# While America Sleeps

*by John J. Fialka*

Slender threads of brownish smoke rose from a forest of chimneys and twisted upward into the winter mist. Collectively they wove a dark cloak that shrouded Edinburgh as a well-appointed carriage bearing an American family appeared in the gloom. The coachman's faint lamp barely penetrated the gathering darkness as the carriage rattled past the outlines of the city's tall, narrow tenements. In search of lodging, the Americans had found themselves in a damp, forbidding place, reeking of dung and smoke—a place that might have served as the perfect setting for a suspenseful spy story.

It was December 1811, and one thing distinguished Francis Cabot Lowell, his wife, and his young children from most other people navigating the city's narrow streets that afternoon. The Lowells had plenty of money, and it showed. Alert coachmen hustled them through the knotty traffic of downtown Prince's Street, and innkeepers always summoned up an extra bit of warmth.

Lowell came from great wealth, but he was no mere rich man's son. A Harvard graduate, he had used his skill as a mathematician to expand a Boston docking and warehouse business. Now, at 35, well dressed and studiously self-effacing, he was a man looking for a much grander venture. Lowell played to local prejudices about the inferiority of the American environment by letting it be known that he was in Scotland for reasons of health. Lowell's neighbors observed that as winter receded the Lowell family carriage appeared almost daily in front of the house, and Mr. and Mrs. Lowell, leaving their children behind with the governess, went on extended trips into the countryside. They often visited places as far away as Lancashire and Derbyshire to take the country air.

That was the cover story. In fact, Lowell was the most skilled economic spy of his generation, and he had ambitions to take in much more than country air. By hitching cotton-weaving machinery to the cheap, perpetual motion of waterpower, Britain had revolutionized the textile industry, transforming Lancashire and Derbyshire into places of phenomenal riches. The newly built mills had literally created the world's industrial age. Lowell plotted his tours as methodical explorations of this 18th-century Silicon Valley. Huge fortunes had been made there by replacing the skilled hand labor of many thousands of people with water-driven looms so simple and so reliable that they could be run by a handful of unskilled women and children. The perpetually humming, swishing, clanking machines changed cheap imported U.S. cotton into bolts of fancy calico that fetched fancy prices in Paris, Berlin, and Boston. They had made rural England and

*A mastery of textile technology helped Britain become an industrial colossus.*

Scotland into a money machine that was the envy of the world.

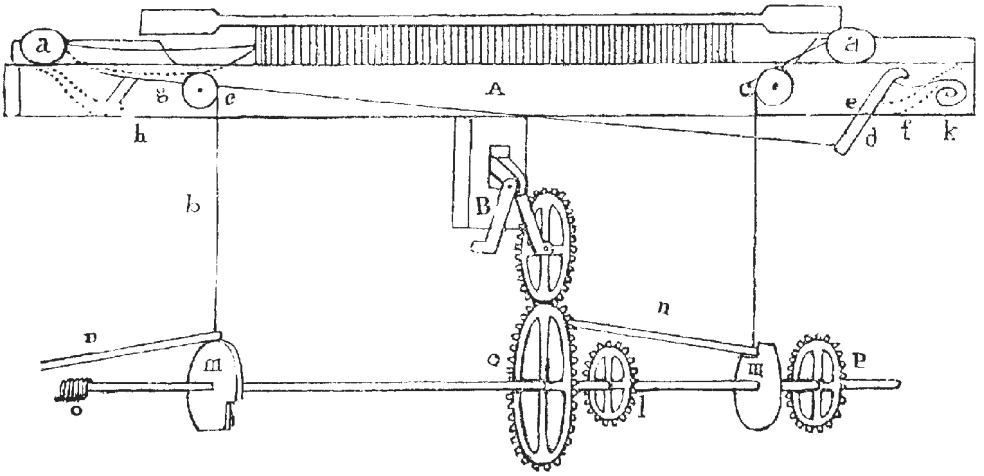
Not surprisingly, His Majesty's Government was determined to protect the sources of the Industrial Revolution from outsiders. By the end of the 18th century, the British passed rigorous patent laws and banned the export of cotton-weaving technology. When foreigners found loopholes by recruiting skilled workers and luring them abroad, this was made a crime. So were the acts of making and exporting drawings of the machinery in the mills. Fortresslike walls topped with spikes and broken glass quickly grew up around the mills, and workers were sworn to secrecy. Skilled technicians who went abroad under false pretenses had their property summarily confiscated by the Crown.

Spies are normally associated with wartime and the theft of military technology. In the vast popular literature about espionage, there is hardly a mention of the peacetime industrial spy. One reason may be that spy stories tend to blossom when wars end. War is relatively clear-cut: there is a winner and an eventual loser, a beginning and an end. The end is normally the signal for the memoir writers to begin, but the economic struggle that attracted Lowell's stealthy genius is not clear-cut. Winners win quietly, and losers are often either unconscious of loss or too embarrassed to admit it. And it is a war that does not end. The stage for the studiously low-key dramas of economic espionage is set, as one perceptive French writer puts it, in a kind of perpetual limbo, where there is neither war nor peace.

Moreover, because economic competition often seems peaceful, economic espionage is usually a more fruitful, less risky business. Sentries are more apt to be napping. Often there simply aren't any. The work of spies in wartime is dangerous and frequently only marginally useful, but the damage a clever spy can wreak in a supposedly peaceful economic setting is often invisible and decisive. And the victims—especially if they must answer to angry stockholders—are not often inclined to want a history.

Against this background, the magnitude of what Lowell achieved has few parallels, even in spy fiction. Few Americans recognize his name, but we are all indebted to this shrewd Yankee. By stealing Britain's most valuable secret, by analyzing it and quickly acting upon it, he brought the Industrial Revolution to New England and built the economic engine that later helped drive the North to victory in the Civil War. That, in turn, laid the cornerstone for a level of prosperity that created the American Century and led to the formation of the world's largest and richest economy.

Yankee ingenuity being what it once was, there were plenty of prominent Americans trying to steal secrets from Britain. But none went so far as Lowell. He was after the Cartwright loom, the crown jewel of the British textile industry. This was a water-driven weaving machine invented by Edmund Cartwright, the fourth son of a country squire, a restless, seemingly unfocused man who dabbled in poetry, the ministry, and experimental farming until he became intrigued by the shortcomings of some of the machinery he chanced to observe in the neighboring Derbyshire mills. So he dabbled in machinery. The result was a loom so powerful and efficient that the British Parliament later awarded him a bonus of £10,000. The importance of the Cartwright loom to Britain's booming economy placed it




*A section of the Cartwright loom*

at the top of a pantheon of industrial secrets.

We still don't know how Lowell got the detailed plans for this tightly guarded machine, but the arrogance of the new lords of Britain's industry probably helped him. They tended to look down upon outsiders, especially the American rustics. Some, such as Edward Temple Booth, owner of a Norwich worsted mill, waived the rule stipulating that all plants be closed to foreigners. He reasoned: "When machinery is peculiarly complicated you may show it with good effect, I think, because it makes the difficulty of imitation appear greater." British customs officers, perhaps sensing that something was up, went through the Lowells' baggage twice when they

> JOHN J. FIALKA, *a former Wilson Center Guest Scholar, is a reporter with the Washington bureau of the* Wall Street Journal. *He is the author of* The Hotel Warriors: Covering the Gulf War *(1992).* 

embarked for home in 1813. They found nothing unusual because Lowell, who is credited by most historians with having a photographic memory, probably carried the blueprints in his head.

Back home, Lowell rented a Boston storefront and hired a first-rate mechanic. Together, they built a scale model of the Cartwright loom. Then Lowell hired a second man to turn a crank until they had all the gears and pulleys working in the rigid, reliable mechanical dance necessary for a perpetual weaving machine. When they had it right, Lowell quickly implemented his other plans, which involved new ways to integrate labor and capital into industrial plants where raw materials would be turned into finished products in the same factory. His company built its first mill at Waltham and later constructed a mill complex in Lowell, the city named for him. By producing up to 30 miles of cloth a day in a nation that then knew very little besides hand labor, Lowell, Massachusetts, provided the first big shock that jolted America into the industrial age.

The object of economic espionage, however, is not simply to gain some secret advantage over a competitor. Steps must then be taken to slow the competitor's attempts to recover. In 1816, a year before he died at the age of 42, Lowell journeyed to Washington, where he persuaded Congress to impose a punishing 6.25 cent tariff on each square yard of imported cotton.

*Francis Cabot Lowell*

From Sidney Reilly to Aldrich Ames, the secrets of wartime spies are the stuff of great drama when they emerge at war's end. But economic wars don't end, and Lowell appears to have taken pains to make sure his secrets would never emerge. He kept no diary, confined his letters to family matters, and appears to have shared the method of his great triumph with no one. A man whose impact was so profound that one historian calls him "an American Newton," Lowell almost managed to erase his own likeness from posterity. But after he died, a workman found a silhouette stuck behind the frame of an old picture in Lowell's office. It shows a man with a long, sloping nose and a weak chin. Apart from the largest, richest industrial economy on earth, it is all we have left to remind us of Francis Cabot Lowell.

If there were a way to revive Lowell and bring him back to his beloved country at the end of the 20th century, the story of Rip van Winkle would not begin to describe the otherworldly shock, the endless ironies, and the boundless frustration that this spy of spies would experience.

He would discover that his world had been stood on its head during the 180 years of his slumber. Let us take him, stumbling, bearded, and bleary-eyed, through some of the many corridors of our economy and see what he would find.

First, the spark of economic life that he helped bring into being has become a beacon to the entire world. The United States of America, once decidedly an economic backwater, a place of dubious investment opportunities, a haven for adventurers, visionaries, and the cast-off poor of other cultures, has become a glistening machine that produces $6.8 trillion in new wealth every year.

But while Lowell's Washington had politicians who had firsthand experience with the results of unheeded security threats—such as being chased out of the White House by British troops during the War of 1812—the Washington that Lowell would find today is a place where most politicians believe that such threats are a thing of the past. Winners of a game that has supposedly ended, they talk endlessly of the perquisites and obligations of "the world's only remaining superpower." The United States has the most powerful economy, the biggest single market, the richest technological treasures, the most widely circulated currency, the largest and freest flow of information, the most powerful military, the most admired university system, and the most elaborate and costly apparatus of protective laws, lawyers, judges, intelligence services, and law enforcement units the world has ever seen.

But once he overcame his initial shock at millions of people whizzing along wide freeways and at vast, brazen cities winking at him by night, Lowell, a remarkably shrewd man, would quickly sense that something was missing. The public's belief in the value of economic intelligence—a belief that made him a national hero and sometimes led citizens in Revolutionary-era communities to parade in the streets when discoveries were brought in from abroad—seems to have vanished entirely. While Lowell knew a citizenry that was hungry for development and preoccupied with building an economy out of scraps of knowledge imported from overseas, he would now find a different breed of American, born with the assumption that all necessary knowledge is here. He would find an America drifting into a profoundly introspective, isolationist, and even anti-intellectual mood.

There would be no end to the paradoxes Lowell would find. Where there was once a small elite of entrepreneurial citizen-spies like himself who rubbed shoulders with the Washingtons, Jeffersons, and Hamiltons of their day, today the business of collecting intelligence has become for Americans a strangely professional, closed, and often suspect activity. It is dominated by huge bureaucracies that seem almost indifferent when it comes to economic affairs. Unlike the people of economic powers such as Japan, Sweden, China, France, South Korea, and Taiwan, countries where citizen-spies such as Lowell still abound, Americans have the feeling they are above this sordid business and that they are somehow removed and protected from it.

Only—Lowell would discover—they are not. The game of economic espionage continues, as it has for thousands of years, but now the tally of wins and losses is locked inside the nation's sprawling intelligence apparatus, which costs some $28 billion a year to maintain. And there is yet another fundamental difference: whereas Lowell's America searched the world for fresh economic intelligence, the United States in the 1990s seems content to stay at home. This America has become the chief target of the world's economic spies—a sizeable force hailing from at least 20 major countries whose identities and doings remain closely guarded state secrets.

Lowell was a wily Yankee who knew how to obtain secrets, so let's suppose that in an effort to orient himself he got his hands on a copy of a report by an intergovernmental working group, the National Economic Council (NEC), which includes experts from the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the departments of Treasury, State, Defense, Commerce, and Justice, and representatives from the White House. Prepared for Congress's intelligence committees in 1994, the report is stamped SECRET NO FORN. (This indicates that the information is not to be shared with any foreign powers, including allies.) The document notes that, "Reports obtained since 1990 indicate that economic espionage is becoming increasingly central to the operations of many of the world's intelligence services and is absorbing larger portions of their staffing and budget."

In the early 1980s, it was estimated that at least 1.2 million people were working in one capacity or another for the world's spy agencies. Lowell would see that, as the NEC reports, nations had turned much of their Cold War spy apparatus to economic espionage, including giant computer databases, word-activated eavesdropping scanners, spy satellites, and an almost unbelievable array of bugs and wiretaps.

Economic espionage against the United States breaks down into three major styles. Agents from China, Taiwan, and South Korea are aggressively targeting "present and former nationals working for U.S. companies and research institutions," according the NEC report. The second category is headed by France, which is said to prefer classic Cold War recruitment and technical operations, including bribery, discreet thefts, garbage searches, and aggressive wiretapping. Russia and Israel carry out similar spying with varying degrees of government sponsorship. Germany is described as planning to increase the number of its Federal Intelligence Service (BND) agents in Washington to improve its collection capabilities. Japan, which does not have a formal intelligence agency but sometimes collectively resembles one, falls into the third category. Japanese industry and private organizations gather "economic intelligence, occasionally including classified proprietary documents and data." The result is an exceptionally efficient spy network that is described as "not fully understood" by the United States.

The United States is now the chief target of the world's economic spies.

The most aggressive operations against U.S. companies occur overseas, especially in home countries where spy agencies are freer to act and where, the NEC report notes, "government controlled national phone networks" and other electronic means can be used to slither inside company communications and data banks. The best place to recruit foreign nationals who work for U.S. companies overseas is in third countries, where "a host country's counterintelligence services do not pose a serious barrier to effective foreign intelligence operations directed against U.S. targets. Furthermore, U.S. citizens tend to be more lax about security matters when living in countries perceived as friendly to the United States."

"Lax" is probably a polite way to describe the laid-back attitudes that

Lowell might find if he wandered among his countrymen today. A recent study by the National Research Council found that one way Japanese businessmen collect information about developments within the U.S. aerospace industry—a major Japanese target today—is to get their U.S. counterparts to brag: "Ego comes into play as engineers try to impress their foreign contacts."

The sublime mismatch between war-trained spies and business people schooled to expect the proverbial "level playing field" has also become worrisome in Canada, where Chris MacMartin, coordinator of the technology transfer program for Canada's Security Intelligence Service, says that of 500 companies queried, fully one-third brought up security problems. Many of them had discovered that people they had once trusted were harvesting company secrets for a foreign government.

"When you're carrying over the family jewels and you're traipsing across several countries who would crawl over broken glass to get what you've got in your briefcase, you will inevitably find that the government has far greater capability to do damaging things to you than your competitor," explains MacMartin. Naive businesspeople who entrust a document in their briefcase to the hotel safe might "just as well photocopy it and give it to the company [that competes with them], because that's where it's going," MacMartin adds.

Just how much espionage costs companies is hard to say. "We have seen damage in terms of lost jobs, lost contracts, and diminished contracts. We have spoken to companies who have had messages intercepted and computers penetrated," MacMartin admits. But nobody wants to talk openly about it. "Companies have very solid reasons not to make this public. They usually have shareholders who think that secrets are what make the company valuable. Invariably in all of these cases, somebody screwed up."

Canada is not about to point fingers at any specific country, but MacMartin says that 39 percent of the spy incidents occurred in Asia and another 30 percent in Western Europe.

U.S. companies aren't much more talkative. An International Business Machines (IBM) representative told a U.S. House of Representatives committee in 1992 that the company had suffered losses "in the billions" from thefts of proprietary information, including thefts by unnamed government agents intent on stealing IBM's software and other secrets for competitors in their country. Corning, Inc., complained of state-sponsored efforts to steal its fiber-optic technology. "It is very difficult for an individual corporation to counteract this activity. The resources of a corporation—even a large one such as Corning—are no match for espionage activities that are sanctioned and supported by foreign governments," explained J. E. Reisbeck, then an executive vice president of the company.

While the need seems obvious, the question of how to mobilize U.S. intelligence agencies to support and protect the U.S. economy has bobbed to the surface in Washington every few years since World War II. When the Truman administration assembled 20 top government officials for a secret meeting in the CIA's cramped, makeshift administration building on the Mall in November 1950, they were told that because foreign economic intelligence was collected by 24 different agencies, many of which didn't communicate with one another, there were "important gaps in the collective knowledge of the government." The turf battles

involved in reassigning areas of responsibility in information gathering proved to be too difficult for this cabinet group, however, and a CIA committee was established to study the problem.

The issue came up again in 1970 when Nixon administration officials, shocked by Japan's bold and well-aimed assault on the U.S. auto industry, told the President's Foreign Intelligence Advisory Board (PFIAB) to suggest remedies. Gerard P. Burke, then PFIAB's chief of staff, recalls that his four-man staff spent about a year studying the problem. A few organizational changes were made to bring economic officials onto policy-making boards in the intelligence community, but as Burke recalls, no one could find a way to address the real issue he had discovered: while the United States was tinkering with its organizational charts, the intelligence agencies of major allies, including the British, the French, the Swedes, and the Swiss, had begun providing direct support to their countries' businesses. "We discussed it ad nauseam," Burke remembers. "We thought U.S. companies needed [support], but we didn't think it should be provided by the U.S. government. There were obvious conflicts of interest."

*A rare catch: Bin Wu worked for Chinese intelligence (and as a double agent for the FBI) before being found guilty in 1993 of illegally exporting high-technology equipment to China.*

Stansfield Turner, the retired navy admiral who took the helm of the CIA in 1977, during the Carter administration, pointed to the same problem. Beyond the Soviet Union, the major threat to the United States came from the economic sphere. "Goddammit," he remembers thundering once at a group of aides, "if [the economy] isn't a national security matter, then what is!?"

But the aides had questions. Should you collect information for Ford and not General Motors? Had CIA agents signed up to risk their lives for a corporation? What about providing intelligence to a U.S. company that was partly owned by Japan? In the end, the aides' skepticism prevailed. Since that debate in the late 1970s, CIA task forces have studied the issue two more times. Each study found a problem but backed away from practical solutions. Admiral Turner recently fired another salvo. One way to break out of this stalemate, he says, is simply to make for-

eign espionage assaults on U.S. companies public. "That may aid U.S. corporations less than some would like, but it also can lessen an advantage foreign corporations have over American firms," he says.

In 1985, during the Reagan administration, Michael Sekora, a young physicist working in the Defense Intelligence Agency, became alarmed by moves being made by French, German, and Japanese intelligence operatives in the commercial arena. Some of them were busy collecting ideas from U.S. universities. Why not create a database to follow the development and flow of key technologies around the world, tapping the whole government for information? he suggested. President Reagan's people liked Sekora's idea and wanted the database and a small staff installed in the White House. The project was called Socrates. But the incoming Bush administration strangled Socrates in its crib. The project posed too many questions. "You can't look at the Japanese, they said, because they're our friends. You can only look at the Russians because they're the bad guys. What we wanted to do was look at the technologies, regardless of who had them. We wanted to get to the bottom line truth, as did the philosopher," Sekora says.

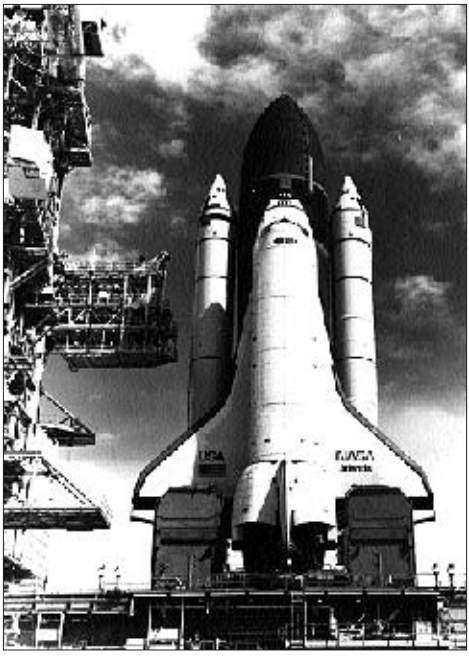
Sekora resigned and is now peddling Socrates in the private sector, with mixed results. He points out that many U.S. companies, preoccupied with quarterly results and the domestic market, have cut back on research units and see no use for strategic information gathered overseas. "When I go into a company, sometimes an old engineer will come up and say that's what we used to do before World War II. We sent our people all over the world."

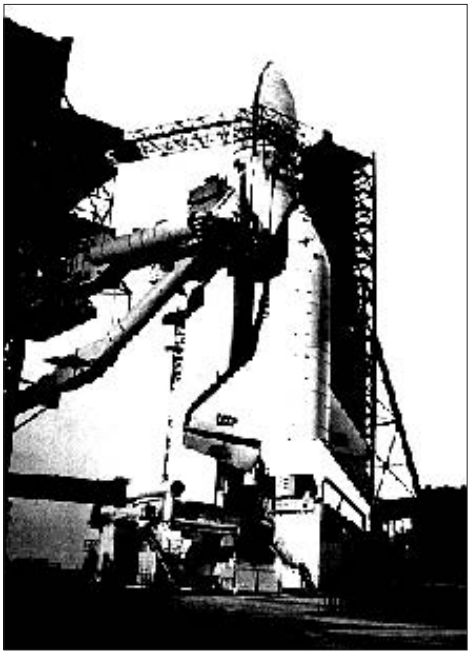
The uncanny ability of American corporations to improve on outside innovations astonished European industrialists in a way that is strikingly similar to the way Japan's success perplexes American managers today.

Indeed they did. The practice of collecting information overseas didn't end with Lowell's generation. "Technology-gathering missions to Europe were commonplace during the late 19th and early 20th centuries as American corporations sent their leading scientists and engineers abroad to learn advanced techniques," writes Richard Florida, a technology expert at Carnegie-Mellon University. "The uncanny ability of American corporations to improve on outside innovations astonished European industrialists in a way that is strikingly similar to the way Japan's success perplexes American managers today."

In his strolls around modern Washington, a place he knew as a tiny village where carriages traveling the unpaved streets often got stuck in red clay mud, Francis Cabot Lowell would find that the report of President Clinton's commission to study the overhaul of the nation's intelligence apparatus had a familiar ring. The first item on its "new agenda"?: "Increasingly, the ability of U.S. industry to compete successfully in the world market is seen as a critical element of U.S. security."

In the years between 1950 and 1996, as proposals to do something about obtaining economic intelligence kept getting mired in Washington's bur-





*Which shuttle is which? The Soviet Union used stolen plans to build its shuttle.*

eaucracy, three successive waves of economic espionage rolled over the country. Measured in terms of economic and strategic impact, they were all tsunamis, probably the most damaging peacetime assaults ever mounted on a nation's economy. Each, in its own way, was worse than the next. But compared with real wars, they caused hardly a ripple.

First came the Russians. In the early 1980s, just as it was about to rev up the arms race, the Reagan administration learned from the French how the Soviet economy, with all its glaring faults, managed to match U.S. technology so quickly: the KGB had been systematically stealing information from U.S. research and development programs. "The assimilation of Western technology is so broad that the U.S. and other Western nations are thus subsidizing the Soviet military buildup," concluded the authors of a CIA report on the matter.

A group known as the VPK, or Military Industrial Commission, a special board of the top executives of Soviet defense manufacturing ministries, had been spending as much as $1.4 billion a year ordering technology and secrets from the West, much of it taken from the electronic brains of new U.S. weapons systems. The list, provided by a KGB spy dubbed "Farewell" by French intelligence agents, was endless and alarming—and embarrassing to the Pentagon. The radars that guided the missiles fired from Soviet fighters were copied from blueprints of the radars on U.S. F-14, F-15, and F-18 fighters. The Soviets' space shuttle was created from documents carted away from NASA. The Soviet Ryad computer had been copied from the architecture of the IBM model 370 mainframe computer. In all, about 5,000 categories of Soviet military equipment entering its arsenals during the 1980s were products of the KGB's efforts; about 60 percent of the blueprints and other documents were taken either from the United States or U.S. allies.

Farewell's reports showed that the KGB had caught the United States

with its barn doors wide open. While the Defense Department verified the information's authenticity, other agencies, true to the ostrichlike code of behavior that prevails among victims of economic espionage, tried to minimize it. The CIA kept most of the evidence under tight wraps. Some former officials of the FBI, which is in charge of counterintelligence, cling to their belief that the barn was never invaded.

Big as it was, the Soviet wave of economic intelligence collection was soon overshadowed by Japan's efforts. While the Soviet Union's industry outside the defense area couldn't readily assimilate U.S. technology, the Japanese economy could, and in the 1970s and '80s it did so at an awesome pace. Like the Soviets, the Japanese found U.S. universities an enormous source of free, lucrative information, and, oddly, the Japanese provided a kind of political cover for the Soviet "students."

Jan P. Herring helped run the CIA's counterespionage efforts in the early 1980s. After several Soviet KGB types were caught stealing secrets at universities, he recalls, the U.S. government was seriously thinking about kicking out all foreign students. But, he says, "the Japanese just went ape over this, so we backed off." Later, as a vice president for the Futures Group, a Boston-based consulting firm, Herring went to universities hunting for ways to help U.S. firms compete against foreign businesses—a novel idea for some of his clients. "We often found that MITI [Japan's Ministry of International Trade Industry] or JETRO [MITI's technology information collection service] had already been there talking to these people. In fact, we didn't run across too many that the Japanese hadn't talked to."

When it comes to other people's ideas, the Japanese are relentless bargain hunters. Every scrap of information is collected and studied. They set up an elaborate network of small research laboratories in university towns. Gaining a sense from the universities of where the cutting-edge U.S. technology was, the Japanese then went out and bought some 40,000 patent licenses for it at bargain basement rates. U.S. experts later concluded that this was a "windfall" that gave Japan the means to take over the television market and muscle into semiconductors. It taught some "hard lessons" to U.S. companies, which enjoyed their royalty checks until Japan's products drove them out of their own markets.

U.S. economists, locked for years in an almost monastic argument over the sanctity of "free trade," have only recently awakened to the notion that the carefully targeted, government-driven campaign Japan uses against the United States in high-technology areas is something different from the bustle and hum of free markets working. It is more like the attack profile of a smart missile: a strategic, "beggar thy neighbor" assault that targets high-tech jobs and snuffs out whole industries. Laura D'Andrea Tyson, who recently resigned as chair of President Clinton's National Economic Council, estimates that Japan's aggressive efforts cost $105 billion in lost U.S. sales between 1985 and 1989, and that "the lion's share of the loss was matched by offsetting Japanese gains."

What is left is a hollowed-out economy that somehow continues to function, even to boom, but is a decidedly pale version of America's manufacturing past. In constant, uninflated dollars, average weekly wages have dropped for 20 years. There are fewer, poorer, "dumber" jobs for blue-collar workers. It is a hollowness that will increasingly res-

onate as an office-threatening issue to politicians who ignore it.

We are losing at a game of economic jujitsu in which Japan, which keeps its markets closed and does relatively little research within its largely closed university system, uses one of the U.S. system's main strengths—its openness—against it. And the struggle continues as MITI targets the remaining crown jewels, the aerospace, biotechnology, and software industries, which are expected to be the drivers of the U.S. economy in the early 21st century. While the fabled and probably fictitious "missile gap" was used politically to galvanize U.S. concerns in the 1960s about the Soviet Union, the patently real "intelligence gap" opened by the Japanese has caused no outcry. But to the eye of a practiced collector such as Lowell, the gap would look ominous and perhaps even frightening. In 1988, Japan sent 52,224 researchers to the United States. Meanwhile, only 4,468 U.S. researchers traveled to Japan. Japanese companies invest the time and money needed to teach English and the rudiments of American culture to the employees they send here, while U.S. companies rarely provide more than minimal cultural orientation for their overseas workers.

What Japan has accomplished in the United States has caused a stir of envy in China and other Pacific Rim nations, including Taiwan and South Korea. Collection efforts by these countries may eventually loom larger and more threatening than the Japanese campaign, which the other Asian powers appear to be using as a model. Like Japan, they have begun in U.S. universities. In 1991, 51 percent of all science and engineering doctorates awarded by American universities went to students from Pacific Rim nations, with the largest share going to the two Chinas. Many of these students, educated largely at the expense of the U.S. government, linger in the United States after obtaining their doctorates, and a large number of high-tech companies and government research laboratories are becoming hooked on this stream of cheaper, often smarter, and more biddable talent. Some of these students eventually become U.S. citizens and help renew the American dream by achieving breakthroughs that mean new jobs and new markets for their adopted country. But more return to their homelands, and government recruiters from their native countries are working in the United States to lure more home, where they join the payrolls of some of America's serious and sometimes dangerous competitors. Meanwhile, the faltering U.S. public education system produces fewer and fewer qualified applicants for graduate-level science and engineering programs.

By far the largest, most problematic player is the People's Republic of China, a nuclear power that is using U.S. technology and some of the profits from a ballooning trade surplus with the United States to modernize its army, navy, and air force. It has begun to flex its growing military muscle in the Pacific. In a series of war games in the Taiwan Straits in March 1996, it fired its new solid-fuel M-9 missiles at target ranges situated near Taiwan's main seaports. China's chief intelligence agency, the Guojia Anquan Bu, or Ministry of State Security (MSS), has flooded the United States with spies, sending in far more agents than the Soviets did even at the height of the KGB's campaign. About half of the 900 illegal technology transfer cases being investigated by the FBI and the U.S. Customs Service on the West Coast involve the Chinese. The MSS recruits students. When money is not persuasive, threats against family members back home are tried. And unlike the KGB's agents, China's spies easily find protective cover in the United

States, among this country's large Asian population.

Although the FBI makes an effort to watch foreign students and businesspeople, China's flood has simply overwhelmed the bureau. "The FBI is ensnarled in a cesspool of Chinese agents and their cases are all stuck at first base," says James Lilley, former U.S. ambassador to China and former CIA station chief in Beijing.

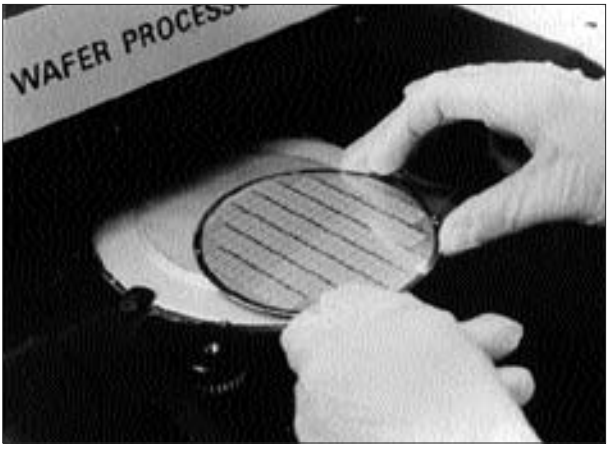
Unlike the Japanese, who have focused on ways to take over commercial markets, China's strategists have military goals. They covet technology such as missile guidance systems that can use signals from the U.S. satellite-based Global Positioning System for precise targeting information. They go after small cruise missile engines, night-vision equipment, upper-stage rockets, and nose cones for globe-spanning nuclear weapons—all items that may shift the balance of power in the next decade and drive countries such as Japan and Taiwan into full-blown nuclear weapons programs. "You're going to see an arms race in Asia that is unequaled in history," predicts Nicholas Eftimiades, the author of *Chinese Intelligence Operations* (1994), the first open study of China's massive efforts.

Despite the ominous look of things, Lowell would find that the worrying was confined to a small group of academics, corporate security experts, and intelligence analysts, and that most of his fellow Americans were oddly serene. They have become accustomed to this seemingly comfortable new post–Cold War drift of things. In the news media, the lowering of trade barriers and the influx of foreign students are often portrayed as part of a vast, multicultural economic march toward a peaceful "globalism." Increasingly, the notion that national borders still matter is dismissed as outmoded.

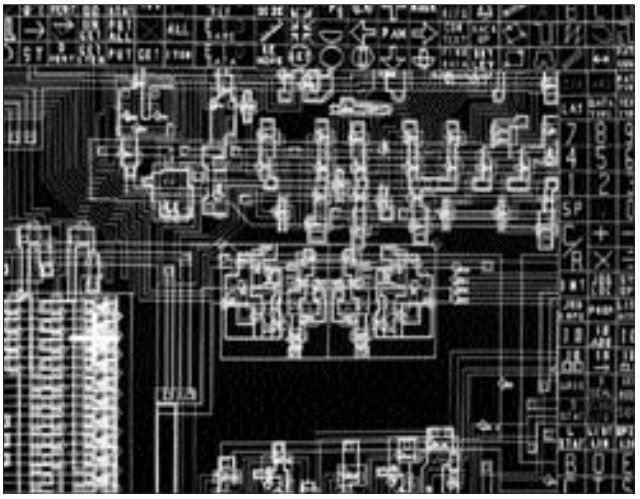
"In Taiwan," according to a recent front-page *New York Times* article, "the high-tech migration is being called the *'rencai hiliu,'* literally the 'return flow of human talent.' But for the thousands of American-trained scientists, weaned on late-night pizza at the computer center and shopping at the mall, it is simply called the reverse brain drain."

To the modern American mind, this might seem normal. To Lowell's 19th-century mind, fresh from a time when the United States fought for its borders and established its industrial base, it would raise a thousand questions. Why were foreign science and engineering students increasingly taking top graduate research posts at places like Harvard and the Massachusetts Institute of Technology? Why was the U.S. government subsidizing these positions? Why had U.S. students' scores in math—a subject that gave Lowell great pleasure and great wealth—dropped to among the lowest in the industrial world? Who had let the U.S. public school system—once the envy of the civilized world—decline to such an abysmal state? Were U.S. brains being drained or starved and rejected? Was the nation's base for creating technology, the bedrock of preparedness for all wars in this century, being exported? Why?

The notion that the United States is in the midst of a "war by other means" might seem foreign to some, but certainly not to Lowell. A fan of protective tariffs, he would not be surprised by the malign effects of lowering trade barriers. One of the more dire effects, not yet widely noticed, is the formation of an alliance among the Russian and Italian mafias and Colombian drug cartels. These allies, taking advantage of the new regime of relaxed national sovereignty, now move money from country to country much faster than national police forces can track it. According to the U.S.




*Knowledge-intensive industries such as semiconductors are key targets of economic espionage. The United States recently regained its lost lead in semiconductors.*



Treasury Department, criminal organizations now send some $100 to $300 billion around the world looking for investments. Casualties caused by the flow of drugs into the United States already closely approximate those of a war. And the massive profits that flow out of this alliance light the fuses of future wars by criminalizing entire countries and buying elections, politicians, and officials to thwart U.S.-backed reforms.

Lowell's world was Darwinian: you could keep what you could protect. It is still Darwinian when it comes to cross-border transactions, but Americans in the post–Cold War era feel they are protected in a snug global cocoon of laws, customs, and rights. When it comes to some new things, such as the nation's addiction to electronic information, the cocoon is hardly more than a fiction.

"People don't understand what's out there," explains Ambassador Anthony C. E. Quainton, who until recently headed the State Department's Overseas Advisory Council (OSAC). The council was formed in 1985 to help U.S. corporations deal with the threat of terrorism. In the 1990s, reports from some of the 1,300 U.S. corporations in communication with OSAC shifted the group's attention more toward economic espionage.

The most aggressive intrusions come in Japan, South Korea, and China, where the threat begins with the telephone sitting on the hotel room's nightstand. Quainton says he knows of entire hotels where the phones are

set to receive, even when they're hung up. "The whole hotel is live." He strongly advises business people not to talk about technology, patents, or business plans in their rooms. "If they can't see the enemy, they may not think he's there, but he is."

This is a hard notion to sell to normally garrulous American executives. Jan Herring, the former CIA counterintelligence expert, recalls making many visits to U.S. companies to warn executives that when they make calls from overseas, they are "talking to the world." On the average call, Herring estimates, a "minimum" of five countries could be listening. "It always begins with your host country, then there were the Soviets, the British, the Chinese, and the Japanese." (By law, he notes, the U.S. National Security Agency, America's eavesdropping agency, can't listen in on Americans, but it might be tapping the second party on the line if that party is a foreigner.) While governments still hold sway over the phone lines, newer forms of communications, including satellite links and cellular phones, are much easier to tap, and have thus tempted thousands, perhaps tens of thousands, of amateurs to get into the spy game.

And the threat is still greater when it comes to computer communications. "If you are using the information highway internationally, especially without encryption, you are at great risk," Roger P. Watson, an FBI deputy assistant director, recently told a group of business security executives. But the bureau has found that new habits are hard to change. Harold Henderschot, the FBI's top computer expert, says he often visits companies and finds they have piled their computer security equipment in a corner, uninstalled. The usual explanation is that it makes the computers too cumbersome and slow.

Lowell, a man used to thinking in terms of the whine of gears meshing and the rhythmic stutter of levers working, might have trouble getting his Newtonian mind around electronic technologies, but he would quickly recognize the law that protects them—the law that hasn't changed all that much since his time. Today, it lags far behind the threat. Part of the problem is that victims don't complain. "The only thing a company will protect more than its information is the fact that they've lost it," explains Dan Swartwood, head of a private security consulting company. If there are mute victims, or victims who don't know they are victims, there are no witnesses, no complaints, no cases, no new law, and no actuarial base for insurance underwriters.

A new survey of 325 unnamed American companies by Swartwood and a colleague, Richard J. Heffernan, shows that this troublesome void is rapidly growing. The anonymous companies reported 32 cases of theft of intellectual information per month in 1995, more than three times the rate found in a similar survey in 1992. The losses amounted to $5.1 billion. The most common suspect was a former employee, contractor, supplier, or temporary. Ranked by nationality and frequency of complaints, the top perpetrators were Chinese, Canadian, French, Indian, and Japanese, in that order.

The survey findings roughly track with the experience of the FBI, which is currently investigating 800 economic espionage cases in 23 foreign countries. The agency's load of such cases has doubled since 1994.

Then there are pesky problems of definition. If a horse is stolen from the neighbor's barn, that is a serious theft; but if his exotic, proprietary, million-dollar software program is surreptitiously removed and zipped away on the

Internet, that may not be a serious theft because the "horse," the original copy, is still in the barn.

Similarly, if a spy comes out of a foreign embassy and snatches a company's secret, that is espionage and automatically brings in the FBI. If a spy comes from a private company or a university and steals the same secret, the FBI may not have a legal basis to intervene. More than a few corporate victims decide to suffer their losses in silence (out of the view of stockholders) and not summon the FBI. "I know it's a controversial topic . . . there are a whole myriad of problems here, but we need each other," explained Pat Bryant, the FBI's chief of internal security, to a group of corporate executives at a recent OSAC meeting at the State Department. He pleaded with the companies to give the bureau more detail about the nature of their losses, and urged them to use their lobbying clout to help push for more modern laws.

"What we need is more ammunition from you to show how great the threat really is," countered one executive.

Edward Miller is a former president of the National Center for Manufacturing Sciences, a government-industry consortium founded in 1984 to help renew U.S. high technology and promote it abroad. He often hears the same kind of death-spiral, chicken-or-egg logic. Without dramatic proof of theft and damage, he says, U.S. companies simply won't change their ways. But unless they do change their ways, many companies will never be able to generate dramatic proof. Miller worries that, thanks to America's feeble defenses against economic espionage from the 1960s to the 1980s, the scent of blood is in the air. It creates a hunger for more. He recalls a barrel-shaped Czech engineer yawning during a technical meeting in Prague some months ago. Miller, also an engineer, had been talking about the promise of new U.S. machines. The Czech shrugged; that wasn't the need in his factory.

Miller challenged him. "I said, if I went into your facility, would I find the latest design capabilities, the latest computer-controlled machines? He says, 'Yeah.'"

During the Cold War, anything the Czechoslovakian government factory needed, the engineer explained, was quickly stolen by the KGB from the United States or developed from stolen blueprints. The process took a few months. Thanks to the KGB connection—now ended—Czech plants today are relatively modern. What we need, said the engineer, are management skills, marketing, and accounting.

"I had one U.S. government representative there whose jaw hit the floor," recalls Miller. "What they were essentially telling us was that their espionage defeated us. If they defeated us when our guard was up, do you honestly think they would stop?"

To Miller, understanding the problem of economic espionage is simple; dealing with it, though, is a formidable problem. "We are an open society. What we have to learn is how to get as much as we give away." It will be a new and daunting challenge for some, but one that would make Mr. Lowell feel quite at home.

---