diffusing. In FY07, the top five targeted technologies accounted for 67 percent of all reported collection attempts. In FY09, these technologies continued to represent over 66 percent of reported collection attempts. However, in FY10, the top five targeted technology categories accounted for 57 percent, and this dropped further in FY11, with the top five categories accounting for just over 51 percent of reported collection attempts.

This apparent broadening of interest in technology has made space systems, processing and manufacturing, and directed energy systems more common targets for collectors. In FY09, collectors targeted space systems in fewer than two percent of reported collection attempts, whereas in FY11, collectors targeted space systems in almost five percent of reported attempts. In the same period, collection attempts aimed at directed energy systems went from one-sixth of one percent to over two percent of all reported collection attempts.

Analyst Comment: If this diffusion of interest continues in FY12 and beyond, it may signify that some competitor countries now consider themselves peers to the United States in those technologies that formerly were the most highly sought after, such as IS technology. Such countries may further turn the focus of their collection efforts to other technology categories, such as space systems, in which the United States retains an advantage. (Confidence Level: Low)

OUTLOOK

Access to and application of the latest technologies is a vital component of being victorious on the battlefield and competitive economically. The technologies resident in U.S. cleared industry represent the latest and greatest advances. But this technological advantage is under perpetual attack from foreign intelligence entities (FIEs) representing political adversaries and economic competitors. This onslaught of espionage targeting U.S. technologies is constant and unwavering. In fact, this year's reporting suggests this persistent attack on U.S. technologies continues to grow.

A technological advantage can be devastating on the battlefield, providing one side with a decisive victory while it suffers limited losses. In 1991, Coalition forces, led by the United States and armed with the most advanced weapons systems, crushed an Iraqi army that had established itself in defensive positions in Kuwait and southern Iraq. The Iraqi army deployed aging equipment, most of which was a generation older than that wielded by the United States and its NATO allies in the coalition. Coalition soldiers, sailors, airmen, Marines, and Coast Guardsmen used stealth technology, precision weapons systems, and superior battlefield surveillance technology to their advantage, helping to lead to a decisive victory.

Conversely, conflict between opponents sharing technologic parity can lead to bloody, costly, and enervating conflagrations. On July 1, 1916, to relieve the pressure on the French army fighting near Verdun, the British army initiated an offensive against German lines near the Somme River. During the week prior to the offensive, the British fired over 1.7 million artillery rounds against the German lines. On the first day of the battle, the British advanced with over 100,000 men—and suffered an estimated 60,000 casualties, including 20,000 deaths. The Battle of the Somme would last until November of 1916 and cost the British 420,000, the French 200,000, and the Germans 500,000 casualties.[4] The Battle of the Somme featured opposing forces largely armed with the same generation of weaponry. It also demonstrated that the offensive tactics of the day could not match the modern firepower wielded by the defense.

Advances in technology are equally important to the economic health of a country. The fortunes of a country can hinge upon an advantage in industry. In 1789, Samuel Slater (1768-1835) emigrated from England to a young and newly independent United States. Prior to leaving England, while working in the textile industry, he had memorized the design and workings of the water mill designed by Richard Arkwright. At that time, England strictly restricted the export of textile machinery or technology. Slater claimed to be a farmer when leaving England, fearing he would not be allowed to leave if authorities knew his true profession. After arriving in the United States, Slater was instrumental in establishing the first water-powered cotton-spinning mill in the country.[5] This violation of export controls, along with Slater's ability to replicate the mill machinery, greatly accelerated the industrial revolution in America. Furthermore, this story demonstrates that it can often be as

important to obtain information and design details of a given technology as the actual piece of equipment.

The battlefield and economic advantage enjoyed by the United States is precarious, and the loss of the advantage on the battlefield would likely have disastrous results for U.S. forces. Concurrently, the continuing invasive collection of U.S. technologies would likely further erode the U.S. technological advantage and cause severe repercussions to the U.S. economy. **(Confidence Level: Moderate)**

Those who attempt to collect U.S. technologies will almost certainly continue to target a wide variety of them, spanning the entire spectrum delineated in the Militarily Critical Technology List (MCTL). Collectors will very likely target, to some extent, technologies in all 20 MCTL sections, in addition to sensitive and classified information held in cleared industry. **(Confidence Level: High)**

Collectors will likely continue to focus greater attention on particular technology sections of the MCTL. Overall, information systems (IS); lasers, optics, and sensors (LO&S); aeronautics systems; and electronics technology will very likely experience the most targeting attempts from foreign entities. **(Confidence Level: High)**

IS technology will almost certainly remain the most sought after category of technology by foreign collectors. The category encompasses a wide range of enabling technologies that can provide military and commercial advantage. Collectors will likely continue to target command, control, communications, computers, intelligence, surveillance, and reconnaissance technologies; modeling and simulation software; and advanced radio technologies. **(Confidence Level: High)**

LO&S technology has held its position as the second most sought after category for the last two years, and will very likely remain a highly targeted MCTL sector. In fiscal year 2009 (FY09), the Defense Security Service treated LO&S as two separate categories, which, if combined, would have been the most targeted technology category. **(Confidence Level: Moderate)**

While IS, LO&S, and aeronautics systems technology will likely remain the most targeted, FIEs will probably increase their targeting of information and technology relating to space systems technology as well as technologies in other MCTL categories with application to the space industry, including radiation-hardened integrated circuits. **(Confidence Level: Moderate)**

Although the methods of operation (MOs) used by collectors will very likely continue to evolve, it is almost certain that attempted acquisition of technology and request for information will continue to be the most prominent MOs. **(Confidence Level: High)**

Cyber-based collection, characterized as suspicious network activity (SNA), will almost certainly continue to increase as adversaries apply new malicious programs to target the vulnerabilities inherent in systems connected to the Internet. **(Confidence Level: High)**

Academic solicitation will likely remain a common MO for entities originating in East Asia and the Pacific and the Near East. **(Confidence Level: Moderate)**

In FY11 reporting, commercial entities were the most common attempted collectors of U.S. technologies in all but one of the six regions. It is very likely that commercial will continue to be the most common collector affiliation overall in reporting data. Some companies seek U.S. sensitive and classified information and technology to develop and sell their own products for profit. But commercial entities can also provide a layer of separation between the collector and the foreign government. This affords the foreign government the ability to deny involvement in the targeting of U.S. information and technology. In addition, collectors likely employ commercial entities in third countries to target U.S. technology in order to hide the identity of the intended end user and circumvent export controls. **(Confidence Level: Moderate)**

Outside the continued predominance of commercial entities as collectors, the number of government entities identified as collecting will likely increase with improved reporting of SNA by industry. Government entities identified as targeting U.S. technology, especially via SNA, will likely continue to most frequently originate in East Asia and the Pacific. **(Confidence Level: Moderate)**

In the other regions, government-affiliated entities such as academic and research institutions or individuals will probably be the next most common type of entities targeting U.S. technologies, after commercial. **(Confidence Level: Moderate)**

Entities from East Asia and the Pacific will almost certainly remain the most prolific in collection attempts reported by cleared industry. This region features contentious boundaries and encompasses economic rivals of the United States. The perceived need within this region for modern militaries combined with growing economies will very likely fuel the continued targeting of U.S. technologies as an efficient and effective method of abbreviating research and development of new and emerging technologies. **(Confidence Level: High)**

The Near East will probably continue to account for the second most reported collection attempts targeting cleared industry. Adversarial forces in the region seek the latest in technology to enhance their security, to re-package and re-sell for commercial gain, and to circumvent international sanctions. **(Confidence Level: Moderate)**

Persistent and pervasive foreign collection attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base will almost certainly continue unabated in the future. FIE MOs will likely evolve and the specific technologies targeted will probably change, but the constancy and aggressiveness of the campaign of collection attempts will almost certainly not subside. **(Confidence Level: High)**

EXPLANATION OF ABBREVIATIONS AND ACRONYMS

ALL ARE U.S. UNLESS OTHERWISE INDICATED

OMITTED: FOREIGN ACRONYMS THAT APPEAR IN ONLY ONE PLACE

BSR	battlefield surveillance radar
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CI	counterintelligence
CPI	critical program information
CV	curriculum vitae
DoD	Department of Defense
DRAM	dynamic random-access memory
DSS	Defense Security Service
ERC	End-User Review Committee
FAVA-RE	failure and vulnerability analysis and reverse-engineering
FIE	foreign intelligence entity
FY	fiscal year
GSR	ground surveillance radar
IC	Intelligence Community
IO	intelligence officer
IS	information systems
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
LO&S	lasers, optics, and sensors
MCTL	Militarily Critical Technologies List
MO	method of operation
M&S	modeling and simulation
NISPOM	National Industrial Security Program Operating Manual
PROM	programmable read-only memory
RAD-HARD	radiation-hardened
R&D	research and development
RFI	request for information
SCR	suspicious contact report
SEE	single-event effect
SNA	suspicious network activity
SRAM	static random-access memory
TAA	trade assistance agreement
UAS	unmanned aerial system
UAV	unmanned aerial vehicle

AFRICA

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

EAST ASIA AND THE PACIFIC

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

EUROPE AND EURASIA

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

NEAR EAST

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

SOUTH AND CENTRAL ASIA

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

WESTERN HEMISPHERE

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

REFERENCES

[1] Source redacted; Available upon request from DSS

[2] BBN Technologies; Internet Security Glossary, May 2000; Accessed on June 6, 2012; tools.ietf.org/html/rfc2828

[3] U.S. Attorney's Office, Eastern District of Virginia; September 20, 2011; press release; Chinese Nationals Sentenced to 24 Months for Illegally Attempting to Export Radiation-Hardened Microchips to PRC; http://www.justice.gov/usao/vae/news/2011/09/20110930chinese.nr.html; News; Unclassified

[4] Open source website; History Learning Site; Battle of Somme; http://historylearningsite.co.uk/somme.htm; Background; UNCLASSIFIED

[5] Open source website; Public Broadcasting Service; Who Made America? – Samuel Slater; http://www.pbs.org/wgbh/theymadeamerica/whomade/slater_hi.html; Background; UNCLASSIFIED

DSS MISSION

DSS supports national security and the warfighter, secures the nation's technological base, and oversees the protection of sensitive and classified information and technology in the hands of industry.

We accomplish this mission by: clearing industrial facilities, personnel, and associated information systems; collecting, analyzing, and providing threat information to industry and government partners; managing foreign ownership control and influence in cleared industry; providing advice and oversight to industry; delivering security education and training; and, providing information technology services that support the industrial security mission of the Department of Defense and its partner agencies.

THIS PRODUCT WAS COORDINATED WITH: ACIC, AFOSI, DIA, & NGA

Produced by the Defense Security Service
Counterintelligence Directorate
www.DSS.mil


DEFENSE SECURITY SERVICE
UNITED STATES OF AMERICA

Administration Strategy on Mitigating the Theft of U.S. Trade Secrets