Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2004

This report was prepared by the Office of the National Counterintelligence Executive (ONCIX). Comments and queries are welcome and may be directed to the National Counterintelligence Officer for Economics, 703-682-4479, STU-III. ONCIX may also be reached at www.ncix.gov.

NCIX 2005-10006
April 2005

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2004

Scope Note

This is the tenth annual report reviewing the threat to the United States from foreign economic collection and industrial espionage. The report seeks to characterize and assess efforts by foreign entities—government and private—to unlawfully target or acquire critical US technologies, trade secrets, and sensitive financial or proprietary economic information. The paper focuses on technologies, the loss of which could undermine US military capability, impede the ability of US firms to compete in the world marketplace, or have an adverse effect on the US economy, thereby weakening national security and eroding the current US technological lead.

The report is being submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809 (b), Public Law 103-359, which requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. It updates the ninth annual report published in February 2004 and includes data for the fiscal year 2004, including the period 1 October 2003 through 30 September 2004.

The contents of this report include the following:

- The types of foreign entities believed to be conducting industrial espionage.
- The kinds of information and technology targeted.
- The methods used by foreign actors to acquire that technology.

This report deals with the acquisition of sensitive US technology—either classified or proprietary—by foreign entities, both government and private. The acquisitions take a variety of forms, including:

- Economic Espionage, which is narrowly defined by Section 1831 of the Economic Espionage Act of 1996 (EAA) to be the theft of trade secrets[1] in which the perpetrator acts intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent. Proving links between foreign governments and entities caught stealing US goods is often impossible, even where such links may exist.

[1] A trade secret is defined as sensitive information that has independent economic value and that the owner has taken reasonable measures to protect. It encompasses all types of financial, business, scientific, technical, economic, or engineering information. It includes patterns, plans, formulas, designs, prototypes, techniques, processes, programs, and codes, whether tangible or intangible and regardless of how the information is stored.

- Industrial espionage or trade secret theft that cannot be linked to a foreign government agent and where the acquisition has been made for the intended economic benefit of someone other than the owner of the trade secret. These violations are covered under Section 1832 of the EAA.

- Violations of export control regulations include the foreign acquisition of restricted US dual-use technologies—having both military and civil applications—by countries or persons that might apply such items to uses inimical to US interests. These include goods that might be related to the proliferation of weapons of mass destruction and their delivery means and those that could bolster the military and terrorism support capability of certain countries. Export Administration Regulations (EAR) issued by the United States Department of Commerce, Bureau of Industry and Security (BIS), cover these violations.

- Illegal exports of US arms and implements of war (including cryptography) and defense technology to proscribed countries that could misuse or cause illegal proliferation of those items. These shipments are prohibited under the International Trade in Arms Regulations (ITAR), which are administered by State Department's Office of Defense Trade Controls.

The paper highlights foreign efforts to target sensitive US technologies even when those efforts are legal. For example, it is not illegal for foreign entities to request classified or controlled information or technology, even though the actual export of that technology would violate US laws. The fact that such technologies are being targeted, however, is considered important information for this report. This paper does not cover violations of US copyright laws, such as the illegal plagiarism of videos, compact disks, or other literary or artistic works.

This assessment is a product of a cooperative effort across the Counterintelligence (CI) Community. It was compiled by the Office of the National Counterintelligence Executive (ONCIX) based on input from a broad cross-section of US Government entities. In particular, databases compiled by the Defense Security Service (DSS), the Air Force Office of Special Investigations (AFOSI), the Army Counterintelligence Center (ACIC), and the Army Case Control Office (ACCO) were instrumental in providing much of the detail for this assessment. The Federal Bureau of Investigation (FBI)—the lead investigative agency for enforcing economic espionage statutes—provided significant analytical and investigative information as did the Department of Defense's (DoD's) Counterintelligence Field Activity (CIFA) and the National Geospatial-Intelligence Agency (NGA).

A host of other organizations within the CI Community also made major contributions to and/or have coordinated on this report, including:

- Bureau of Immigration and Customs Enforcement (ICE)
- Central Intelligence Agency (CIA), including the Counterintelligence Center (CIC), the Foreign Broadcast Information Service (FBIS), the Information Operations Center (IOC), and several geographic offices
- Defense Intelligence Agency (DIA)
- Defense Threat Reduction Agency (DTRA)
- Defense Technology Security Administration (DTSA)
- Department of Energy (DOE)
- Department of Justice (DOJ)
- Department of State, including the Bureau of Intelligence and Research (State/INR) and the Bureau of Diplomatic Security (State/DS)
- National Aeronautics and Space Administration (NASA)
- National Reconnaissance Office (NRO)
- National Security Agency (NSA)
- Naval Criminal Investigative Service (NCIS)

Contents

	Page
Scope Note	iii
Key Findings	ix
The Threat to US Technologies	1
The Key Collectors	3
The Tools and Techniques of the Trade	4
All Technologies at Risk	9
The Road Ahead	11
CI Community Efforts to Counter the Problem	12

Appendices

A: Foreign Countries Experiencing Technology Losses	15
B: Glossary of Terms	17

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2004

Key Findings

Foreign individuals from both the private and public sectors in almost 100 countries attempted to acquire sensitive US technologies in fiscal year 2004 (FY2004), about the same number as FY2003. The US Counterintelligence (CI) Community judges that the technology lost as a result of these efforts has imposed a significant, but difficult to quantify, cost on the United States. Foreign access to sensitive dual-use and military technology has eroded the US military advantage, degraded the US Intelligence Community's ability to provide information to policymakers and undercut US industry.

Several factors, which have contributed to US economic and technological success, have at the same time facilitated foreign entities' technology acquisition efforts. For example:

- The openness of the United States has provided foreign entities easy access to sophisticated technologies.
- New electronic devices have vastly simplified the illegal retrieval, storage, and transportation of massive amounts of information, including trade secrets and proprietary data.
- Globalization has mixed foreign and US companies in ways that have made it difficult to protect the technologies these firms develop or acquire, particularly when that technology is required for overseas operations.
- Sophisticated information systems that create, store, process, and transmit sensitive information have become increasingly vulnerable to cyber attack.

The most serious threat to US technologies in FY2004 came, as it has in previous years, from entities in a small number of countries. These countries perennially top the CI Community's list of most aggressive collectors. The Community is uncertain about exactly how much of the FY2004 collection effort was directed by foreign governments and how much was carried out by private businessmen, academics, or scientists for purely commercial or scientific needs. Anecdotal evidence and incomplete statistical information indicate that most trade secret and technology theft took place without direct intervention by state actors, though most foreign governments involved have not discouraged such theft and themselves often benefited from the transfers. It is clear, however, that some foreign countries, including the major players, also continued to employ state actors—

including their intelligence services—as well as commercial enterprises, particularly when seeking the most sensitive and difficult to acquire technologies.

Most of the foreign entities attempting to acquire US technology last year employed tools and techniques that were easy to use, inexpensive, low risk, and sometimes legal. In a majority of cases, foreign collectors simply asked—via e-mail, phone call, FAX, letter, or in person—for the information. Other techniques foreign entities used to gain access to sensitive technology, proprietary information, and trade secrets included:

- Offering services or technology to US firms with access to sensitive items.

- Exploiting visits to US businesses, military bases, national laboratories, and private defense suppliers.

- Targeting US technology and economic information at conventions, expositions, and trade shows.

- Using cyber tools to extract information.

Virtually all kinds of US trade secrets—military and civilian—were collected against during the past fiscal year. The CI Community pays closest attention to technologies with direct military application and to those on the Defense Department's militarily critical technologies list, many of which are dual-use, with both military and commercial applications. In fact, most of the foreign illicit technology transfer efforts that were tracked by the Community in FY2004 involved dual-use items. **Information systems**—the foundation of almost all modern civilian and military production processes—continued to top the list of targeted technologies. There was also significant foreign interest in **sensors**, which provide the eyes and ears of many military **systems**; aeronautics, because of the demonstrated advantage of airpower in recent international conflicts; **electronics**, which are either contained or used in the production of virtually every weapons system in the US arsenal; and **armaments & energetic materials**, the technologies required to develop and produce conventional munitions and weapons systems of superior operational capability.

Tracking the foreign targeting of purely civilian technologies is difficult. US firms have sometimes been reluctant to raise alarms about possible technology theft out of concern for the potential impact on investor and consumer confidence and stock prices. Nevertheless, recent legal cases alleging technology theft provided samples of the items targeted, which included: semiconductor production processes; computer microprocessors; software; proprietary information; and chemical formulas.

The CI Community expects no decline in foreign demand for sensitive US technologies over the next few years. The United States remains the source of much of the world's most advanced technology, and, in many industries, foreign entities depend on that innovation to improve their competitiveness. At the same time, the task of slowing the illicit outflow of technology will only become more difficult. Globalization, while benefiting the United States economically, is making it challenging to isolate trade secrets from foreign managers and employees. Increasingly, US firms are conducting research and development in centers located outside US borders, where providing physical security will be difficult and where legal protection of technology, trade secrets, and innovation is weak or nonexistent. At the same time, however, US businesses prefer to operate in an environment where their trade secrets are protected, which may gradually pressure foreign governments to strengthen legal safeguards.

We expect little change in the countries posing the most serious threats to US technology over the next few years. What may change, however, is that foreign collectors may increasingly conduct acquisition efforts from international trading centers or from countries that are close US allies and that face few US trade restrictions. Until such host countries begin cracking down on activities, there is little incentive for middlemen to relocate their operations.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2004

The Threat to US Technologies

> *"American innovation and discoveries are the foundation of our technological strength worldwide."*
>
> *Jon Dudas, Under Secretary of Commerce for Intellectual Property*

Sensitive US technologies—those that both underpin the US economy and contribute to US military prowess—remained prime targets for economic espionage, trade secret theft, and illegal export in fiscal year 2004 (FY2004). Certain foreign companies, scientists, academics, government entities, and others see the acquisition of US technology as key to overcoming US economic and military superiority. The continued ability of foreign entities to acquire state-of-the-art US technology at little or no expense has undermined US national security by enabling foreign firms to push aside US businesses in the marketplace and by eroding the US military lead.

The openness of the United States, while contributing greatly to the country's economic prowess, has, at the same time, simplified for foreign entities the task of gaining access to sensitive technologies.[2] For example:

- US firms, universities, national laboratories, and even sensitive government facilities employ the services of foreign workers.[3] A small number of these employees come with both the skills and the intent to illegally acquire US technology for transfer to their home countries. Others discover, while resident in the United States, that the trade secrets and proprietary information that they have access to can easily be converted into profits when transferred to their home countries.

- While conferences, trade shows, and exchanges provide useful opportunities for US scholars and scientists to legally share important findings and information with foreign experts, these venues also provide opportunities for the illegal transfer of US technological secrets.

New electronic devices have vastly simplified the illegal retrieval, storage, and transportation of massive amounts of information, including trade secrets and proprietary data. Compact storage devices the size of a finger and cell phones with digital photographic capability are some of the latest weapons in technology transfer.

Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but, instead, can work within their own borders. There, US firms have difficulty securing their secrets and have few legal protections once proprietary information has been lost. Globalization is forcing US companies toward a more diversified business model that includes foreign outsourcing and external partnerships. Sensitive blueprints, formulas, and computer codes are being transferred abroad to enable foreign firms to supply specially tailored inputs to high-tech products that are manufactured in the United States. These arrangements, while making US firms more competitive by providing a source of inexpensive inputs, at the same time make sensitive US technologies more vulnerable.

[2] In this report, 'sensitive technology' is defined as technology that is either classified or is protected. Protection can take the form of US Government export controls, or it can be measures taken by the private sector to prevent the loss of the technology.

[3] US universities continue to be major attractions for foreign researchers. A recent study by China's Jiao Tong University placed eight of the world's top-10 universities and 17 of the top-20 in the United States.

Conducting due diligence on foreign partners is difficult, but the problem becomes geometrically more complicated when the foreign partners themselves outsource to other firms. According to a private sector study, less than one-third of US companies that are involved in outsourcing conduct regular assessments of their information technology (IT) providers to monitor compliance with information security policies; "they simply rely on trust." These trends not only leave US firms more exposed to a direct outflow of technology but also make it difficult to guarantee that the foreign-provided inputs—particularly IT hardware and software—are free from Trojan horses or back doors that could be used later to extract sensitive technology.

US businessmen traveling abroad are another valuable source of information. Foreign governments and businesses continue to acquire sensitive US proprietary information from all types of electronic storage devices, including laptop computers, personal digital assistants (PDAs), and cell phones carried by US businessmen traveling abroad. A recent US private sector study indicated that two-thirds of PDAs are used to carry client details and corporate information but without adequate protection. Foreign businesses and security services gain access to such information by using clandestine entry to hotels and business establishments or by electronically downloading information during routine security inspections at airports or other ports of entry. In addition, technology weaknesses in some PDAs make it easy for foreign entities to extract information without directly accessing the storage devices.

Global connectivity via the Internet adds to US vulnerability. A variety of evidence suggests that foreign interests continue looking to cyber tools as a means to illegally acquire trade secrets. The number of information security incidents reported to the US Computer Security Readiness Team is an indicator of the rapid rate at which cyber activity has grown in recent years. The number of such incidents rose from about 500,000 events in 2002 to 1.4 million in 2003 and then to 56 million events in the first six months of 2004, according to press reports.[4]

Detection of such intrusions is difficult but, even when detected, a recent private US survey indicated that more than half of the impacted firms do not report the breach for fear of reducing shareholder value. As a result, no one is certain how much technology and sensitive proprietary information are lost annually to cyber theft. In addition, the Internet has given foreign interests an easy, inexpensive, and safe way to spot, assess, and target US firms and individuals who may be willing to ignore or short-circuit export restrictions on sensitive US technologies.

Estimating total losses to the United States resulting from the illegal foreign acquisition of US technologies and trade secrets is extremely challenging, and the CI Community knows of no such recent estimate.[5] One measure of the extent of the problem, however, is the number of prosecutions for the illegal export of US technology. During FY2004, the US Department of Immigrations and Customs Enforcement (ICE) conducted more than 2,500 export investigations involving violations of the Arms Export Control Act, International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), Inter-

[4] The numbers may overstate the rate of increase of cyber incidents. Increased focus on cyber issues, better collection methods, and improved reporting may also have contributed to the sharp rise in incidents.

[5] Any such estimate would have to make fair market value estimates of the technologies lost by firms and the value of replacement technologies necessary to remain competitive. The figure would also have to consider factors such as lost sales as well as marketing and shipping costs. One of the challenges that makes calculating the cost of industrial espionage particularly difficult is that the technology losses often are not readily apparent. The only indication a US company may have that its research and development plans or its marketing strategies have been stolen is a shrinking or even a more slowly growing market share as foreign and domestic firms take advantage of price and product information to steal customers. Likewise for national security secrets, often the only evidence of a loss of a key military technology is the emergence of a new or more sophisticated weapon or countermeasure in a foreign arsenal years later.

national Emergency Economic Powers Act, and the Trading With the Enemy Act. These investigations resulted in 146 arrests, 97 criminal indictments, and 79 criminal convictions.

In less tangible terms, the CI Community believes the long-term impact of the technology losses on US national security includes the following:

- The loss of sensitive dual-use and military items has undercut the US military.
- The US Intelligence Community's ability to provide information to policymakers has been weakened.
- Even the loss of less sensitive proprietary material, such as marketing and research and development (R&D) plans, has hurt US industry, weakening our comparative economic advantage and thereby degrading security.

The Key Collectors

Individuals from both the private and public sectors in almost 100 countries attempted to illegally acquire US technologies in FY2004, roughly the same number of countries as last year, according to data collected by various members of the CI Community. Most of the countries from which the collectors originated are small players and do not compete with the United States in the international marketplace or on the global security stage. Individuals from these countries were involved in one or two incidents during the year.

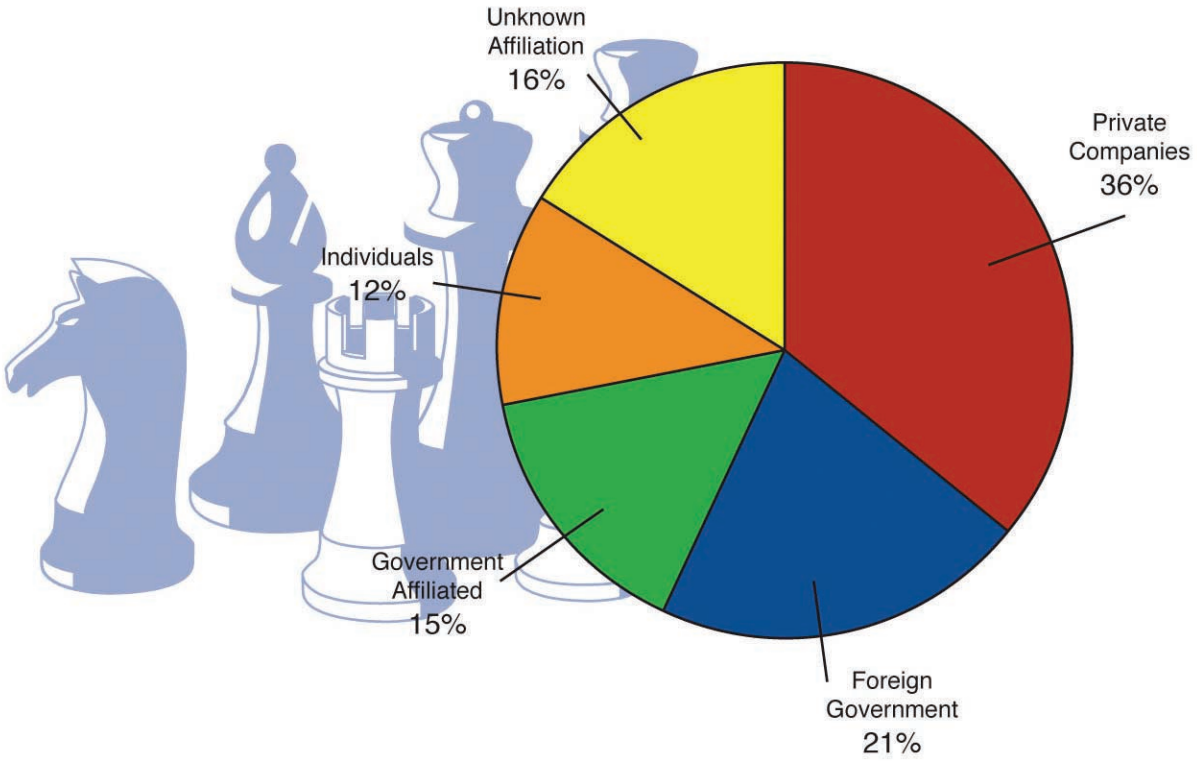
The gravest threat to US technologies, however, comes from foreign entities in only a few countries. Despite the fact that members of the CI Community focus on protecting different types of technologies and use different tracking techniques to monitor foreign efforts to acquire US technologies, there is, nonetheless, a high degree of unanimity among Community members as to which collectors pose the most serious threats. None of the major collectors are new to the technology acquisition game, and many have been aggressive for as long as the CI Community has tracked their activity.

It is impossible to determine exactly how much of the collection effort by these countries has been directed by foreign governments and how much has been carried out by private businessmen, academics, or scientists for purely commercial or scientific needs. The CI Community believes that most trade secret theft takes place without direct intervention by governments, though the governments often do not discourage such theft and themselves often benefit from the transfers.[6] It is clear, however, that some foreign countries, including the major players, also continue to employ state actors—including foreign intelligence services—as well as commercial enterprises, particularly when seeking technologies that are the most sensitive and difficult to acquire.

The best estimate we have of the level of state participation comes from DSS data, which categorizes foreign entities involved in suspicious efforts to acquire sensitive militarily critical technologies from US defense contractors. The DSS data for FY2004 (See Figure 1.) showed that foreign state actors accounted for about one-fifth of suspicious incidents and government-related organizations accounted for another 15 percent. Commercial organizations and private individuals with no known affiliation to foreign governments together accounted for nearly half—36 percent and 12 per-

[6] For many advanced countries, the private acquisition of a US technology does not necessarily imply that the host foreign government will have automatic access to that technology. In fact, in developed countries where governments are bound by rule of law, firms, eager to protect any newly gained competitive advantage, might have little incentive to pass stolen technology to government authorities. In less developed countries, however, particularly dictatorships, where rule of law is weak and companies have little ability to refuse government demands, any acquisition of advanced foreign technology is likely to move quickly to intelligence and military organizations.

Figure 1: (U) Types of Foreign Collectors Targeting US Technology, 2004 (DSS Data)



This figure is Unclassified.

cent respectively—of all suspicious incidents. In another 16 percent, the contractors were unable to determine the affiliation of the foreign parties involved in the elicitation.

The Tools and Techniques of the Trade

While the conduct of traditional espionage is associated with the use of sophisticated clandestine tradecraft, most technology theft takes place using far simpler and less diplomatically risky tools and techniques. These tools and methods of operation change little from year to year, though major technological advances—such as the Internet—sometimes alter the approaches. DSS and AFOSI both make efforts to track techniques used by foreign actors to elicit sensitive militarily critical technologies. (See Table 1.) Both of these databases demonstrate, not surprisingly, that the simplest, least expensive methods are the ones implemented most often. Almost three-quarters of the suspicious incidents reported by cleared defense contractors to DSS in FY2004 involved **direct requests**[7] **by foreign collectors**. These are simple requests—via e-mail, phone call, FAX, letter, or in person—for technology of a controlled nature. These techniques can be applied at virtually no cost to the foreign entity; there is no penalty associated with requesting controlled technologies, and search costs are minimal. It is not uncommon to see one or more middlemen send out multiple requests for a

[7] The "direct request" category used here combines two categories broken out by DSS and AFOSI—"Request for Information" and "Attempted Acquisition of Controlled Technology."

technology, hoping to find one seller willing to take shortcuts on export licensing procedures.

The success of direct requests depends largely on three factors:

- **The knowledge of US organizations regarding export laws**. When diversion of US technology is discovered following a direct request by a foreign entity, a common argument used to mitigate punishment for the transfer is that the US supplier was unaware that the item was controlled or was a trade secret.

- **The willingness of US organizations to carry out due diligence on the foreign buyer**. In some cases, direct requests are placed through organizations whose names provide no indication of the foreign nature of the requestor. If, in addition, the person attempting the acquisition does not state that the item is to be exported, the US seller may feel no need to make a more concerted effort to learn about the final destination of the product.

- **The honesty of the US seller**. In a number of cases over the past few years, the seller has simply chosen to ignore clear indications that the item was to be transferred overseas. Indeed, many US firms—eager to make a sale—have been complicit in efforts to disguise either the type of equipment being exported or the end-user destination.

A technique that is closely related to the direct request is the **solicitation of marketing services**, which, according to DSS data, accounted for more than 10 percent of suspicious efforts to acquire US technology in FY2004. One way that foreign players used this technique was to offer themselves as middlemen to move US goods. In many cases, the foreign firms were registered in

Table 1: (U) Methods of Operation–Comparing DSS and OSI data for FY2004 (percent share of total)

DSS (percent share of suspicious incidents)		AFOSI (percent share of incidents in AFOSI database)	
Direct request*	68	Direct request*	66
Exploitation of relationships	5	Joint ventures	15
Targeting at conventions, expos, and seminars	3	Conferences	9
Exploitation of a foreign visit to US	5	Foreign visitors	5
Solicitation of marketing services	13	Solicitation	3
Foreign employees	0	Seeking employment	3
Suspicious Internet activity	3		
Other	2		

* (U) The "direct request" category used here combines two categories broken out by DSS and AFOSI.

This table is Unclassified.

the United States, and there was no violation of export laws to sell to them. Once in possession of the sensitive technology, some of these firms later masked the movement of the goods abroad.

In another form, foreign entities using this technique have offered products and services—particularly IT-related support—to US firms involved in sensitive projects. Such deals, at a minimum, have provided foreign visitors access to facilities where trade secrets or proprietary information are located. In their most dangerous forms, however, these deals can result in foreign companies subverting US firms' supply chains by selling tainted products. These subversions could give foreign companies long-term, remote access to significant proprietary information and trade secrets. Well-executed supply chain subversions are almost impossible to detect, even years after implantation. Several countries have developed expertise in niche software packages, which they market to US firms.

Exploitation of foreign visits to the United States is yet another technique that foreign entities used to acquire US technology. According to DSS data, about 5 percent of suspicious incidents in FY2004 involved this approach. The increased demand for foreign labor in US high-tech industries and the sharp rise in foreign direct investment in the United States over the past decade have given foreign entities increased access to US businesses and, hence, to US trade secrets.[8] In addition, recognizing the mutual benefits of an unhindered exchange of information, the United States opens its military bases, national laboratories, and private defense suppliers to foreign visitors. There were more than 14,000 requested visits to official US facilities in FY2004, according to CIFA data, most with several foreign nationals in each visit. In most cases, such visits were one-day excursions, but training visits, in particular, have occasionally run several weeks in length. Although facilities hosting foreign visitors generally employ security measures to minimize the loss of trade secrets and sensitive technologies during these visits, the CI Community continues to see reports of losses.

The losses that result from such visits can be significant. Foreign visitors to sensitive US facilities are often among their nations' leading experts and may be much more effective at extracting sensitive information than would be traditional foreign intelligence officers. Specialists know their countries' or companies' specific technological gaps and can focus collection efforts to target critical missing information. Finally, such experts are also in a position to recognize and exploit information that may be inadvertently exposed during visits.

Technology losses through this technique have occurred in a number of ways. For example, foreign visitors have:

- Sought out knowledgeable US experts at these facilities and engaged them in conversation, even when such contact has been explicitly proscribed under terms of the visit. While laws against "deemed exports" make it illegal to convey sensitive information even in oral discussions, such laws are difficult to enforce, since the conversations frequently involve only the individual from the foreign country who is seeking the information and the US citizen who is passing it.

- Wandered away from approved areas and supervisors in order to view sensitive items or, in some cases, attempted to gain access to denied areas and even computer networks.

- Attempted to circumvent potential security obstacles by showing up unannounced to request a visit. This is particularly effective when the prospective foreign visitor represents

[8] The stock of foreign direct investment in the United States rose from almost $400 billion in 1990 to almost $1.4 trillion in 2003, according to the Survey of Current Business.

a company or organization that is negotiating for some kind of major business arrangement with the US entity. The US hosts have, at times, been reluctant to disappoint a potentially lucrative customer by turning away visitors until a formal visit can be scheduled and adequate security arrangements made.

Long-term visitors have several advantages over daylong visitors that can be particularly helpful in efforts to extract sensitive US technologies, trade secrets, or proprietary information. For one thing, those who stay on site for extended periods of time become familiar with security procedures meant to limit their access to sensitive technologies, and the insights thus gained may enable them to circumvent those security practices. This is particularly true of cyber security practices. A long-term presence may allow visitors time to acquire passwords and to learn where on hard drives sensitive information is stored. Then too, whereas short-term visitors are viewed as strangers, long-term visitors become part of the landscape. Their activities naturally receive less notice, which enables them to wander into sensitive areas without attracting undue attention.

One of the oldest methods used to extract technologies is the **targeting at conventions, expositions, and trade shows.** According to DSS data, this activity accounted for only about 3 percent of all suspicious incidents in FY2004. The whole purpose of conventions is to share information in order to sell products or to advance global knowledge in a certain field. The collegiality fostered at such meetings lends itself well to the collection of sensitive information. Standard collection procedures involve clandestinely filming equipment, stealing exhibitors' technical reference manuals, and engaging exhibitors in discussions that might yield classified material or fill collection gaps. Exhibitors, on occasion, have also had their equipment searched and photographed at ports of entry or have had their hotel rooms clandestinely entered and searched for sensitive information.

Finally, foreign entities also continued to employ the **Internet** to gain access to sensitive US technologies and information. The techniques included hacking, probing, scanning, phishing, spamming, and virus dissemination. Collectively, according to DSS statistics from cleared defense contractors, these techniques accounted for only about 3 percent of total suspicious incidents in FY2004. Determining the origins of such attacks can be difficult. Cyber intruders from one country sometimes cover their tracks by routing their attacks through compromised computers in another. However, it is likely that some attackers are not masking their country of origin—either because they are unaware of the footprint they leave, do not know how to hide it, or intend to send a message to their target. As a result, data about cyber attack origins serves as a potential indicator of a country's use of cyber methods to gain information on US technologies. It is important to note that most private companies and all US Government agencies are subject to such attacks.

The private sector, where computer security in many sectors is catch-as-catch-can, according to industry experts, is probably most susceptible to losses from cyber attack, though, US Government systems are not immune to attack. For example, a three-year research project by a private security firm recently concluded that, although most private companies believed their virtual private networks (VPNs) were invulnerable to hackers, actually nine out of ten of the VPNs had exploitable vulnerabilities. In some cases, the report stated, VPNs were actually the weakest security link in an organization. Determining the extent of commercial losses from cyber attack is difficult, but a separate private sector survey attempting to estimate losses found that 43 percent of responding firms said they did not know the damages resulting from cyber breaches, while 33 percent reported no financial loss. Around one-in-five reported damages of less than $500,000, while 5 percent had losses of greater than $500,000.

Table 2: (U) Targeted US Militarily Critical Technologies

Incidents reported by cleared US Government contractors to DSS (Percentages represent share of total suspicious incidents)				Illicit technology transfer attempts (Based on AFOSI database)	
Technology Categorized by 2004 MCT List	**2004 % of Total**	**Technology Categorized by 2003 MCT List**	**2003 % of Total**	**Technology Using AFOSI Categorization**	**2004 % of AFOSI Reporting**
Information Technology	21.0	Information Technology	22.0	Information Technology	15.1
Sensors	12.6	Sensors and Lasers	17.3	Sensors	11
Aeronautics	11.8	Aeronautics	10.2	Armaments and Energetic Materials	10.8
Electronics	11.1	Electronics	9.4	Electronics	10.5
Armaments and Energetic Materials	9.6	Armaments and Energetic Materials	8.8	Materials and Processing	8.6
Lasers and Optics	7.5	Chemical and Biological Systems	5.0	Space Systems	7.4
Signature Control Technology	4.7	Space Systems	4.8	Aeronautics	7.2
Materials and Processing	3.3	Marine Systems	4.2	Manufacturing and Fabrication	6.5
Chemical Technology	3.0	Materials and Processing	4.1	Guidance, Navigation, and Vehicle Control	5.5
Space Systems	2.7	Guidance, Navigation, and Vehicle Control	3.7	Nuclear, Biological, and Chemical Systems	5.3
Positioning, Navigation, and Time Technology	2.5	Manufacturing and Fabrication	3.3	Directed and Kinetic Energy Systems	4.8
Marine Systems	2.2	Power Systems	2.2	Marine Systems	4.5
Biological Technology	1.7	Signature Control	1.2	Power Systems	2.9
Power Systems	1.7	Directed Energy Systems	0.9		
Manufacturing and Fabrication	1.7	Information Warfare	0.9		
Biomedical Technology	1.2	Ground Systems	0.8		
Ground Systems Technology	0.6	Nuclear Technology	0.8		
Directed and Kinetic Energy Systems	0.5	Weapons Effects	0.5		
Nuclear Technology	0.4				
Weapons Effects	0.2				

This table is Unclassified.

All Technologies at Risk

Because foreign collectors can include everyone from foreign intelligence officers to businessmen, virtually all categories of US trade secrets—military and civilian—are targeted and have been collected against over the years. The CI Community pays closest attention to technologies with direct military application and to those on the Defense Department's Militarily Critical Technologies List (MCTL), many of which are dual-use, with both military and commercial applications. In fact, most of the foreign illicit technology transfer efforts that were tracked by the Community in FY2004, involved dual-use items.[9] The majority of the technology targeted was unclassified, according to DSS data, although much of it was controlled under either the ITAR administered by the Department of State or the EAR administered by the Department of Commerce. [10]

The MCTL technologies most highly targeted by foreign entities in FY2004 varied little from those that topped the list in previous years. Although DSS began using volume III of the MCTL in 2004, which categorizes the technology in more detail than the volume II version used in earlier years, a quick comparison of FY2004 and FY2003 figures shows an almost identical pattern of technology collection. DSS's findings also track closely in most categories with AFOSI's data. (See Table 2.)

In FY2004, as in earlier years, **information systems** (IS) continued to top the list of targeted technologies, accounting for 20 percent of suspicious incidents reported by DSS and more than 15 percent of AFOSI's database. Included in this category are both efforts by foreign entities to acquire sensitive software and hardware as well as offers to sell software to cleared defense contractors involved in developing sensitive technologies. The high-level foreign interest in IS probably reflects several factors.

- Global demand for IS products remains strong. Computer hardware and software increasingly are the foundation of almost all modern systems, both civilian and military. Processes from design to manufacture to shipping are computer-based, and the entities with the most sophisticated and up-to-date systems often have the advantage both in the marketplace and on the battlefield.

- Foreign access to this field is high. More than 40 percent of the Ph.D.s employed in computer and information sciences fields in the United States in 2001, the most recent year for which data are available, were foreign-born. By comparison, only about 10 percent of all employed doctoral scientists and engineers were born abroad.

After information systems, the next four most highly sought-after technologies on the MCTL last year were:

- **Sensors**. These are largely enablers for military action, providing the eyes and ears of many military systems. The fact that the United States has retained the global technological lead in this category has accounted for the continued strong demand by foreign collectors. Sensors accounted for just over 10 percent of DSS and

[9] Purely military technologies are less often the subject of foreign theft, probably because such exports are scrutinized more closely and involve more obstacles, including the registration of exporting companies. In addition, there is a tighter network of manufacturers, exporters, regulators, and enforcers involved in military exports.

[10] Dual-use items that would make a significant contribution to the military potential of another country are regulated under the Export Administration Act and are on the Department of Commerce's Commodity Control List. The Commodity Control List includes items from the MCTL and technology that could support the proliferation of chemical, biological, or nuclear weapons or missile technology. The Arms Export Control Act regulates the export of defense articles and services. Such exports may be licensed only if their export will strengthen US national security, promote foreign policy goals, or foster world peace. The Arms Export Control Act is administered by the Department of State, Center for Defense Trade Controls, through the International Traffic in Arms Regulations and the US Munitions List. The Munitions List is a list of defense articles that require a license prior to export.

AFOSI suspicious incident reporting in FY2004. Included in this category of technology are high-speed cameras, night vision equipment, and sensor platforms placed on unmanned aerial vehicles (UAVs).

- **Aeronautics**. The demonstrated advantage of airpower in recent international conflicts has provided added impetus to collection against this technology. In FY2004, 12 percent of DSS and 7 percent of AFOSI suspicious incidents involved aeronautics. A significant portion of that collection went against UAV technology. The success of UAVs in surveillance, intelligence collection, and even as offensive weapons during the Afghanistan and Iraq conflicts has led to stepped-up international interest. Other aeronautics technologies targeted included composite materials, onboard computer management systems, and experimental and developmental aerospace platforms.

- **Electronics.** This is one of the critical technologies that gives the United States its modern military capabilities. Electronic technologies are either contained or used in the production of virtually every weapons system in the US arsenal, and they enable a dramatically higher performance and reliability with smaller size and longer power. This militarily critical technology accounted for about 11 percent of both DSS and AFOSI suspicious incident reporting in FY2004. Specific technologies collected against included components for test equipment and missile development as well as technologies such as microwave amplifiers, advanced semiconductor devices, and integrated circuit-test equipment.

- **Armaments & Energetic Materials.** These technologies are required to develop and produce in quantity safe, affordable, storable, and effective conventional munitions and weapons systems of superior operational capability. Roughly 10 percent of DSS and AFOSI suspicious incident reporting last year focused on this technology, including specific efforts to target naval anti-cruise missile systems, land-attack cruise missile systems, and antiballistic missile air defense systems.

As difficult as it is to track foreign collection efforts against items on the MCTL, it is even more challenging to monitor, on a regular basis, foreign targeting of purely civilian technologies. US firms are reluctant to raise alarms about possible technology theft, out of concern for the potential impact on investor and consumer confidence and stock prices. In addition, many companies fear that prosecution of a technology theft case could lead to the disclosure of other closely held trade secrets or proprietary information, although sections of the Economic Espionage Act of 1996 (EEA) specifically protect against such release and the history of prosecutions under the EEA demonstrates that the courts are committed to preventing additional damage.

Recent legal cases alleging technology theft as well as cases pursued by the Department of Justice (DOJ) under the EEA over the past few years illustrate the wide variety of technologies that have been targeted. Some of those reported in the press include:

- **Software and proprietary information on company operations.** In April 2003, the United States Attorney's Office for the Northern District of California announced that a citizen of Singapore had pled guilty to theft of trade secrets. He admitted that in early 2002, while working for a language translation company, he delivered a laptop computer and a hard drive that contained trade secrets and confidential proprietary information to a competitor. Separately, an Indian software engineer employed by a US company's software development center in India is accused of "zipping up" proprietary software source code for printing identification cards and uploading it to her personal e-mail account in July 2004.

- **Computer microprocessor.** In November 2003, a China-born US permanent resident pled guilty to illegally exporting 80 military-formatted microprocessors to a Chinese organization that develops radar systems for both military and civilian uses.

- **Networking equipment.** In early 2004, according to press reports, a major US company filed a motion asking a US district court to enforce a deal it had struck earlier with Huawei Technologies, to stop Huawei using the US firm's intellectual property. The US company charged that Huawei had misappropriated and copied trade secrets to build cheap but sophisticated gear bearing a striking similarity to the US company's products. Following an earlier agreement, Huawei had pulled some of its products off the market and promised not to copy more of the US company's code.

- **Formulas for production of epoxy resins.** In August 2004, a US manufacturer and developer of epoxy resins filed a lawsuit seeking damages of at least $100 million against Formosa Plastics Corporation alleging unlawful conduct, including unfair competition, misappropriation of trade secrets, fraud, and conspiracy.

The Road Ahead

At least in the near term, the CI Community expects no letup in foreign demand for sensitive US technologies. Although some countries have already effectively mastered stolen US technologies and have applied them successfully in military and civilian applications, staying on the cutting edge, for many, will be a challenge. For the next few years, at least, the United States will likely remain the provenance of much of the world's newest and most creative technologies in many fields. As long as that dominance continues, foreign entities will depend on US innovation to remain competitive, insofar as competitiveness depends on technology.

But protecting the US advantage is likely to be increasingly difficult. Foreign access to state-of-the-art technology can only rise as an increasing share of Doctorates awarded by US universities in the fields of science and engineering go to foreign-born researchers and as foreign participation in the US economy increases.[11] Foreign governments in several countries have already proven effective at tapping these overseas scientific communities for access to US technology, a trend that will continue and will become further refined as these communities grow.

At the same time, rapidly improving political and economic conditions in some of the key labor-supplying countries mean that a larger share of arriving students may return, at some point, to work in their homeland. When they depart, their US educations and their accumulated scientific and commercial expertise leave with them. Ironically, the United States, which has long benefited from its ability to attract some of the best and brightest minds from around the world, could experience a significant brain drain of its own over the next few years. Unlike the movement of labor from less developed countries, however, this return flow of businessmen, scientists, and academics will come with a bonus for the foreign countries—state-of-the-art US technology.

The further intertwining of US and foreign capital and assets that is accompanying globalization also will continue to complicate the problem of protecting US technologies. US firms will increasingly move their R&D outside US borders to overseas centers like the one that a major US high-tech firm recently opened in Tokyo, Japan, and one that another such firm is scheduled to open in 2005 in Bangalore, India. The growing pool of relatively cheap scientific talent makes these locations ideal for innovative research. Protecting the US technologies that will serve as

[11] There has been a steady rise since 1995 in the share of Doctorate degrees awarded in science and engineering to non-US citizens. In 1995, about 28 percent of PhDs in science and engineering went to non-US citizens, compared to 38 percent in 2003, according to the National Science Foundation.

the foundation for this research will be difficult by itself in these overseas environments, let alone safeguarding the cutting-edge results of foreign research. In fact, in a very real sense, the results of the global R&D effort are likely to go to the global marketplace, not the US market.

The continued inflow of foreign investment into the United States will create corporate entities that are part foreign and part US.[12] Ensuring that sensitive US technology does not pass through these entities to the country of origin of the parent firms will be difficult at best. Historically, the United States has been a major beneficiary of such foreign investment, but most past investment has come from Europe and Canada, where similar legal systems and close political and economic alliances have helped dampen the outflow of sensitive technologies. The interlinking of US firms with those from less developed countries, however, where technological gaps are wide and legal structures protecting technology are immature, creates the potential for less controlled outflows. However, over time, commercial pressures may lead foreign governments to strengthen legal protection for trade secrets in order to remain competitive and to comply with requirements of multilateral institutions such as the World Trade Organization (WTO).

For the most part, the CI Community expects the countries that are major threats today will remain so for the foreseeable future. As to new collectors that may emerge as threats in the foreseeable future, the only trend apparent at this time is an increased tendency to funnel US technology through middlemen in international trading centers and through key US allies. At present, the CI Community sees few signs that these places are taking increased measures to crack down on such activities. Until they do, we expect to see collectors step up use of these locations.

[12] The United States has a mechanism in place to prevent foreign investment that is deemed to threaten US strategic interests. The Committee on Foreign Investments in the United States (CFIUS) reviews such investments and has the authority to prevent a foreign acquisition or, in the event that takeover has already occurred, to order divestiture. Similarly, US federal laws require firms that have access to US classified information to be generally free from foreign ownership, control, or influence (FOCI).

CI Community Efforts to Counter the Problem

The US CI Community devotes significant resources to protecting US technologies from foreign theft. The goal of these efforts is to inhibit illegal foreign acquisition of certain sensitive US technologies that might undercut US economic or military prowess. At the same time, however, the Community is eminently aware of the need to avoid impinging on the international flow of goods and technologies that are part of the US economic engine. Over the past few years, the CI Community has made significant strides in accomplishing this task. A few of the major accomplishments include:

- **The CI Community as a whole** has significantly increased interagency cooperation. Projects are under way to bring together intelligence collectors, analysts, and enforcers to ensure timely sharing of information and more rapid prosecution of key cases. The large number of agencies that cooperate in producing this Annual Report to Congress, similarly, is a demonstration of the CI Community's ability to combine resources in order to better understand the problem of foreign theft of US technology.

- **The Counterintelligence Field Activity (CIFA)** has used its Research and Technology Protection Division (RTP) to provide CI products, including risk assessments for critical US technologies, to DoD and other US Government organizations. RTP products are aimed specifically at protecting research, technologies, programs, and facilities that are considered vital to US national security.

- **The Defense Threat Reduction Agency (DTRA)** has embedded CI and security personnel into teams that are responsible for technology

testing and evaluation. These personnel are inserted at the earliest possible time to afford technology protection from concept to fielding. CI and security personnel are also actively involved in briefing DTRA's test division members on CI issues. In addition, they review test-related information being published in open sources prior to release for publication to ensure that sensitive technical information is not inadvertently released. Moreover, DTRA shares intelligence with other US Government agencies regarding threats to emerging technologies.

- **The Defense Security Service (DSS)** has integrated CI into the National Industrial Security Program by providing threat information and CI briefings to the nearly 12,000 cleared defense contractors located across the United States. Based on the information reported by these contractors, DSS tracks and analyzes the changing nature of the threat to US technologies. In addition, DSS has hosted and supported numerous regional interagency working groups to coordinate Community responses to threats against US industry and advanced technology.

- **The Federal Bureau of Investigation (FBI)** has created an Economic Espionage Unit within the Counterintelligence Division to program manage the theft of trade secrets by foreign agents. It has also organized and maintained major outreach efforts to provide specific threat information to both the public and private sector. The Awareness of National Security Issues and Response (ANSIR) program provides threat awareness information to the private sector, while InfraGard is a partnership between the FBI and the private sector aimed at sharing information and analysis in order to prevent hostile acts against the United States. In addition, over the past year, the FBI has hosted three regional conferences, with a total of 332 federal and state law enforcement agents and 60 private sector attendees. Moreover, the FBI produced a training video to educate private industry and law enforcement on the issues of foreign economic collection and economic espionage. It has also established a 1-800 number for private industry to directly report suspicious activities or complaints regarding the theft of trade secrets, critical technologies, or proprietary information. In addition, the FBI and the Naval Criminal Investigative Service have joined together in a pilot program to protect US institutions (public and private) in the San Francisco area that have or are developing technologies identified by the US Navy as critical.

- **The National Geospatial-Intelligence Agency (NGA)** has initiated a research and technology protection program designed to protect NGA's most critical technologies. Critical technologies and programs are identified, multidisciplinary CI threat assessments conducted, and program protection plans prepared, including CI support plans. NGA has also stepped up its employee CI awareness programs, to include advising personnel of steps that can be taken to protect against foreign elicitation of sensitive information as well as against inadvertent disclosure. Briefings are given both to employees likely to host visitors and to those likely to attend conferences, trade shows, symposiums, air shows, etc. NGA has also published Advanced Technology Assessment Reports and Technology Assessment Control Plans, both designed to allow NGA to rapidly, but safely, inject new and emerging technologies into normal NGA processes.

- **The National Reconnaissance Office (NRO)** has worked to improve the identification of espionage threats to NRO operations, information systems, and personnel, and to increase the awareness of targeting efforts by nontraditional threat countries and groups. To keep the NRO population informed on current threats, NRO's Office of Counterintelligence (OCI) publishes several products that are posted to its homepage and mailed on a regular basis to

individuals and firms that do not have connectivity. Similarly, to help its contractor community stay apprised of threats to technology, NRO provides tailored briefings for contractors and security officers. Briefing schedules are announced over the Government-wide Area Network. In addition, NRO has streamlined its CINet, a secure and automated web-based application residing on the Contractor Wide Area Network. CINet is designed to electronically report foreign travel and contacts and to disseminate threat information to security officers and authorized users within and outside of government facilities. The CINet also provides users with a means of submitting requests for specific CI services.

Appendix A

Foreign Countries Experiencing Technology Losses

The United States has undoubtedly suffered more as a result of trade secret and technology theft than any other nation, but protecting against this problem is not a uniquely US challenge. Over the past year, a number of other countries have suffered from foreign industrial espionage, and Washington may find common cause with some of them in seeking tougher international regulations and enforcement to protect proprietary information and technology.

- **China**: In April 2004, a court in China sentenced a former engineer from a Wuhan Iron & Steel Company to 18 years in jail for taking bribes and industrial espionage, according to press reports. The individual was found guilty of selling sensitive corporate information to an unidentified foreign company bidding for the project to produce high-end steel products and cold-rolled steel sheet. The foreign company accused of receiving the information reportedly pulled out of the bidding process after the individual was arrested.

- **Russia**: In April 2004, Russia's Federal Security Service claimed to have uncovered an industrial espionage network that was preparing to pass information on Russia's satellite program to the Chinese. The theft would have enabled China to close the gap with Russia in satellite production and delivery, according to press reports.

- **South Korea**: In mid-2004, a South Korean employee of a Hong Kong-based cell phone distributor was arrested on charges of espionage for attempting to give 75,000 internal computer files from a South Korean handset maker to a Hong Kong firm. The computer files contained secret information about the South Korean company's technology for making mobile phones. Prosecutors estimated that if the information had leaked, it would have cost the company $3.8 billion in lost exports.

Appendix B

Glossary of Terms

ACCO	Army Case Control Office
ACIC	Army Counterintelligence Center
AFOSI	Air Force Office of Special Investigations
ANSIR	Awareness of National Security Issues and Response
BIS	Bureau of Industry and Security
CFIUS	Committee on Foreign Investments in the United States
CI	Counterintelligence
CIA	Central Intelligence Agency
CIC	Counterintelligence Center
CIFA	Counterintelligence Field Activity
CINet	Counterintelligence Network
DIA	Defense Intelligence Agency
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DS	Diplomatic Security
DSS	Defense Security Service
DTRA	Defense Threat Reduction Agency
DTSA	Defense Technology Security Administration
EAR	Export Administration Regulations

EEA	Economic Espionage Act of 1996
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FOCI	Foreign Ownership, Control, or Influence
FY	Fiscal Year
ICE	Bureau of Immigration and Customs Enforcement
INR	Bureau of Intelligence and Research
IOC	Information Operations Center
IS	Information Systems
IT	Information Technology
ITAR	International Traffic in Arms Regulations
MCTL	Militarily Critical Technologies List
NASA	National Aeronautics and Space Administration
NCIS	Naval Criminal Investigative Service
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
OCI	Office of Counterintelligence
ONCIX	Office of the National Counterintelligence Executive
PDAs	Personal Digital Assistant
R&D	Research and Development
RTP	Research and Technology Protection

UAV	Unmanned Aerial Vehicle
US	United States
VPNs	Virtual Private Networks
WTO	World Trade Organization