Secrets Stolen, Fortunes Lost
How economic espionage and intellectual property theft destroy businesses and endanger the global economy

By Christopher Burgess and Richard Power

Christopher Burgess worked in the clandestine service of the U.S. Central Intelligence Agency (CIA) for 30 years. In the course of his career, he served both as chief of station and senior operations officer. Richard Power, as editorial director for Computer Security Institute (CSI) and then as director of global security intelligence for Deloitte Touche Tohmatsu (DTT), researched cybercrime and economic espionage for more than a decade.

We have found two profound misconceptions common among CEOs. One of the great misconceptions is that the threat of economic espionage or trade secret theft is a limited concern—that it is only an issue if you are holding on to something like the formula for Coca-Cola or the design of the next Intel microprocessor. The case studies included here illustrate the fallacy of thinking that this threat is someone else's problem.

The other great misconception, held by many business leaders who *do* acknowledge the danger to their trade secrets and other intellectual property, is that the nature of this threat is sufficiently understood and adequately addressed. Often, on closer inspection, the information-protection programs these business leaders rely on are mired in Industrial Age thinking; they have not been adapted to the dynamic and dangerous new environment forged by globalization and the rise of the Information Age.

This article is based on open-source (i.e., not classified) intelligence. There is a compelling lesson in this fact. A decade ago, such stories rarely made it onto the news wire or into the courts. Today, they are commonplace. Unfortunately, the awareness and defenses required to thwart such damaging activities, although economical and effective, are far from commonplace. Our hope is to change that.

To provide a comprehensive overview of the diverse vectors of attack, and how to evaluate whether your enterprise has the necessary defenses in place, we will look at actual cases organized into three broad categories:

- When insiders and competitors target businesses
- When state-sponsored trade secret theft targets businesses
- When counterfeiters, pirates and organized crime target products

And in our conclusion, we have provided some analysis of the economic and geopolitical impact, and a comprehensive checklist of proactive security and intelligence measures.

Part I: When Insiders and Competitors Target Businesses

Economic espionage or intellectual property theft conducted by insiders, competitors or combinations of the two are the most tangible, most common and most destructive threats.

Such an attack can take many forms, like an employee, a member of the management team, a corporate board member, a third-party contract manufacturer or a collaborative partner in a joint venture. Here are several recent examples, ranging from the sordid to the spectacular:

Lightwave Microsystems

In late 2002, Lightwave Microsystems, a privately held company in California, announced it would cease operations because of financial difficulties. But Lightwave's inability to turn a profit didn't mean it was without value. It held patents and had developed saleable trade secrets. It was subsequently bought by NeoPhotonics (San Jose, Calif.), but not before some ugliness.

Brent Woodward held a trusted position at Lightwave. He was its director of information technology. He copied the company's trade secrets, which had been stored on backup tapes, and then attempted to sell them to a competitor.

No one detected Woodward's unauthorized activity. As the company's IT director, he had natural and unencumbered access to the information and, indeed, it was his responsibility to protect it.

Using an alias ("Joe Data") and a Web-based e-mail account (lightwavedata@yahoo.com), Woodward contacted the chief technology officer for JDS-Uniphase (JDS), and offered to sell Lightwave's data. But JDS immediately contacted the U.S. Federal Bureau of Investigation (FBI), agreed to cooperate in the investigation and allowed the FBI to monitor its communications with "Joe Data."

The FBI trace determined that the "Joe Data" messages were originating from an Internet connection within Woodward's residence. After executing a search warrant, the FBI charged and arrested Woodward on one count of theft of trade secrets.

In August 2005, the U.S. attorney's office for the Northern District of California announced that Brent Woodward pleaded guilty to the charge and was scheduled to be sentenced in December 2005. Woodward faced the possibility of 10 years imprisonment and a fine of $250,000.

Of course, Woodward was an amateur and was acting by himself, for himself, and thus had no interests other than his own. His methodology was very sophomoric. But even a bumbling amateur can deliver a devastating blow.

Consider what would have happened had Woodward offered the purloined data to a less ethical competitor. Would the value of Lightwave have been jeopardized and its sale to NeoPhotonics canceled if the unethical competitor got to market fast enough? Certainly.

And, if the trade secret theft was revealed only after NeoPhotonics purchased Lightwave, what recourse would NeoPhotonics have had available to it? Little more than a lengthy litigation to protect intellectual property it wasn't aware had been stolen prior to the purchase.

America Online (AOL)

In April and May 2003, an AOL software engineer named Jason Smathers used a colleague's access codes to acquire information on 30 million AOL customers. The stolen data, which consisted of 92 million separate records, included e-mail addresses, screen names, ZIP codes, customer credit card types and telephone numbers associated with AOL customer accounts.

Smathers sold the stolen AOL e-mail addresses to Sean Dunaway for US$27,000. Dunaway, a resident of Las Vegas, Nev., utilized the addresses to advertise his own online gambling website, and then resold the AOL data to "spammers" for approximately $52,000.

Smathers' use of a colleague's administrative log-in proved to be an effective way to bypass AOL's internal security controls. (His colleague had the natural access; Smathers didn't.) AOL knew that it had a problem and was cooperating with law enforcement, but Smathers remained an AOL employee, and unidentified as the culprit, until mid-2004.

The U.S. Department of Justice (DoJ) prosecuted this case under the Controlling the Assault of Non-Solicited Pornography and Marketing (Can-Spam) Act.

In February 2005, Smathers pleaded guilty. In October 2005, he was sentenced to 15 months in prison and fined $84,000, triple what he garnered through the sale of the data. (Smathers clearly knew the data was worth something, but he grossly underestimated the street value of the information.)

Though DoJ recommended that Smathers be barred from the software profession, the judge noted Smathers' cooperation in the investigation and believed that the cooperation and Smathers' contrite behavior warranted leniency. Smathers told the court that AOL had said his theft and subsequent sale had cost the company at least $400,000. (Potentially, it cost it millions of dollars.)

But the real damage may still be looming out there in the dark alleys of cyberspace. What costly mischief could e-mail fraudsters ("phishers") or unscrupulous telemarketers carry out with the collation of those e-mail addresses, user names and user telephone numbers? Such personal information is priceless in the underworld industry of identity theft.

There is also the risk to one's reputation in such incidents. AOL is advertised as a "family-friendly" environment, one where the customer doesn't have to be a technological marvel to enjoy the wholesome pleasures of the Internet and not be exposed to its seedier side. AOL admitted that the Smathers caper cost the company at least $400,000; the downside may be much greater as it creates software to mitigate the

loss of customer data, while simultaneously working to regain the trust of its customer base.

Casiano Communications Inc.
In mid-October 2005, Casiano Communications Inc. (CCI), the prominent publisher of Caribbean business and travel literature magazines, filed suit against John Bynum, a former employee. CCI alleges that Bynum stole its intellectual property, specifically databases, which Bynum forwarded to his personal e-mail account from CCI's computers. According to CCI, he stole client and advertiser information, which violates the company's electronic mail and company resources and equipment policy.

CCI alleged that Bynum had been selling a database of key business contacts in Puerto Rico, to assist companies in marketing their products and services.

The Superior Court of San Juan, Puerto Rico, issued a temporary restraining order against Bynum. It required him to cease and desist from utilizing, transmitting, selling or reproducing any form of database, or other trade secrets obtained during the course of his employment with CCI. The injunction granted CCI the right to seize all of its materials contained in any computers, disks or other information-technology items in the personal possession of the defendant.

Corning Inc.
Jonathan Sanders was an employee of Corning Inc. who worked at the Harrodsburg, Ky., plant. On Oct. 20, 2005, DoJ charged him with the theft of trade secret material belonging to Corning, specifically material pertaining to an overflow downdraw fusion glass-making process used to produce thin filter transistor liquid crystal display (LCD) flat panel glass.

It is alleged that Sanders began his theft of Corning's intellectual property in December 1999, and that it continued through December 2001. It is also alleged that Sanders subsequently sold the material to PicVue Electronics, a Taiwanese corporation.

In his statement to the FBI, Sanders indicated that he found blueprints containing the Corning trade secrets within a Corning warehouse in 1999. The blueprints were in a container of material awaiting destruction. Sanders took the blueprints home instead of destroying them. He traveled to California and met with Jacob Lin, PicVue's president, and Yeong C. Lin, a consultant working with PicVue. According to Sanders, he did not actually show them the drawings; he only described the fusion draw process. Subsequently, PicVue allegedly offered him a job, which he declined.

Many months later, in September 2000, PicVue wired US$30,000 to a California bank account. Lin, the consultant, took control of the funds and enlisted a college roommate, Danny Price, to deliver $25,000 of it to Sanders, so as to obfuscate the connection between PicVue and Sanders. In exchange for the money, Sanders gave Price the stolen Corning blueprints.

PicVue's engineers took digital pictures of the blueprint documents and transferred the images to a digital storage device. The engineers hand-carried the device back to Taiwan. The blueprints were then allegedly destroyed.

In November 2000, engineers from PicVue traveled to Kentucky and met with Sanders to discuss the blueprints he had sold to PicVue.

In September 2001, PicVue representatives traveled to Saint-Gobain Ceramics, a company in Niagara Falls, N.Y., to purchase a part for the fusion process. Because of their prior commercial relationship with Corning, Saint-Gobain personnel recognized the utility of the part as being applicable only to the fusion draw process, and alerted Corning to the possibility that its trade secrets had been compromised. Corning representatives visited Saint-Gobain's offices, reviewed the specifications provided by PicVue, and concluded that Corning trade secrets were involved.

Corning contacted the FBI, and an investigation commenced in October 2001, which led to Sanders' arrest and indictment in late 2005. The prosecuting attorney noted that the intellectual property carried a value of $100 million. Sanders pleaded guilty to the charges and was to be sentenced on April 18, 2006. Corning and PicVue were able to arrive at a settlement, with PicVue allegedly having paid Corning $15 million in damages. In April 2006, Sanders was sentenced to four years imprisonment and fined $20,000.

Corning apparently had a set of procedures in place to destroy company confidential documents, but it appears that it had no mechanism to ensure that documents put into the "to be destroyed" bin were, in fact, subsequently destroyed.

This case offers another example of a company being ignorant of the theft of its intellectual property until the recipient of the stolen secrets approached one of the few organizations in the world able to create the parts necessary to make the purloined documents effective in the marketplace. It was the strength of the relationship between Corning and Saint-Gobain that brought the illegal activity to light—certainly not any of Corning's internal procedures.

Avery Dennison

Avery Dennison, headquartered in Pasadena, Calif., is one of the country's largest manufacturers of adhesive labels. It spends a great deal of money on research and development of adhesives, and retains the formulas as its intellectual property. The company's adhesives and methodologies provide it with a significant advantage in the global adhesive label market.

Four Pillars Enterprise, a Taiwanese competitor with market share both in the United States and the Far East, targeted Avery Dennison's Concord, Ohio, research facility, and stole Avery Dennison's intellectual property from 1989 through 1997.

The theft is a classic example of a competitor's methodical harvesting of technological advances and research. Avery Dennison was unaware of the economic espionage until a former Four Pillars employee applying for work with Avery Dennison revealed that an Avery Dennison employee had been supplying Four Pillars with adhesive formulas for the preceding eight years.

The FBI, together with Avery Dennison, contrived a successful sting operation to identify the employee who was working for Four Pillars. The culprit was Ten Hong Lee (a.k.a. "Victor Lee"), a U.S. citizen and a senior research engineer within Avery Dennison's Concord, Ohio, research facility.

Lee, who received his undergraduate degree at the National University of Taipei, his master's degree in polymer science from Akron University and his PhD in chemical engineering from Texas Tech, had been invited to visit Taiwan by the Industrial Technology Research Institute to give a lecture. While there, he was invited to present a technical lecture to Four Pillars.

Lee was enticed to enter into a covert relationship with Pin Yen Yang, Four Pillars' president and CEO, as a "secret consultant," for which he was paid US$25,000 his first year. Lee, Yang and Yang's daughter, Hwei Chen Yang, (a.k.a. "Sally Yang"), conspired to obtain Avery Dennison's intellectual property and business methodologies. In exchange, Lee would be paid substantial sums of money.

Four Pillars had targeted an individual with whom the Yangs could relate on an ethnic basis, leveraging Lee's desire to help a fellow countryman and pandering to his ego by providing him "recognition" for his intellect. Of course, it also paid him US$150,000 over the years, and deposited the funds with Lee's relatives in Taiwan to keep his skullduggery out of view of tax authorities, lenders or others who might have questioned the supplemental income.

When confronted, Lee admitted his guilt and was persuaded to act as a cooperative witness for the DoJ, which wanted to prosecute this theft of the intellectual property of a U.S. corporation by a foreign national under the powers of the Economic Espionage Act of 1996.

In September 1997, Lee met with the Yangs at a Holiday Inn in Westlake, Ohio, and provided them with more of Avery Dennison's intellectual property. The room was under FBI surveillance. Following the meeting, the Yangs were observed using a knife to cut the headers and footers off the documents provided by Lee.

The Yangs were subsequently arrested. In 1999, U.S. District Court Judge Peter C. Economus convicted both Yang and his daughter of stealing trade secrets, and also convicted Four Pillars on economic espionage charges. Yang was sentenced to six months of home confinement and fined US$250,000. His daughter was fined $5,000 and received a year's probation. Four Pillars was fined $5 million for accepting the pilfered trade secrets. Lee pleaded guilty to wire fraud and defrauding his employer.

Yang's investment of approximately $150,000 resulted in estimated losses of $30 million to $50 million for Avery Dennison. Four Pillars appealed the conviction to the U.S. Supreme Court, but the convictions were upheld in October 2002.

Toshiba and Lexar Media

In 1994 and 1995, Cirrus and Toshiba were involved in discussions on how Cirrus would collaborate with Toshiba in creating flash memory controllers in support of Toshiba's preferred flash memory technology.

In mid-1996, some Cirrus employees founded Lexar Media.

On Dec. 1, 1996, Toshiba, Toshiba America and Toshiba America Electronic Components were given access to Lexar's intellectual property under a five-year non-disclosure agreement.

In 1997, Toshiba invested $3 million in Lexar, and also placed a member of its own on Lexar's board of directors. Lexar continued to share intellectual property.

In April 1998, Toshiba and Lexar entered into a partnership to compete in the flash memory market. The joint relationship apparently prospered throughout 1998 and most of 1999. But in October 1999, Toshiba entered into a joint agreement to develop and manufacture Gigabit Scale flash memory with SanDisk, Lexar's main competitor in the flash memory market. Lexar felt that its "partner" had sold it out. Not only had Toshiba been a partner in numerous joint development projects, but Toshiba's presence on Lexar's board of directors also provided Toshiba with intimate knowledge of all of its strengths and weaknesses.

Toshiba assured Lexar that the agreement with SanDisk did not involve Lexar technologies, and was between a separate division within Toshiba than that involved with Lexar.

Soon, SanDisk and Toshiba signed a $700 million deal to create a joint fabrication facility in Virginia to produce multilevel cell (MLC) flash memory chips. Lexar believed that its intellectual property, specifically the multipage write technology, was being used, and that without it the MLC flash memory initiative would not be financially viable. But Lexar didn't have the proof until 2001, when Toshiba published the technical specifications used in its MLC smart memory application.

In late March 2005, a California Superior Court jury found Toshiba guilty of the theft of Lexar Media's trade secrets, and assessed total damages of $465.4 million, including $84 million in punitive damages. According to Lexar Media, its trade secrets were being utilized in Toshiba products such as NAND flash chips, Compact Flash cards, xD-Picture Cards and Secure Digital cards. In December 2005, the same court agreed to Toshiba's request for a new trial. The litigation continues; no new trial date has been set.

Particularly noteworthy in this case is Toshiba's apparent brashness. It had a seat on the board of directors of the company whose intellectual property it allegedly purloined. It also participated in a number of joint development projects, during which Lexar's intellectual property was fully disclosed to Toshiba, and which Toshiba then apparently leveraged for its own benefit in another product line.

Citroen and SigmaTel

What do Citroen, the French automobile manufacturer, and SigmaTel, a U.S. manufacturer of audio entertainment devices, have in common?

Both corporations allege that patented methodologies were misappropriated by Chinese competitors and used in products marketed in China so that, in effect, Citroen and SigmaTel ended up competing against their own product designs. Furthermore, because the Chinese had little or no research costs associated with development, the products were made available at a price considerably lower than the company that owned the patent could possibly afford to offer.

In January 2005, SigmaTel filed suit against Actions Semiconductor Company (Actions Semi) of Zhuhai, Guangdong, China, alleging that integrated circuits inside of Action Semi's MP3 players infringe upon multiple patents related to SigmaTel's portable audio devices. In March 2005, it followed up by filing a complaint with the U.S. International Trade Commission (ITC) requesting that the ITC initiate a Section 337 investigation. (According to the International Trade Data System, under Section 337 of the United States Tariff Act of 1930, imported products that allegedly violate U.S. intellectual property rights can be barred from entry into the country. Complaints under Section 337 are made to the ITC, and generally involve allegations of infringement of intellectual property rights, such as patents, trademarks or copyrights. Relief, in the form of an exclusion order (import prohibition of a specific article) or a cease-and-desist order (an order prohibiting a party from importing) or both, may be granted to the successful complainant. In the complaint, SigmaTel identifies the specific patents that it believes have been infringed and requests a permanent exclusion order banning the importation of the products into the U.S. market, and also requests a cease-and-desist order to halt sale of these same products.

Actions Semi claims no infringement of SigmaTel's patents has occurred.

The trial found in favor of SigmaTel and concurred that Actions Semi infringed upon SigmaTel's patents. SigmaTel prevailed in the ITC trial, and it has protected itself within the United States, one of its prime markets, but the victory will have no effect on the Chinese or European markets.

Citroen alleges that Chinese auto manufacturer Shanghai Maple used Citroen's core chassis technology in producing a series of Shanghai Maple models. It claims that its patent on "special chassis technology" had already been filed with the world intellectual property rights organization, and had not been licensed to Shanghai Maple. Shanghai

Maple, a subsidiary of Geely Automobile, claims no knowledge of any infringement, and that the automobiles are created from its own designs.

The unlicensed use of technology apparently is not an unusual occurrence within the Chinese automotive manufacturing sector. In May 2005, General Motors Daewoo alleged that Cherry QQ copied its "Spark" sedan design, and demanded 80 million yuan (approximately US$10 million) as compensation for patent infringement. Dongfeng Honda and Toyota Auto have also sued Hebei Shuanghuan Auto and Geely Auto for similar reasons.

Zhang Zhenzhi, a deputy engineer within the China Automotive Technology & Research Center, offers a remarkable perspective:

> It's inevitable for domestic automakers to imitate other advanced technologies, no matter from other domestic companies or foreign firms. But in the future, we would be able to better our designs after getting more experience on developing our own autos.

It would appear that loss of intellectual property is expected within the nascent Chinese auto industry, and that "borrowing" of intellectual property should be considered the norm, to be expected of young companies and tolerated by more established firms.

Both Citroen and SigmaTel took all the right steps to protect their intellectual property, including filing patents. And yet, they find themselves caught up in a still-developing legal system, which some have described as a litigation quagmire, where it is almost impossible to effectively litigate patent violations.

Part II: When State Entities Target Intellectual Property

State-sponsored economic espionage and intellectual property theft are the most sophisticated and formidable threats.

Why do nation states engage in economic espionage and intellectual property theft? Primarily, to acquire technology to advance a military program, or to advance the economic competitiveness of the nation's industrial base, or simply to ensure that the major companies and contributors to the nation's GDP continue to make that contribution. How do nation states affect the acquisition of coveted intellectual property? In some instances, they engage their own law enforcement or intelligence services to surreptitiously acquire it, while in other instances, they publicly engage the owners of the intellectual property with a demand, which it believes is in the best interest of their citizens.

State-sponsored economic espionage and intellectual property theft are global issues. The threat is not unique to U.S. businesses or researchers. Many nations conduct such activities, and the interests of many nations are targeted.

When an insider is co-opted by an intelligence service, the activity becomes more sophisticated, and the ability to detect and/or defend against it is beyond the means of most corporate security mechanisms.

Ironically, sometimes the target is a company that was itself found guilty by the legal system as having instigated instances of industrial espionage, and to have stolen a competitor's intellectual property. Here are some examples.

French Intelligence
One well-documented historical case concerns Airbus's egregious attempt to bribe its way into the 1994 Saudi Arabian Airlines fleet-modernization effort by offering bribes to individuals from both the Saudi airlines and government.

During a 1994 visit to the late King Fahd, then-French Prime Minister Edouard Balladur had hoped to follow through and secure the $6 billion order for Airbus. But he was derailed when the United States provided the Saudis with U.S. National Security Agency (NSA) intercepts, which fully documented the nefarious French activity.

Without the U.S. government's intercession, the U.S. aviation industry might have been found "non-competitive."

Pierre Marion and Charles Silberzahn, former directors of the French foreign intelligence service, Direction Generale de la Securite Exterieure, have publicly stated that one of its priorities is to collect economic intelligence. Silberzahn even noted that French efforts had been successful, and theft of classified and proprietary information was a long-term government policy.

Russian Intelligence
In January 2005, Russian Prime Minister Michail Fradkov requested the leadership of Russia's internal security service, the Federal'naya Sluzhba Bezopasnosti (FSB), to increase its efforts to assist Russian commercial enterprises:

> We continue to require up-to-date information from the FSB that allows us to form a quality legal foundation and to make decisions on leveling the playing field for competition, developing businesses and creating an attractive investment climate.

While no surprise to many experts who believe that Russia has been covertly engaged in such activity since even before the Cold War, Fradkov's statement was nevertheless tantamount to a public declaration that the Russian government's intelligence and security services engage in collection and reporting activities in support of Russian commercial enterprises.

In late October 2005, the Public Safety Department of the Tokyo Police charged Vladimir Saveliev, an officer in Russia's foreign intelligence service, the Sluzhba Vneshny Razvedki (SVR), with having recruited an employee of Toshiba Discrete Semiconductor

Technology. Saveliev, who was serving undercover as a diplomat assigned to the Russian trade mission in Tokyo, is alleged to have paid this unidentified Toshiba employee 1 million yen (approximately US$9,000) for proprietary information that had military applicability and referenced semiconductor systems for electric flux control, missile guidance systems and jet fighter radars.

In early 2004, Saveliev, posing as an "Italian consultant," introduced himself to the unidentified Japanese citizen. They met nine times between September 2004 and May 2005, in Tokyo's cheap beer shops and bistros. The information was passed on to Saveliev via "smart memory cards." In June 2005, Saveliev quietly departed Japan.

Why did the SVR target Toshiba? Perhaps the information would be used to augment Russian military knowledge of technology used in an adversary's weapon systems? Perhaps it was provided to a Russian commercial or state-owned entity to jump-start research and development activities, and thus garner greater market share in the global economy? Whatever the motivations behind the theft, its implications aren't limited to Toshiba, or to the Japanese law enforcement and counterintelligence entities involved in the investigation. And although Toshiba claims the loss is minimal (the information stolen is now freely available), there are, nevertheless, long-term issues to be addressed.

Future users must consider the fact that the technology was of sufficient importance to the Russian Federation that it used its most valuable intelligence resource (an undercover intelligence officer) to acquire Toshiba's intellectual property. Remember, Saveliev was posted abroad, serving under diplomatic cover within the Russian commercial office in Tokyo. He opted to undertake a high-risk operation—using an alias persona in a city where he was well known in his true persona. Is this a case of incompetence? Why was the information of such import that it warranted the risk of discovery, especially when it appears that the information could have been obtained by Saveliev via direct overt contact? Surely, the SVR resident—i.e., the head of the SVR field entity—in Tokyo weighed the risks, or blowback, against the potential gain. The technical requirement levied by headquarters must have been extraordinarily important.

In this case, a government had a need, and its special services moved forward to fulfill the need, and used its human intelligence tools to recruit someone who had access to information of interest, i.e., an insider.

But that isn't the only covert methodology used by nation states.

Japan's Institute of Physical and Chemical Research (RIKEN)

In May 2001, the U.S. attorney in the Northern District of Ohio indicted Takashi Okamoto and Hiroaki Serizawa for the theft of intellectual property belonging to the Lerner Research Institute of the world-renowned Cleveland Clinic Foundation (CCF). According to DoJ, from January 1998 through September 1999, Serizawa and Okamoto conspired to misappropriate genetic research materials from the CCF, specifically, "deoxyribonucleic acid (DNA) and cell line reagents and constructs" developed to study "the genetic cause of and possible treatment for Alzheimer's disease." The indictments

charged that Okamoto and Serizawa then provided the stolen research to the Japanese Institute of Physical and Chemical Research (RIKEN), a research facility owned by the government of Japan. Subsequently, the indictments further allege that RIKEN, at the direction of the Japanese Ministry of Science and Technology, formed a Brain Science Institute to conduct research in the area of neuroscience (which includes the genetic cause and possible treatments for Alzheimer's).

DoJ alleged that Okamoto intended not only to purloin the CCF's research and results, but also to destroy and sabotage the DNA and cell line reagents and constructs that were left behind. Okamoto shipped the boxes of stolen materials to Kansas, where Serizawa resided, and then hand-carried them to Japan a month or so later. The investigation showed that Serizawa had been an unwitting accomplice of Okamoto, and was duped into storing the stolen research. Serizawa was convicted of making false statements to the FBI, fined $500 and placed on probation for three years. In addition, his movements were restricted, and he was ordered to perform 150 hours of community service.

The government of Japan claimed no knowledge of the activity. The DoJ continues to seek the extradition of Okamoto from Japan.

There are important questions that remain unanswered. Was Okamoto sent to the CCF to obtain a trusted position and then abscond with the intellectual property, to provide RIKEN with a baseline from which to begin its efforts on Alzheimer's disease? Or was Okamoto simply a conniving individual who saw an opportunity to propel himself to the front of the Japanese research community? And why won't the government of Japan deliver Okamoto to the United States for prosecution by the DoJ?

TsNIIMASH-Export

TsNIIMASH-Export is a state-owned Russian space technology company run by the Central Scientific Research Institute for Machine Building, and located in Korolyov, the center of Russian space community and home to the "Mission Control" for all Russian space flights.

On Oct. 25, 2005, TsNIIMASH-Export Director Igor Reshetin, along with his deputy Sergei Tverdokhklebov and Tverdokhklebov's aide, Alexander Rozhkin, were arrested by the FSB, and charged with embezzlement and the selling of secret Russian space technology to China. They were alleged to have illegally provided Russian space technology to a Chinese import/export company specializing in precision engineering. The dual-use technology apparently had applicability to Russian weapon systems, and could have potentially provided the Chinese military with valuable, secret information. The trio was also charged with embezzling approximately US$1 million of TsNIIMASH-Export's funds through multiple front companies.

Is this case an instance of state-sponsored economic espionage, personal greed and opportunism, or both? The FSB is certainly treating it as if it were state-sponsored, and has also deemed it of sufficient importance to publicize the arrest of the head of one of Russia's most respected technological concerns and link his alleged crimes to a Chinese

organization. The timing, in the midst of the successful Chinese manned space flight, invites another question: Is there a message being sent to the People's Republic of China (PRC) by the Russian Federation?

There has been no comment from the government of the PRC, nor has the identity of the Chinese company or its employees been revealed.

Coca-Cola in India

There are also, of course, overt nation-state attempts to garner intellectual property from corporate entities for a variety of reasons.

Currently, the estimated value of Coca-Cola's trademark is greater than US$70 billion. Would it be at this current value had Coca-Cola acquiesced to the government of India in 1977? Maybe, maybe not, but Coca-Cola didn't take any chances. It protected its intellectual property.

In 1977, Coca-Cola controlled the Indian cola soft-drink market, and Indira Gandhi's Congress party had just lost control of the legislature to the Janata Party. One of Ghandi's prime financial backers was the Coca-Cola bottler/distributor. In an apparent act of political revenge, new Industry Minister George Fernandes applied the Foreign Exchange Regulation Act, which at the time strictly limited foreign investment in domestic companies to 40 percent. Coca-Cola's equity investment exceeded the threshold. Fernandes told Coca-Cola officials to divest, and transfer their intellectual property, i.e., the syrup formula, to their Indian partners. The only alternative was to leave the Indian market. Coca-Cola opted to leave. It returned 12 years later, in 1989.

Fernandes continues to advocate the removal of Coca-Cola from the Indian domestic market. Would or could this happen today?

Countries can, and sometimes do, nationalize commercial concerns.

Abbott, Merck and Gilead in Brazil

In 2005, the Brazilian Ministry of Health presented Abbott Laboratories of Chicago with an ultimatum: Either you reduce the price of Kaletra (an effective AIDS/HIV drug), or we will break the patent and produce the drug ourselves. After a month of negotiation, Abbott opted to reduce the price for Kaletra, from $1.17 a pill to 63 cents a pill, effectively reducing the cost to the government of Brazil by approximately $339 million over six years. Health Minister Jose Saraiva Felipe noted:

<blockquote>With the agreement, the need for breaking the patent is suspended. The price we reached is what the national AIDS program could pay.</blockquote>

Brazil has also engaged other pharmaceuticals in discussions aimed at reducing the price of the antiretroviral drugs. It wants Merck Laboratories to allow it to produce a generic version (efavirenz) of Stocrin. It wants Gilead Laboratories to give it a discount on the

price of Viread, which costs about $7 a capsule, but is available in generic form (tenofovir) from India at less than $1 a capsule.

There is nothing covert about Brazil's effort; it is publicly stated policy. The amount of funds available in the nation's coffers to provide free AIDS/HIV antiretroviral drugs to the infected population of Brazil is defined. Brazil has opted to engage in a frontal attack on the pharmaceutical industry. Some call this tactic no more than industrial blackmail; others call it socialism at its best.

Roche in India

The avian flu outbreak in the Far East has created a fear of a global pandemic, and governments around the globe are demanding product.

In India, Dr. Ashwani Kumar, drug controller general of India, has noted that Roche Holdings of Switzerland does not have a Tamiflu product patent in India, and therefore, India does not recognize the international patent license, which Roche does possess. Kumar has invited Indian companies to file license applications with the government to produce a generic form of Tamiflu.

Although invited to break the patent, two Indian biopharmaceutical manufacturers, Cipla and Ranbaxy, are reported to be working with Roche to license Tamiflu, and then develop the generic Tamiflu (oseltamivir) without resorting to breaking the patent. In addition, Roche has approached a number of other drug manufacturers to discuss licensing Tamiflu, which Roche itself obtained via exclusive license agreement from Gilead Laboratories in 1996. While there is no guarantee any of these discussions will lead to a licensing agreement, Roche is hopeful that such will be possible, and that an equitable relationship will be sought to address the emergency need for Tamiflu.

In 2003, the World Trade Organization agreed to allow governments to override patents during national health crises, but as of October 2005, no member state had invoked the clause with respect to the avian flu.

Despite requests from a number of countries to allow generic production of the drug, Roche is standing firm on its unwillingness to relinquish the patent, which is protected into 2016, and demanding a licensing fee. It stood to earn approximately $1 billion from Tamiflu sales in 2005. Roche spokeswoman Martina Rupp defends the position: "*Since we have been making this drug for the last 10 years, it would be best for countries to enter into discussion with us.*" Rupp noted that the 10-step process of manufacturing Tamiflu is complex.

What will prevent a nation from extending the concept that worked so well with pharmaceutical manufacturers to other sectors? The precedent has been set. The World Intellectual Property Organization must address this issue; otherwise, the basic incentive to invent, create and innovate will be dealt a severe blow.

Where Does It End?

Attacks on intellectual property, whether covert or overt, have profound consequences and sweeping implications.

A lawless world, in which government intelligence services routinely insinuate themselves into competition between commercial enterprises in the private sector, and internationally recognized patents can be unilaterally disregarded by governments, whether motivated by the social good or geopolitical ambition, will certainly not contribute to the establishment of peace and prosperity for all nations. Nor does a lawless world, in which private-sector corporations can move freely and globally, without restraint, conscience, accountability or international oversight, lead us any closer to that lofty goal.

The United States has no program or policy to provide economic or industrial competitive intelligence to U.S. businesses. The country's economic policy precludes it.

U.S. governmental efforts are focused on the protection of intellectual property owned by U.S. persons or U.S. corporate entities, and keeping the economic pitch level as U.S. corporations compete within the global marketplace.

Discussion points have been made both for and against allowing U.S. governmental agencies and departments, such as the Department of State, Department of Commerce, the National Intelligence Director and the various agencies that make up the U.S. intelligence community, to devote resources and provide economic intelligence to U.S. persons or corporations.

The best approach is to maintain the current policy, except when U.S. corporate interests are specifically targeted by a foreign government-sponsored activity, or when the economic playing field must be leveled. The U.S. government's abilities should be dedicated to national security issues. No U.S. intelligence officer should put his or her life in jeopardy to improve shareholder value. The ultimate sacrifice should be reserved only for the nation's security.

According to a study published by USA for Innovation (www.usaforinnovation.org) in late October 2005, intellectual property in the United States alone carried the value of US$5 trillion to $5.5 trillion, equivalent to 45 percent of the gross domestic product, far larger than the GDP of any other nation. The intellectual property retained by U.S. companies is central to U.S. economic security. This study also indicates that a direct correlation exists between the level of a nation state's protection of foreign-owned intellectual property and the level of foreign investment in that same country—i.e., where the state offers increased protection of the investor's intellectual property, investors increase their investment in the nation's economy.

The United States is under economic attack, according to the National Counterintelligence Executive's report to U.S. Congress in February 2005. The report goes into some depth in identifying the types of foreign entities conducting industrial and economic espionage, the kind of information targeted by these foreign entities, and which

foreign entities are attempting to acquire sensitive U.S. technology (either classified or proprietary)—be they private or governmental.

The report indicates that individuals from almost 100 separate countries attempted to acquire sensitive U.S. information. Characterizing the role of the state-supported intelligence collection effort against U.S. technology and intellectual property, it states: *"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."*

The report identified several dual-use areas as being targeted, including:

- Information systems
- Military production processes and communication systems
- Aeronautics
- Electronics
- Armaments
- Energy materials

The report laments the difficulty of tracking the foreign targeting of purely civilian technologies, and highlights U.S. organizations' reluctance to share information. Such reluctance, it opines, is due to their not wishing to highlight their losses, because such revelations could have a deleterious effect on "*investor and consumer confidence and stock prices*."

Commercial technologies identified as stolen by foreign entities included:

- Semiconductor production processes
- Computer microprocessors
- Software
- Proprietary information
- Chemical formulas

The U.S. counterintelligence community expects no decline in foreign intelligence activities, and also notes that stemming the flow of information will become even more difficult. The report specifically mentions the challenge of isolating trade secrets from foreign managers and employees and U.S. companies' increasing practice of placing their research and development centers in foreign environs.

U.S. corporations must take appropriate steps, on their own initiative, and incorporate security procedures in order to effectively protect their intellectual property against the efforts of foreign governments eager to obtain it.

Part III: When Counterfeiters, Pirates and Organized Crime Target Products

The counterfeiting and piracy of products, activities often sponsored by organized criminals, make up the most insidious intellectual property threat, and certainly the most pervasive threat to the global economy as a whole.

The U.S. Chamber of Commerce estimates that counterfeit and pirated products account for 5 percent to 7 percent of the global economy, and results in the loss of more than 750,000 jobs and approximately $250 billion in sales to the United States alone.

Via trade missions and educational programs, the chamber has directed its efforts at China, Brazil, South Korea and Russia, and toward the goal of encouraging enhanced enforcement of intellectual property protection laws within these countries. In addition, it offers an intellectual property protection toolkit for each of these countries. And in 2005, working with various law enforcement entities, the chamber initiated Strategy Targeting Organized Piracy (STOP).

In the United Kingdom, the Alliance Against IP Theft has produced a 40-page primer, *Proving the Connection: Links Between Intellectual Property Theft and Organised Crime*, detailing the deleterious effect on the U.K. economy, and the clear and unambiguous involvement of organized criminal elements. It cites case studies identifying organizations with points of origin in Russia, South Asia, China and Ireland, which serve as points of origin for either the financial backing to achieve the manufacture, distribution and sale of pirated and counterfeit goods in the United Kingdom, or as points of origin for the counterfeit goods themselves. The alliance puts the value of these illegal items at more than 9 billion pounds.

Software

According to a December 2005 global study commissioned by the Business Software Alliance, piracy rates in 50 countries have increased over the prior year. Leading the list is Vietnam, where it is estimated that 92 percent of all software purchased is pirated. But while the top 20 countries with a high rate of software piracy include mostly developing nations, the list also includes China with a rate of 90 percent and Russia not far behind at 87 percent. By comparison, the United States has the lowest rate at 21 percent. The study opines that a 10-point drop in piracy in Asia-Pacific alone would generate $135 billion worth of additional economic growth and create approximately 2 million new jobs.

Law enforcement is the critical issue, and the biggest problem. For example, in October 2005, two people were arrested in Cebu City, Philippines, for attempting to sell pirated software valued at approximately 9 million Filipino pesos (more than US$160,000). If convicted, they face fines from 50,000 to 1.5 million Filipino pesos (approximately US$900 to $25,000) and prison terms from one to nine years. However, according to the Filipino press, no one has ever been convicted of software piracy in the Philippines. It appears that these are token arrests and enforcement efforts, and are not directed at the large wholesale piracy efforts.

Technology

Counterfeiting isn’t limited to software, of course. Samsung, for example, has been repeatedly targeted. Crimes perpetrated against the Korean technology manufacturer range from outright theft of its intellectual property to the counterfeiting of its cutting-edge product lines.

In November 2005, four people, who were all current or former Samsung employees, pilfered blueprints and other documents related to a new mobile phone design. They were caught by the National Intelligence Service (NIS), South Korea's counterespionage organization, which discovered the group attempting to deliver the files to Chinese mobile phone manufacturers. (Note that the Korean NIS exercises its counterespionage capabilities within the economic espionage milieu and in support of Korea's industrial base.)

According to Samsung, its investment in the design project was 25 billion won (approximately US$25 million). If the quartet of thieves had been successful, Samsung could have taken a market hit of approximately 500 million won (US$500,000) in the handset market. It also stood to lose almost 8.8 trillion won (approximately US$8.8 billion) worth of intellectual property on its entire line of technology products, which were included in the data trove. What company could withstand a fiscal loss valued at more than $8 billion due to blueprints and documents being stolen?

One of the perpetrators was discovered sharing approximately four gigabytes of computer files, including documents, blueprints, program source code and circuit diagrams for mobile phones. This individual used multiple technological avenues to successfully transfer data to his co-conspirators outside of Samsung, such as DVDs, e-mail and wireless connectivity between laptops. Of course, Samsung had a "policy" in place, which prohibits employees from sharing data outside the company, or retaining or copying such data for personal retention. So what? Policies without enforcement programs are relatively meaningless.

A study conducted by Samsung's own Economic Research Institute indicates that 39 percent of all technology stolen from Korea is destined for China. Korean manufacturers of mobile phones and other electronic devices, such as MP3 players, say that approximately 70 percent of LG Electronics and Samsung products available in the Chinese marketplace are counterfeit products.

Working closely with the Chinese law enforcement entities in efforts to thwart counterfeit activity, Marksman Consultants, a Hong Kong-based company, has conducted surveys and investigations. "One big problem," according to Joseph Tsang, chairman of Marksman, is that "too many scammers have ties to local officials, who see counterfeit operations as a major source of employment and pillars of the local economy." According to Tsang, two or three of their raids have failed because of local protection.

Shoes and Apparel

Counterfeit shoes are commonplace in the open markets of Southeast Asia. Adidas, the German sports clothing conglomerate, recently filed a lawsuit against three separate Chinese companies for intellectual property violations. Adidas has requested 3 million yuan (approximately US$370,000) in compensation from the three companies for violating its logo and trademarks.

The apparel and fashion goods industries have also proven to be juicy targets. In early November 2005, the assistant U.S. attorney for the District of Massachusetts, the U.S. Immigration and Customs Enforcement in New England (ICE) and the U.S. Internal Revenue Service announced the arrest and indictment of four people charged with trafficking in more than US$1.4 million worth of counterfeit goods. The 10-count indictment details how the four people used 13 separate self-storage units within a storage facility as their base of operations. (Ten of the units were for storage, two were showrooms, and one was the manufacturing facility.)

When raided, the units contained: 12,231 counterfeit handbags, 7,651 counterfeit wallets, more than 17,000 generic handbags and wallets, and counterfeit labels and medallions in sufficient quantity to turn more than 50,000 generic handbags and wallets into copies of the "originals." Trademarked brands that were "copied" included Louis Vuitton, Kate Spade, Prada, Gucci, Fendi, Burberry and Coach, and those of other manufacturers. Other items contained in the storage units included scarves, belts, umbrellas, sunglasses, duffle bags, hats, visors, garment bags, coats, shoes, necklaces, bracelets, rings and earrings bearing counterfeit marks. The indictment places the value of the counterfeit goods at approximately $1.4 million and $6 million had the goods been authentic.

The sales methodology used by this group of counterfeiters, according to the indictment, was to sell the items at flea markets or "purse parties." Indeed, it is alleged that they held more than 230 purse parties throughout Massachusetts.

According to an ICE statement:

> The public needs to know that when they buy a counterfeit purse at a house party or on the street, their dollars are ultimately helping to finance large-scale counterfeiting organizations. And every time they buy a knock-off purse, they are contributing to legitimate companies losing billions of dollars in revenue to counterfeiting every year.

Entertainment

In November 2005, a judge in Hong Kong sentenced Chan Nai-ming to three months in jail for the copying and distribution of three motion pictures via the Internet. Chan operated under the Internet alias "Big Crook," utilized BitTorrent software to conduct the file sharing, and apparently did not charge for the films.

The Chan case was the first in Hong Kong to result in a jail sentence for the online piracy of motion pictures. Customs investigators determined that 30 to 40 individuals accessed Chan's computer to obtain illicit copies. The fact that Chan did not charge for the films was not found to be material.

Meanwhile, Antipiratbyran, the Swedish anti-piracy group, was disciplined by the country's Data Inspection Board for breaking privacy data rules in its hunt for illegal file sharers. In its exuberance to locate and identify individuals who were illegally sharing music and film files over the Internet, it hired a paid informant within Bahnof, a Swedish

ISP, to provide the IP addresses of "file sharers" within the network. The Data Inspection Board noted that an individual's IP address is considered private, and the manner in which the information was collected illegal.

In August 2005, the Motion Picture Association of America (MPAA) declared Internet-driven film piracy losses to be approximately $1.9 billion, and that the overall piracy of films in other formats was estimated to be $3.5 billion.

And yet, instead of expending its energy searching out wholesale pirates, the MPAA, on behalf of the major studios, filed 286 lawsuits against individuals whose names were provided by 30 BitTorrent site operators who were shut down earlier in 2005. These prosecutions, although appropriate, are insignificant. Of course, the suits against individuals aren't difficult to win, since most individuals don't have the fiscal resources to compete with the MPAA or the motion picture industry itself. But it would certainly be more effective for the MPAA to invest its investigative funds in identifying those organizations with robust infrastructure producing thousands of copies.

According to the DOPIP Security Counterfeit Intelligence Report, in October 2005 alone, there were more than 341 separate incidents involving goods valued at more than U.S. $1 billion, and involving more than 54 separate countries. Not surprisingly, the top 10 brands counterfeited included Adidas, Nike, Louis Vuitton, Microsoft, Chanel, Gucci, Prada, Fendi, Manchester United and Puma.

The report also highlighted the evidence of links between copyright and trademark infringements and more serious crimes. In 37 percent of the cases, counterfeiters were involved in drug trafficking; in 20 percent of cases, they carried weapons; in 11 percent they committed other frauds, and in 26 percent they carried out other crimes such as assault, extortion, murder, theft, immigration violations, money laundering, identity theft and robbery. Increasingly, violent criminals are becoming involved because the profit margins are higher, and penalties and chances of being arrested are relatively low.

Conclusion

Today, the U.S. economy faces many threats, including spiraling energy costs, corporate governance abuses, huge federal deficits, foreign ownership of the national debt, the loss of jobs to offshore outsourcing and the impact of disasters (whether terrorist related or environmental). And of course, there is the looming possibility of a bird flu pandemic or other global health emergency that could result in the closing of borders, the interruption of business, the cessation of travel and the deaths of many thousands.

But as you can see from this overview, there is another threat, difficult to quantify or even detect, one that has not yet grabbed the headlines or captured the imagination, and yet is relentlessly and efficiently looting, pillaging and plundering the U.S. and global economies of the magic ingredient—i.e., trade secrets.

Economic espionage is as real a threat as terrorism or global warming. But it is subtle, insidious and stealthy. Even if the United States finds the will to come to grips with the

many threats it faces, this silent, invisible hemorrhaging of intellectual know-how and trade secrets could deliver the death blow to our pre-eminent place in the global economic world before we even wake up to the magnitude of the danger.

According to the U.S. Commerce Department, intellectual property theft is estimated to top $250 billion annually (equivalent to the impact of another four Katrinas), and also costs the United States approximately 750,000 jobs, while the International Chamber of Commerce puts the global fiscal loss at more than $600 billion a year. But both estimates appear to be woefully underestimated; by some other estimates, there was over $251 billion worth of intellectual property lost or illegal property seized in August 2005 alone.

The United States, like other great nations, stands on three legs: military power, political power and economic power. Arguably, economic power is the most vital of the three. Without economic power, the political elite would be bereft of the consultants and lawyers who insulate it; it would have nothing to bargain with at the geopolitical roulette table, and it would lack the bureaucratic muscle to impose its will domestically. Without economic power, the military would be unable to deploy advanced weapons systems, spy on its enemies from space, span the globe with bases or even raise an army.

Secrets are the magic ingredient of power. When state secrets—i.e., political and military secrets—are stolen, governments fall and wars are lost, people are disgraced and people die. When trade secrets, such as scientific or engineering secrets, are stolen, corporations lose their competitive edge, small entities cease to exist, and whole sectors of the economy weaken and fall behind in the global marketplace; people lose their livelihood and their children's futures.

In other words, the United States could win the war on terrorism, overcome the challenges of global warming, balance the federal budget, strengthen the United Nations, end global armed conflict and restore our edge in science and engineering, and still end up behind China, India, Japan, Russia or Brazil in several vital sectors of the economy, and at a serious, if not fatal, disadvantage within the global marketplace.

The threats of economic espionage, intellectual property theft, counterfeiting and piracy are global, dangerous and increasingly common.

It is within your power to decide for yourself if your enterprise is going to be a hard target or soft target. The time for action is now. You can be prepared.

Preparation Tips

Remember, it is important to invest in protective measures commensurate to the value of the asset being protected. Here are some recommendations for a comprehensive program:

Organization

Where security reports within an organization is perhaps the most vital issue of all. Consider appointing a chief security officer, who reports to either the chief executive office or the chief financial officer. This person should hold the reins of personnel

security, physical security and information security, and should not be a stranger to the board room.

Awareness and Education
Educate your workforce on an ongoing basis about the threats of economic espionage, intellectual property theft, counterfeiting and piracy. Help them understand your expectation that they will protect the enterprise's intellectual property and, by extension, their own livelihood. Provide general education for the entire workforce, and specialized education for executives, managers, technical personnel, etc.

Personnel Security
Implement a "Personnel Security" program that includes both background investigations and termination procedures. You need policies that establish checks and balances, and you need to enforce them. Know the people you are going to hire. Don't lose touch with them while they work for you. Consciously manage the termination process if and when they leave the enterprise.

Information Security
Recruit certified information security professionals (e.g., CISSP, CISM, etc.) Adopt best practices, and establish a baseline. Utilize appropriate information security technologies, such as firewalls, intrusion detection, encryption, strong authentication devices, etc. Pay attention to data retention and data destruction as well as data access.

Physical Security
Do not overlook the "Duh" factor. It is pointless to invest in information security, or commit to background investigations, if agents of an unscrupulous competitor or a foreign government can simply walk away with what they covet.

Intelligence
You need both business and security intelligence. Know your competition, your partners and your customers. Research the market environment. Keep abreast of the latest trends in hacking, organized crime, financial fraud and state-sponsored economic espionage. You can outsource this expertise. But someone must be looking at both streams of intelligence, with the particulars of your enterprise in mind.

Industry Outreach
Actively participate in industry working groups appropriate to your sector and environment. Talk with your peers about the types of attacks or threats they are encountering.

Government Liaison
Leverage your tax dollars. Avail yourself of threat information from law enforcement, foreign ministries, elected officials, regulatory and trade organizations in your enterprise's country, and in those countries where you conduct business.

Legal Strategies

Realize that even when right is on your side, a market may be lost to you, and protecting a portion of the global market is sometimes a viable survival strategy. Litigation is not the solution; it is confirmation that intellectual property theft has occurred. Work to protect your intellectual property and avoid the costs associated with litigation. Don't let a small legal mind make decisions about big legal issues. Get expert legal advice on intellectual property issues.

In sum, your security is in your hands. Employees tend to apply effort and intellect to the issue in portions commensurate with management attention to the topic of intellectual property protection. Employees line up smartly behind the leader providing direction, guidance and support. Providing that leadership is essential to your own continued economic viability in the global economy of the 21st century.

Christopher Burgess has recently retired as an officer of the U.S. Central Intelligence Agency, with 30 years of experience in the clandestine services. He can be reached via e-mail: cburgess@att.net. Richard Power (www.wordsofpower.net) is an internationally recognized authority on cybercrime, information age espionage and other threats. He can be reached via e-mail: richardpower@wordsofpower.net.

NOTE: Portions of this study were reviewed, and cleared without objection, by the Publication Review Board of the U.S. Central Intelligence Agency.