The Attack on America's Intellectual Property

Espionage after the Cold War

by S. Eugene Poteat, *South Carolina Gamma '57*

ENGINEERING STUDENTS about to graduate naturally have a tough time concentrating on their final exams. No wonder, they are often preoccupied with dreams of that exciting new job, innovating, filing their first patent application, and of the wealth and good life that can come from innovation and the fruits of their own labor. New engineers need to be reminded that within the very first year after the birth of our new nation, the Congress passed the laws that established our patent system and set up the U.S. Patent Office. By this action, the Congress was making it clear that a viable patent system and the protection of individual's intellectual property were the key to the new nation's future economic health and wealth. The President, the Secretary of State, the Attorney General, and the Secretary of War all signed the early patents. The implications here were that ownership and protection of an individual's intellectual property—and the right to profit from it—are civil rights, the theft of intellectual property was prosecutable and could affect international relations, and we were willing to fight over foreign infringement. Alexander Hamilton would be the driver who set up the national banking system that the new corporate system needed to turn patents into profits—another key to a strong economy.

Our upstart young nation was known throughout the world at the time as the "great experiment," and the rest of the world waited for the inevitable failure of the experiment. Ours was the first nation in which the individual had certain inalienable rights, based on recognition of the existence of a Natural Law—a law higher than any that could be established by any other authority—through which citizens could choose their own leaders and expect human rights and economic justice. Our long-standing patent laws, which have served us well, have recently been changed—and in radical, questionable ways.

INDUSTRIAL ESPIONAGE

Espionage, or spying on one's enemies, also known as the world's second-oldest profession, has been around since the dawn of time. Spying on one's friends or competitors, however, usually means industrial espionage. Lowell, MA, is named after Francis Cabot Lowell, a Harvard graduate and America's first premier industrial spy. In 1800, England's economic crown jewels were its new water-powered Cartwright looms, the engines that powered the world's première textile industry, protected by strong British patent and export laws and fed by the raw material and labor of the *Colonies*. Using the cover story that he was in Scotland for his health, Lowell visited several mills normally closed to visitors, and with his photographic memory, was able to skirt British customs inspectors searching for stolen plans and blueprints. Back home, Lowell built his first textile plant in Waltham, and America was well on its way into the industrial revolution.

Our founding fathers were more than right. Now, more than two centuries later, America is the world's strongest economic and sole military superpower, principally because of the strength of its economy, and it has 10 times more intellectual property than the rest of the industrialized world combined. Since the collapse of the Soviet Union and the end of the Cold War, the power of a nation is again judged more by the strength of its economy than by its military power. At the same time, there has also been a shift from classical espionage, which targeted nations' military technology, plans, and intentions, to economic espionage, targeting others' economic and commercial research and development and intellectual property. The United States, as the world's strongest economy and also the most technically advanced, is the center of the world's research and development and, therefore, the principal target of this new wave of economic espionage. Since the end of the Cold War, however, there has been a virtual feeding frenzy of economic and industrial espionage by other nations—both friend and foe alike—to steal America's trade secrets and intellectual property for economic and competitive advantage. While classical wartime espionage between adversaries was accepted as necessary for a nation's defense, peacetime economic espionage is coming to be viewed as ordinary theft of intellectual property that costs people's jobs. The magnitude and nature of this espionage is also placing new strains on the conduct of diplomacy and statecraft, especially among Western nations and former allies.

Ours was the first nation in which the individual had certain inalienable rights, based on recognition of the existence of a Natural Law—a law higher than any that could be established by any other authority . . . .

COLD WAR ESPIONAGE

When looking at the morass and moral and economic decadence into which the former Soviet Union seems permanently mired, one cannot help but wonder just what accounted for its meteoric rise to the largest military power in history. The answer, however, is so simple as to be unbelievable to many Western scholars who for decades had ac

cepted socialism and its variant communism, even with its unworkable economy, as a legitimate alternative to Western democracy and our free enterprise system. The answer is that the Soviet intelligence services successfully stole virtually all the West's military and defense technology secrets, thereby saving the time and enormous cost of research and development. They then spent the bulk of their GNP on building and fielding weapons in large inefficient government-owned factories, while ignoring the building of a strong private-sector economy to fill the needs and wants of their people. Many of us remember the crowds of Russians queued up during the height of their world-power status to buy their daily bread from government-owned bakeries. Stalin's own words might best explain the mission of the Soviet Union's intelligence services, the KGB and the GRU (military intelligence), when he said that he wanted only the secrets locked in the American safes. In carrying out Stalin's orders, Soviet intelligence was incredibly successful. Their espionage successes helped create one of history's strangest paradoxes, the turning of a third-world nation into a superpower that challenged the West both militarily and technologically for half a century. The GRU stole America's greatest secret of World War II, the atomic bomb, in real-time, with the result that Stalin knew of the bomb's existence even before President Truman. The Soviets were then able to duplicate the bomb in an incredibly short time without the need for extensive research, development, and testing. Stalin then went on to match and surpass the West in nuclear weaponry, thus forcing the West to grant a third-world country world-power status and recognition—a status the Soviets could never have achieved otherwise. These intelligence victories continued until recent times with the KGB stealing the U.S. Patriot anti-missile technology on which the Soviets based their modern version, the S-300, which it now exports to any buyer for hard currency.

During the 1970s and 1980s, a Soviet colonel, working undercover for the French intelligence service DGSE, brought out the details of an incredibly successful Soviet intelligence operation. The Soviet KGB's "Line X" unit, working mainly through the East German STASI intelligence service, had succeeded in stealing practically every technical secret in American and NATO arsenals. The Soviet goal was to close the gap with the West's lead in computers, communications, and information technology. Unfortunately, the hapless colonel, known as "Farewell," was eventually caught and executed—but not before his information was used to plug the flood of secrets to the Soviets, thus hampering and stalling their efforts to match the West's technical superiority.

THE NEW WORLD ORDER

In our global economy, economic competition has replaced military confrontation in world affairs. America's intellectual property and industrial and trade secrets are not only the bases of our strong economy and military, but also the strength of our economic competitiveness. Their loss through economic espionage to foreign governments poses a serious threat to the future of our nation. Economic espionage is a relatively low-risk enterprise with extremely high payoffs and few consequences, even when offenders are caught.

The GRU stole America's greatest secret of World War II, the atomic bomb, in real-time, with the result that Stalin knew of the bomb's existence even before President Truman.

There is, nonetheless, a widely held perception that the end of the Cold War means that (except for a few scattered terrorism and drug problems) we no longer face a truly serious foreign threat to our national security, and that these past threats have turned into nothing more than normal economic competition or business as usual. On April 27, 1997, President William J. Clinton stated that the practice of economic espionage is normal and goes on all the time. He then cited the cases of Israel and Greece trying to influence American policy as being OK—shortly after several other "friendly" countries were caught engaging in both military and economic espionage against the U.S.

The loss of our advanced technology to foreign governments through this aggressive economic espionage means not only loss of jobs and wealth, but a weakened economic base, loss of political clout, loss of technological superiority, and even disadvantaged armed forces. In former Secretary of State Warren Christopher's words, ". . . in the post-Cold War world, our national security is inseparable from our economic security." Safeguarding our sensitive proprietary technology and economic information should now receive the same priority and attention as do our defense and military secrets.

Russian, French, German, Japanese, Israeli, South Korean, and many other foreign intelligence services and foreign private companies are aggressively targeting Americans, firms, industries, and our governmental and university laboratories to steal trade secrets and other scientific and technical information and products in order to provide

their own economic and industrial sectors with competitive advantages—with military and defense theft receding into second place. The Pharmaceutical Research and Manufacturers of America states that India, Brazil, Argentina, and Turkey are the greatest abusers of United States pharmaceutical patents.

The intelligence services of other countries, including those in continental Europe, routinely steal our trade secrets and pass them to their own companies for competitive advantage over rival American companies. Many of these same countries also legally use bribes to challenge American competitors for lucrative foreign sales—the bribes are often being tax deductible. Our Foreign Corrupt Practices Act makes such practices illegal for U.S. companies. American intelligence services—yes, the CIA—have pointed this out to the Congress. These allies-now-competitors have countered that the CIA and the National Security Agency (NSA), with the help of Britain, are using a network of satellites, called Echelon, to spy on European companies by intercepting their companies' telephone, fax, and e-mail messages and passing them to their American competitors. When pressed, and reminded of the Aspin Brown commission report that states, "U.S. intelligence agencies are not tasked to engage in 'industrial espionage,' i.e., obtaining trade secrets for the benefit of U.S. companies," these European governments routinely back off. Our intelligence services do, by the way, spy on European and allied countries to expose their companies' use of bribes to win a sale over American competition or to sell dual-use technologies that can also be used to manufacture weapons of mass destruction to nations not friendly to the U.S.

America is the prime intelligence target of all spying nations, exceeding 20 in number, both friendly and unfriendly, because of our advanced technology and the ease with which our open society can be mined for secrets, both legally and illegally, using the internet, exhibits, conventions, seminars, and promises from large foreign corporations of possible acquisitions of small American companies. Open-source intelligence collection in America is easy and yields vast amounts of highly technical secrets readily obtained from eager, naïve, or careless businessmen, engineers, and scientists either unfamiliar with the threat or without regard for the consequences of their actions. American business's preoccupation with short-term profits, rather than long-term national interest, further eases the industrial spy's task. More disconcerting to Americans is the foreign intelligence services' use of ethnicity in identifying and recruiting potential U.S. agents for espionage.

The list of economic and technical information sought by foreign intelligence services is extensive and includes such critical technologies as aeronautics, energy, chemical, biology, directed energy, electronics, guidance and navigation, information and communications, manufacturing, materials, nuclear, sensors and lasers, signature control, space systems, weapons effects, and countermeasures. According to the White House Office of Science and Technology, economic espionage is costing U.S. companies an estimated $100 billion a year in lost sales. According to the FBI's national counterintelligence center, 74 U.S. corporations reported more than 400 incidents of suspected foreign targeting against their businesses last year, and others go unreported for fear the publicity would affect stock values.

The loss or compromise of our proprietary technology in 1996 has also been estimated by the American Society for Industrial Security (ASIS) to be in excess of $2 billion a month. ASIS estimates for 1997 doubled this figure. Industrial and economic espionage against the United States is rampant and tantamount to a feeding frenzy by determined foreign intelligence services. These services are aware of our cultural characteristics—openness, trust of everyone, lenience, and unwillingness to offend others at all costs.

There are a large number of counterintelligence and security organizations, services, boards, centers, and programs to deal with this industrial and economic espionage, primarily with counterintelligence organizations and law enforcement. The FBI is the central agency for collecting, analyzing, and investigating foreign threats and enforcing the law. The FBI's awareness of national security issues and response program provides the interface with the U.S. corporate community to communicate and educate the industry to the foreign espionage threat. Other key players supporting American industry are the state department's defense information counter espionage program and the National Counterintelligence Center—to list but a few.

The Economic Espionage Act of 1996 makes economic espionage a punishable crime, using much the same language as the Espionage Act of 1916 which made the stealing of national defense information a crime. Section 809 of the act requires the President to report to the Congress on foreign industrial espionage targeted against U.S. industries. This act provides the first legal tool to effectively counter this espionage threat by prosecuting the culprits. In 1997, the President also signed the new Internet Law, the no electronic-theft act intended to help software companies in their battle against modern hackers and crackers infringing upon their copyrighted materials.

CHANGES IN FOREIGN ESPIONAGE

The Russian and Chinese intelligence services have seen and understood the change from military competition to worldwide economic competition, have completed the shift in their intelligence collection requirements accordingly, and have now become masters of economic and industrial espionage. This shift to economic and industrial espionage is also reflected by the Russian and Chinese military planners who have stated that in the future they must be prepared to engage in both offensive and defensive information operations and economic warfare. In the meantime and until Russia is back on its feet, they will rely on their continuing development of newer, modern weapons systems, such as the SU-34 bomber, MiG-31 fighter, multi-purpose nuclear submarine launched missile, and the land-mobile SS-29 ICBM, as their place-holders at the super-power table. Russian intelligence is attacking other advanced countries as well. According to Japan's largest daily newspaper, Japanese authorities revealed on February 3, 1998, that Russian agents have conducted extensive industrial and economic espionage to collect technical information during the last decade. Similar stories have appeared in South Korea and all other countries with advanced technolgy commercial industries.

Japanese see business as *war* and have a well-established and successful economic espionage campaign to acquire America's intellectual property and technical know-how. Their methods are usually not in the classical espionage (illegal) style, since they do not operate intelligence services in the same manner as the rest of the world. Instead, their Ministry of International Trade Industry (MITI) and

its JETRO, MITI's technology information collection service, operate effectively as such. Their approach to acquisition of our science and technology usually applies legal, rather than illegal, methods. They insinuate themselves into the heart of America's research and development establishments. They have built R&D laboratories adjacent to our universities and other research laboratories, made large monetary contributions to the universities, then hired their students, staff, and disgruntled workers from company laboratories—a process called "tunneling." These laboratories also hire job switchers and American scientists as consultants, just long enough to drain their brains. In pursuit of a microwave lamp device to instantly dry inks, invented by Donald M. Spero *[New York Delta '62]* of Fusion Systems in Maryland, Mitsubishi Electric bought one and reverse engineered it. The firm next filed for 257 patents of its own that duplicated the device. Mitsubishi then hired powerful Washington lawyers and lobbyists, found support in the congress and senate to counter Spero's patents, and eventually acquired the device on its terms.

China's Guojia Anquan Bu intelligence service uses both legal and illegal methods for defense and economic espionage. This group appears to have successfully stolen and duplicated our latest and smallest nuclear warheads. It took advantage of hard times at McDonnell Douglas by buying a complete factory for computer-controlled machine tools—duel-use technology that China is known to be exporting to third-world countries inimical to the United States.

Two major American aerospace companies have been recently charged with providing China with details of launch satellites that are said to enhance their ICBMs that could be targeted at the U.S. The FBI estimates there are more than 800 American companies that are actually Chinese *fronts*. Our wide trade deficit with China, along with our push to set up technical joint ventures in China and our universities' training their students in science and engineering, is tantamount to our subsidizing the modernization and buildup of their military. The Chinese government recently paid $3.5 million for a Washington mansion for their education counselor, Wei Liqing, whose job has been described as *overseeing* the thousands of Chinese students and scholars in this country.

France makes no bones about their engaging in economic espionage against America and giving the products to their companies to improve their commercial competitive positions. They successfully placed spies in IBM, Corning Inc., and Texas Instruments. After the FBI captured many of the French spies, and diplomatic protests, the French apologized, but the spying did not stop. There is one well-known story of the French having bugged the business-class seats on Air France. In another case, the French government-owned company, Machines Bull, sued Texas Instruments over a patent infringement. While Texas Instruments was willing to pay, it then discovered that the French patent was actually based on a Texas Instrument design stolen earlier by a French spy. According to James Woolsey, CIA director in 1993, American intelligence learned that the French had bribed the Saudi Arabians in a $5 billion deal to sell airliners. The Boeing Corporation obtained the business only after American diplomatic protests.

Israel, an ally that owes its very existence to America, was caught in a high profile case when its paid agent, Jonathan Pollard, was arrested and jailed for passing thousands of highly classified intelligence documents to Israeli intelligence. *Lakam* is an Israeli-government intelligence organization whose sole mission is to acquire U.S. technology. Its economic espionage, however, receives little publicity. In 1986 the Israelis signed a $45 million contract to buy specialized aerial cameras from Recon/Optical in Illinois. The Israelis insisted their engineers be on-site in Recon/Optical during construction of the cameras. When caught taking blueprints and technical documents out of the factory, the Israelis were sent home—but not before enough information had been passed to an Israeli competitor which then undercut Recon/Optical's market. The firm eventually had to lay off 800 employees.

The U.S. model for fair economic competition has always been to go for the level playing field—a model which is considered naïve and rather quaint by our allies and competitors and which only offers increased opportunities for espionage. America's economic competitors well understand the increasing dependence of the U.S. economy and infrastructure on computers, communications and information technology, and that this means increased vulnerabilities-and opportunities for information operations and warfare, i.e., on-line espionage.

S. Eugene (Gene) Poteat earned his B.S. in electrical engineering from the Citadel in 1957. He began his career in research and development at the Bell Telephone Laboratories, working in New Jersey and Cape Canaveral, FL. He joined the CIA in 1960, and his career spanned more than 30 years in technical intelligence. He served abroad in London and Scandinavia.

Upon retiring as a senior executive, Gene founded the Petite Research Group in McLean, VA. He has done graduate study in foreign policy, national security, and intelligence at Cambridge University and the Institute of World Politics in Washington, DC. He now writes and lectures on these subjects. Gene is the president of the Association of Former Intelligence Officers.

ENTER S-1948

Clearly our patent laws, along with our free enterprise system and the rule of law, account for the strongest economy the world has ever known. It was the superiority of our economy and high-tech industry that prevailed in the Cold War, more than the superiority of our military and its nuclear weapons. Yes, our defense and intelligence establishments held the Soviet's in check, but it was the Soviet's weak, centrally controlled economy, once denied unlimited access to Western technology and Western financial credits, that led to the inevitable collapse of the Soviet Union. There is an old saying among engineers—"If it ain't broke, don't fix it." So, why have America's patent laws been radically changed with little fanfare or publicity? S-1948, with the backing of the United Nation's World Intellectual Property Organization, became law in 1999, creating a separate government patent and trademark office—with an advisory board that could include representatives of foreign corporations.

In light of these examples of foreign economic espionage and the disregard for America's intellectual property, there should be no question about where others stand or what their views of our patent system are, all of which could lead to problems for Americans when filing for new patents. In the former Soviet Union, for example, the state owned all intellectual property. Today, Russia, which is struggling and experimenting with a capitalist economy and where the unimaginable is routine, has come up with its own version of patent protection. According to the *Washington Post,* a Russian company won a patent last year from its new official patent office, Rospatent, for *glass containers*—bottles, as we would call them, that have been around for thousands of years! The company then sent letters to Russian breweries informing them they owed the company royalties, since it now owned the patent. Rospatent has also received applications for patents on such common items as nails and railroad tracks. Russia has no modern patent law or court system sufficiently developed to deal with such bizarre cases. If you are or your company is looking to file for new patents, it would be a good idea to learn as much as possible about our new system.

For additional reading:

John J. Fialka, *War by Other Means,* Norton & Company, NY, 1997, ISBN 0-393-04014-3.

Daniel Burstein, *YEN! Japan's New Financial Empire and Its Threat to America,* Simon and Schuster, NY, 1988, ISBN 0-671-64763-6.

Nicholas Eftimiades, *Chinese Intelligence Operations,* Newcomb Publishers, VA, 1998, ISBN 0-9649531-2-9.