

★ ★ ★ ★ ★ ★ ★ ★ ★ ★

# RED STAR OVER WASHINGTON

**The case of Wen Ho Lee and the W-88**

**warhead should come as no surprise.**

**From the start, the Clinton admin-**

**istration has spared no expense—**

**even that of U.S. security—to court**

**the People's Republic of China.**

★ ★ ★ ★ ★

## Kenneth R. Timmerman

★ ★ ★ ★ ★ ★ ★ ★ ★ ★

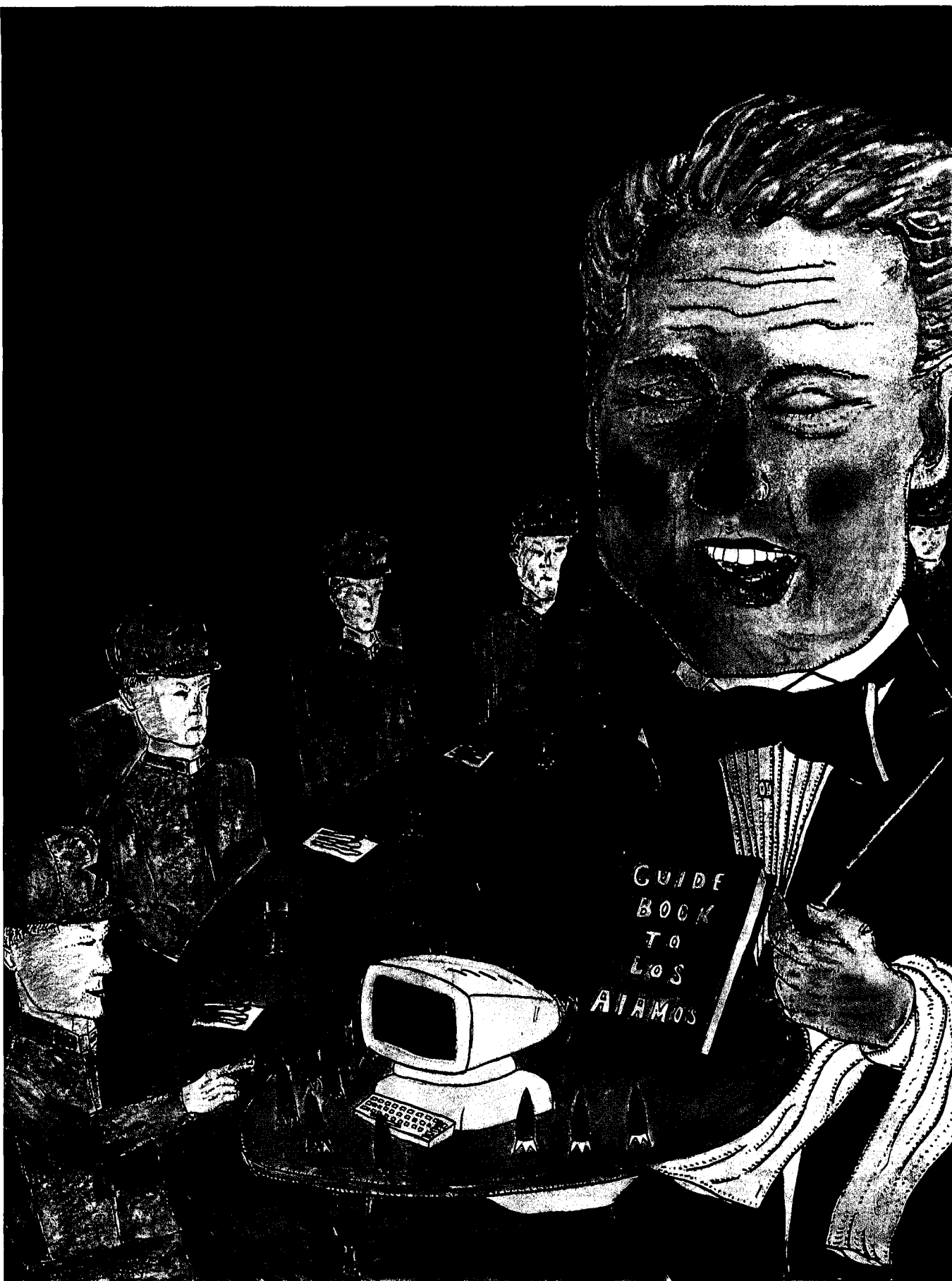
**F**or Paul Redmond, the CIA spycatcher who caught Aldrich Ames, the case of the Chinese government espionage ring operating at the very heart of the U.S. nuclear weapons establishment was “worse than the Rosenbergs.” Not only had the design secrets of our most advanced nuclear warhead been delivered lock, stock and barrel to Peking, but the Chinese had been able to operate inside our labs for more than 14 years, from 1985 until this March, apparently undetected.

But unlike Julius and Ethel Rosenberg, who were executed in 1953 for delivering atom bomb secrets to the Soviet Union, the Taiwan-born suspect who worked at the Los Alamos National Laboratory was merely fired from his job—and that was only after details of the case were revealed by the *New York Times*. Even more unsettling: The Department of Energy, which oversees the labs, revoked Wen Ho Lee's Top Secret security clearance only this February, despite warnings dating back to 1995 from its counterintelligence office of ongoing Chinese efforts to acquire U.S. nuclear weapons secrets.

The case of Wen Ho Lee, who allegedly compromised the secrets of the W-88 warhead used on our Trident missile system, is not the only one in which the Clinton administration's cavalier attitude toward nuclear weapons and national security has encouraged spying. In December 1997, another Taiwan-born scientist working in a U.S. nuclear weapons lab, Peter Lee, pleaded guilty to giving the Chinese the secrets of a highly specialized laser plasma system used to test nuclear weapons. The system is considered crucial to maintaining the viability of the U.S. nuclear weapons stockpile, now that the major nuclear powers have agreed to a moratorium on nuclear testing. Until the invention of the laser system, the U.S. had to actually detonate nuclear weapons from the stockpile to ensure that they worked. “This system gives China the means to test new weapons and to validate their designs, without anyone having a clue to what they are doing,” a former U.S. intelligence officer told *TAS*. For his crime, Peter Lee was fined \$20,000 and sentenced to 12 months in a halfway house, from which he has since been released.

It seems that every day brings new revelations about Chinese spying in the United States and the weapons programs that have been compromised. Yet National Security Advisor Samuel “Sandy” Berger continues to assert that the White House has responded “swiftly” to each case. In his solo news conference on March 19, President Clinton was flustered when a reporter asked about the theft from one of the labs of an Electromagnetic Pulse (EMP) weapon—a Top Secret, non-nuclear device that destroys an enemy's silicon-based computer chips, and thereby his ability to communicate and to use most of his weapons. “You say they stole? Is that the word you used?” Clinton replied, buying time. Then: “To the best of my knowledge, no one has said anything to me about any espionage which occurred by the Chinese against the labs during my presidency.” Even in the arena of national security, Bill Clinton invokes the Lewinsky defense of galese and potentially faulty recollection.

KENNETH R. TIMMERMAN is a contributing editor for *Reader's Digest* and a frequent contributor to *The American Spectator*.



COULTER YOUNG

The cases of Chinese nuclear spying revealed to date are “perhaps just the tip of an iceberg,” says Senator Richard Shelby, the powerful chairman of the Senate Select Committee on Intelligence. The reason is simple, and systemic: From its first days in office this administration has disdained nuclear weapons, seeing them as the cause of an expensive environmental clean-up, not the cornerstone of fifty years of world peace. Add the belief that we might share U.S. military technology with the Chinese, because we will always stay “one step ahead” of potential adversaries, and the result is contempt for any form of national security export controls. Whether it’s nuclear weapons secrets from our labs, or supercomputers and advanced telecommunications gear from Silicon Valley, this administration has presided over the greatest transfer of military technology to a potential adversary of any administration in history. Repeated statements by Clinton and his advisors on the need to “engage” China, regardless of the spying scandals, can only encourage the Chinese to go for more.

## THE COX REPORT

Further evidence of Chinese spying is found in a 700-page, still-classified report compiled by the House Select Committee on U.S. National Security and Military-Commercial Concerns with the People’s Republic of China, established last year to examine the impact on U.S. national security of U.S. technology transfers to China (See “Loral Exams,” TAS, July 1998). When Chairman Christopher Cox offered a vague summary of the Select Committee’s findings on December 30, he promised that more details would follow once the report had been scrubbed to protect classified sources and intelligence-gathering methods. Three months later, the administration was still fighting to keep the report secret. According to committee staff members, an interagency review board was even trying to classify information taken from newspaper accounts, in their efforts to bottle-up the scandal. Cox told reporters on December 30 that the Select Committee had made 38 specific recommendations for action to remedy lax security arrangements governing U.S. technology transfer to China, and confirmed that the assistance provided by Hughes Aerospace and Loral to the Chinese following the failure of a Chinese rocket in 1996 had harmed U.S. national security. “The technology transfer that has occurred goes beyond the examples of the Loral and Hughes cases,” Cox added. “It goes beyond, indeed, missiles and satellites, and includes military technology. And the technology acquisition efforts of the PRC have been targeted at the United States for a period of at least two decades, undoubtedly longer.”

TAS has learned that the most sensitive section of the report for the White House does not deal with the satellite launches, or even the theft of W-88 nuclear weapons design. The White House leaked that information to the press in an apparent effort to inoculate the public against the worst of the Cox Report revelations: details of how the People’s Republic of China has used its extensive network of commercial companies in the United States to procure highly sensitive U.S. military technology and otherwise spy against the United States. Based on interviews with FBI agents, Customs Service investigators, Pentagon technology security officers, and other intelligence agencies, the

message of the Cox Report is devastating in its simplicity: Communist China is spying the pants off us, and it is using some 1,000 commercial companies, employing more than 10,000 Chinese nationals residing in the United States, to do so. “The weapons suppliers and procurement companies are also collectors,” says one source familiar with the report’s conclusions. “The operations that led to some of our most significant losses were not run by [China’s] Ministry of State Security, but were done right out of those companies, which are closer to cabinet departments than commercial companies.” The administration is desperate to quash this information because it has done nothing to curtail Chinese spying in the U.S. since Clinton claimed the White House. Some would say the president and his policies actively encouraged the Chinese to expand their intelligence and influence-peddling operations in the United States.

U.S. law enforcement officials say they are “overwhelmed” by the sheer number of Chinese Communist agents operating in the United States, and can only focus on a few high-profile cases. On February 11, for instance, Customs undercover agents in Boston arrested Chinese national Collin Shu (a.k.a. Zhihong Xu) on charges of attempting to purchase state-of-the-art fiber-optics gyroscopes (FOGs) used in guidance and navigational systems for ballistic missiles and combat aircraft. An affidavit by the chief Customs agent involved in the case shows that Shu and another Chinese national, Yao Yi, had initially attempted to buy the gyroscopes from their Massachusetts manufacturer and have them shipped directly to Peking, supposedly for use in various Chinese universities. But because the gyroscopes were purely military items, their export was controlled by the Department of State, which denied them a license.

Next, Shu and Yi shifted their business to Lion Photonics in Montreal, Canada, a company they had set up “specifically for the purpose of sending technology to China,” according to Special Agent in Charge Allan Doody, who oversaw the investigation in Boston. “They were hoping to get around the U.S. licensing requirement by claiming the gyros would be used in Canada,” Doody tells TAS. When that also failed, they tapped a small Montreal-based computer company run by Chinese nationals to make the purchase, but they neglected to change the wording in their purchase order. The manufacturer smelled a rat and contacted the U.S. Customs Service, which set up a dummy company to handle the sale, gathering evidence that led to the February arrest. “For every case like this one,” a Customs agent says, “there are probably a hundred other cases we never see at all. We only catch these cases because we get lucky, or because someone tips us off. When the Chinese work with only Chinese networks, we never see a thing.”

## WHY SPY IF YOU CAN GET IT FOR FREE?

I have been investigating Chinese high-tech espionage activities in the United States since 1993, and discovered early on just how sensitive a subject this can be. As a congressional staffer working for California Democrat Tom Lantos, I requested licensing records of U.S. high-tech exports to China from the Department of Commerce. When Commerce finally delivered the several-



thousand-page print-out to the Rayburn House Office building in late March 1993, I was prevented for three weeks from even looking it over, despite the fact that the information was not classified. Leading the charge to prevent my access was Rep. Sam Gejdenson (D-Conn.), currently slated to become chairman of the House International Relations Committee if the Democrats win back the chamber in 2000, and his top staffer John Scheibel, who went on to become a Washington, D.C. lobbyist for a computer export lobbying group. They did not want the story to leak out of just how much dual-use technology U.S. companies had been allowed to sell to the Chinese military, for fear that would impede the U.S.-China high-tech pipeline.

Unbeknownst to most people at the time was a plan devised by top Clinton administration appointees to lift export controls on a wide range of strategic technologies. The plan was first laid out in a 1992 National Academy of Sciences study authored by William Perry, Ashton Carter, and Mitchel Wallerstein, who all went on to top Pentagon jobs under Clinton. Calling export controls a “wasting asset,” they argued that for U.S. high-tech firms to maintain a technological edge over their foreign competitors they needed to be allowed to export ever-more sophisticated equipment, so they could plow those profits into developing new technologies. What began as an academic study in 1992 soon became election strategy, as Clinton’s campaign manager Ron Brown set out to woo corporate America to the Democrats. First to join the Democrats’ bandwagon with hefty campaign contributions and high-profile political support was the Silicon Valley computer industry, led by John Sculley, then-CEO of Apple, and Ed McCracken of Silicon Graphics.

After the election, William Perry became deputy secretary of defense and went to work putting the plan into action within the bureaucracy. Ron Brown, as secretary of commerce, was tasked with selling the decontrols to corporate America and Congress as part of an administration-wide “Trade Promotion” package, aimed at creating jobs and “growing” U.S. exports. On September 30, 1993, Brown issued a landmark report, “Toward a National Export Strategy,” which first made the argument—oft-repeated until the Loral-Hughes satellite scandals erupted last year—that each additional \$1 billion in U.S. exports creates 20,000 jobs in the U.S. Brown’s report urged the administration and Congress to facilitate exports to ten “Big Emerging Markets.” It just happened that the largest of those markets, Communist China, was most interested in purchasing precisely the type of technology that had long been subject to export restrictions because of its military and strategic applications. (As it turned out, U.S. companies exporting to China exported technology *and* jobs, since the Chinese required them to build factories in China to replace products they would otherwise buy from America.)

Regulations governing export controls span hundreds of pages, and are required under the Export Administration Act (EAA), first passed in 1979 to ensure that U.S. high-tech goods could not enhance the defense industries in Soviet bloc countries and Communist China. In 1993 and 1994 the administration tried to rewrite the EAA to eliminate most controls, but Congress balked; so they simply made an end run around the law, and dismantled the controls through executive branch regulations. The admin-

istration’s efforts reduced the voluminous licensing lists I had once received, and Defense Department officials now complain there are no more records of what has been shipped to the Chinese military—and thus no way to gauge the damage to U.S. national security. Like small-time hoods dreaming of the perfect crime, Clinton’s “best and brightest” thought they had covered up all traces of their acts.

After leaving the Hill in late 1993, I joined *Time* magazine. After a three-month investigation into Chinese procurement activities in the United States, I discovered the sale to a Chinese state-owned aerospace firm, CATIC, of virtually an entire defense plant owned by McDonnell Douglas in Columbus, Ohio, where the B-1 bomber had been made. The CATIC deal was part of an audacious, and until then unreported, Chinese effort to buy cutting-edge U.S. defense manufacturing gear at auctions, as more and more defense plants closed in response to the Pentagon’s defense build-down. My story was pulled by *Time* the week O.J. Simpson burst onto the front pages—but not because of O.J. The Commerce Department had written a letter to *Time*’s editors (which I subsequently obtained), calling my reporting “one-sided” and “unfair”—all this before my story was even printed! *Time* fired me within hours.

*The American Spectator* published my article some six months later (“China Shops,” March 1995), and has since published nearly a dozen of my feature-length investigations of China’s creeping infiltration of U.S. society. When I exposed the efforts of Defense Secretary William Perry to help the Chinese buy highly sensitive U.S. telecommunications gear over the objections of the National Security Agency (“Peking Pentagon,” April 1996), Perry threatened to sue this magazine for defamation. Instead, he called prominent conservatives to his office in an attempt to organize a counter-attack against me. Meanwhile, I learned, photocopies of my article were being passed around gleefully behind Perry’s back.

## MAKING THE CHINESE FEEL AT HOME

Congressman Cox at first intended to pursue my investigation into a Chinese government procurement ring in California (“California Take-Out,” *TAS*, November 1998), but abandoned the effort for lack of time and resources. Instead, he focused on the larger picture of Chinese intelligence and procurement operations in the United States—operations

★ ★ ★ ★ ★ ★ ★

**The Cox Report shows**

**that China is spying the**

**pants off us, and using**

**some 1,000 commercial**

**companies, employing**

**more than 10,000 Chi-**

**nese nationals residing**

**in the U.S., to do so.**

★ ★ ★ ★ ★ ★ ★

which have blossomed like a thousand flowers under the security-lax Clinton administration.

One of the more shocking details I uncovered in my investigation of China's California networks was that a front company owned by the PLA's largest weapons manufacturer had set up shop directly above the CIA office responsible for contacts with U.S. aerospace manufacturers in the Los Angeles area, where some of the agency's most secret projects have been developed. The Chinese operated there for more than two years without the CIA ever knowing. U.S. law enforcement officers in the L.A. area told me.

Given what we are now beginning to learn from the W-88 spy case, this monumental security lapse seems not an accident but

★ ★ ★ ★ ★ ★ ★

**“Confidence-building  
measures” with the  
People’s Liberation  
Army have meant the  
presence of Chinese  
observers at U.S mili-  
tary exercises and  
nuclear weapons labs.**

★ ★ ★ ★ ★ ★ ★

our policy convinces China that we are a threat, then that increases the possibility that China will devote the resources to significantly expand their strategic capabilities, and it is not in our interest to see that happen.” The priority, then, is reassuring China, not protecting our military secrets.

Bill Clinton and his top advisors see Communist China as a strategic partner of the United States, not a potential adversary. During his March 19 press conference, Clinton recited the litany of all the good things China has done in response to the administration's policy of engagement. “I think if we hadn't been working with China, China would not have signed the Comprehensive Test Ban Treaty, the Chemical Weapons Convention,” Clinton said. “They would very likely not have refrained from transferring dangerous technology and weaponry to countries that we don't believe should get it. I doubt if they would have helped us as much as they have to try to contain the North Korean nuclear threat or that we would have had the level of cooperation we had in trying to limit the Asian financial crisis.” But many of Clinton's assertions are a matter of dispute, with Congress complaining that China has actually encouraged North Korea to up

its price for opening an underground nuclear facility, and that China has continued to sell nuclear and missile technology to Iran, despite U.S. efforts to stop them.

The Pentagon has been engaged for the past two years in an extraordinary series of military-to-military exchanges and “confidence-building measures” with the People's Liberation Army, which include the presence of Chinese military observers at U.S. military exercises and visits to U.S. nuclear weapons labs. No reciprocal lab visits are allowed in China. During last July's Cope Thunder war games, which are the largest joint military exercises the U.S. holds with our Association of South East Asian Nations (ASEAN) allies, the Chinese were first-hand witnesses at command headquarters when a computer glitch brought U.S. re-supply efforts grinding to a halt. “That provided the Chinese with a tremendous piece of intelligence,” an aide to Republican Congressman Dana Rohrabacher said. “They were able to see first-hand how dependent we are on computers to run our entire military. It's no accident that the Chinese have been devoting tremendous resources to developing new information warfare techniques to capitalize on this vulnerability.” According to a January 1999 Pentagon report to Congress on the security situation in the Taiwan Strait, “the PLA has incorporated [information warfare]-related scenarios into several recent operational exercises,” putting into practice what they learned at last year's Cope Thunder. (Rohrabacher has been carefully monitoring the build-up of Chinese military capabilities for some time, and provided first-hand testimony of China's military occupation of the disputed Spratley Islands in the South China Sea when the Philippine air force flew him over Chinese warships anchored off the islands last December. For his efforts, he earned a White House reprimand for interfering with U.S. foreign policy.)

The U.S.-Sino defense exchange program was dreamed up by William Perry following the Taiwan Strait crisis in February 1996, as a means of increasing the comfort level of the Chinese (who had been made decidedly uncomfortable when two U.S. aircraft carrier battle groups steamed off the Chinese coast as a warning to Peking to cease its intimidating missile strikes during the Taiwanese presidential election campaign). TAS has obtained a copy of this year's exchange program “gameplan.” For March it shows the U.S. training a delegation of Chinese military procurement officers in program management, a set of skills sorely lacking in the PLA's weapons development efforts. In April the U.S. was scheduled to host a PLA Air Force logistics delegation. In June the PLA has been invited to observe a National Training Center demonstration by the 82nd Airborne, to include future-generation unmanned battlefield aerial surveillance vehicles (UAVs), remotely-targeted missiles, and battlefield management computer systems.

Also in June, a flight of U.S. Air Force C-130 and C-17 military transport aircraft will visit Peking, schooling the Chinese in how to improve their ability to airlift troops and materiel, skills undoubtedly of great use, say, in providing relief to flood victims (though also potentially helpful in moving troops across the Taiwan Strait). In August and September, the Chinese will attend an eight-week-long seminar in Hawaii on military medicine, perhaps in the hope of encouraging them to join international humani-

tarian missions. For several weeks in October and November, the PLA will participate in a workshop at the Sandia National Nuclear Laboratory on "cooperative monitoring," where the secrets of U.S. weapons-monitoring efforts, such as those arrayed against Iraq, will be shared. Both Secretary of Energy Richardson and National Security Advisor Sandy Berger have said the lab visits will not be canceled in the wake of the W-88 spy scandal, because there is "no evidence" that spying has occurred during foreign visits to U.S. nuclear labs or that any nuclear weapons information has been compromised.

But in fact, the Department of Energy itself, in a 1983 report, acknowledged that "a significant amount of important technology may have been lost to potential adversaries through visits" to the labs, a conclusion buttressed by a 1988 General Accounting Office review. On March 15 of this year, Senate Intelligence Committee Chairman Richard Shelby called on the administration to suspend Chinese visits to U.S. nuclear labs, since "the counterintelligence measures initiated by Secretary Bill Richardson will require several years to be fully implemented."

## THE MALOOF MEMO

When the Clinton administration took power in 1993, the Chinese had two ICBMs capable of targeting the United States. Today, says Deputy National Security Advisor Gary Samore, that has grown to "less than two dozen." But thanks to the theft of the W-88 warhead design, and the transfer by U.S. satellite manufacturers of technology used to boost multiple satellites to different orbits, the Chinese may be able to put up to five Multiple Independent Reentry Vehicle (MIRV) warheads on each missile. According to reports for the Office of Naval Intelligence, the Chinese will soon begin building two new-generation missile systems, the DF-31 and DF-41, also equipped with multiple warheads, which could expand their nuclear forces exponentially over the next five to ten years. From the bottom rank among the five declared nuclear weapons states (not including India and Pakistan, which demonstrated their nuclear weapons capabilities last year), China will soon slip into third place, just behind the United States and Russia. All this has happened as a direct result of the Clinton administration's policy of engagement.

Similarly, prior to January 1996, when computer export controls were lifted after intensive lobbying from Silicon Graphics and other top DNC contributors, the Chinese had only three U.S. High Performance Computers (HPCs), all of which were subject to stringent Defense Department monitoring. In April 1997—just 14 months after the decontrol—Undersecretary of Commerce William Reinsch told Congress that U.S. companies had sold 46 supercomputers to Chinese end-users, and that the Chinese were not allowing the U.S. government to verify how they were being used. By June 1997, concerned that we were helping the PLA to improve weapons design, missile targeting, and nuclear simulation, the House voted to restore licensing requirements on HPCs. But the measure was ultimately defeated under intense industry and administration pressure.

In January 1999, Reinsch's Bureau of Export Administration delivered its first congressionally mandated report detailing supercomputer exports over the preceding 12 months. Out of a

total of 390 HPCs exported by the United States during that period, 191 of them had gone to China. Despite U.S. efforts, the Chinese only allowed government officials to inspect three of them once they had reached China. Congressional sources tell TAS that they have been told by administration officials that as many as 600 HPCs have been sold to the Chinese since the 1996 decontrols—more raw computing power than can be found in the Pentagon and the Department of Energy's nuclear weapons labs, combined.

Supercomputers are only one element in a deadly mix of high technologies released for sale to the Chinese by the Clinton administration since 1993. An internal memorandum written by Michael Maloof of the Pentagon's Defense Technology Security Administration (DTSA), subpoenaed by the Cox committee, paints an astonishing picture of the cumulative impact of U.S. technology transfer to the Chinese military over the past five years. The combination of supercomputers, satellite sales, and advanced telecommunications switching technology since 1994 "have provided the Chinese military with a nationwide encrypted command, control, communications, computers and intelligence (C4I) network that will serve it well into the next century," Maloof warned his superiors. "Together, they provide the PLA with a communications infrastructure that it could not have developed on its own."

Extensive manufacturing technologies were decontrolled along with the actual products U.S. companies were allowed to ship to China. Since 1993, the PLA has been importing massive amounts of equipment to manufacture fiber-optics cable, which allows for secure communications links impervious to electronic eavesdropping. And companies tied to former colleagues of then-Deputy Defense Secretary William Perry led the way in transferring encrypted Asynchronous Transfer Mode (ATM) telephone switching equipment, now used by the PLA for its military communications network. "The decision to allow... ATM switching technology in 1994 occurred over the objection of DoD technical experts," Maloof wrote. "Despite initial NSA concerns, it was silent when the decision finally occurred." As I wrote in "Peking Pentagon" in April 1996, it appeared that William Perry personally intervened to get NSA to drop their objections to the sale of this technology, despite the fact that the Chinese buyer was a PLA-owned company.

More recently, Maloof wrote, was the decision to allow Hughes to sell more than 500 ground stations to accompany the telecommunications satellites sold by Hughes to companies controlled by the Chinese military. "The VSAT ground station terminal equipment... was supplied and wittingly installed by Hughes for Chinese ground and rocket forces and the PLAAF [Air Force]," Maloof wrote. "This equipment also was available to the Ministry of State Security," and included "an additional port for encryption equipment." Chinese encryption efforts have been given "a great boost... from the U.S. high performance computers it has received and the training in software development." A spokesperson for Hughes Network Systems, Judy Blake, declined to comment on the Maloof memo or respond to detailed questions about Hughes's business in China. Export licensing

*(Continued on page 76)*

CLINTON'S ENERGY DEPARTMENT  
CARES MORE ABOUT ENVIRONMENTAL  
CORRECTNESS THAN NATIONAL SECURITY.  
THE LATEST CHINESE SPY CASE IS JUST  
A HINT OF THE DAMAGE IT HAS DONE.

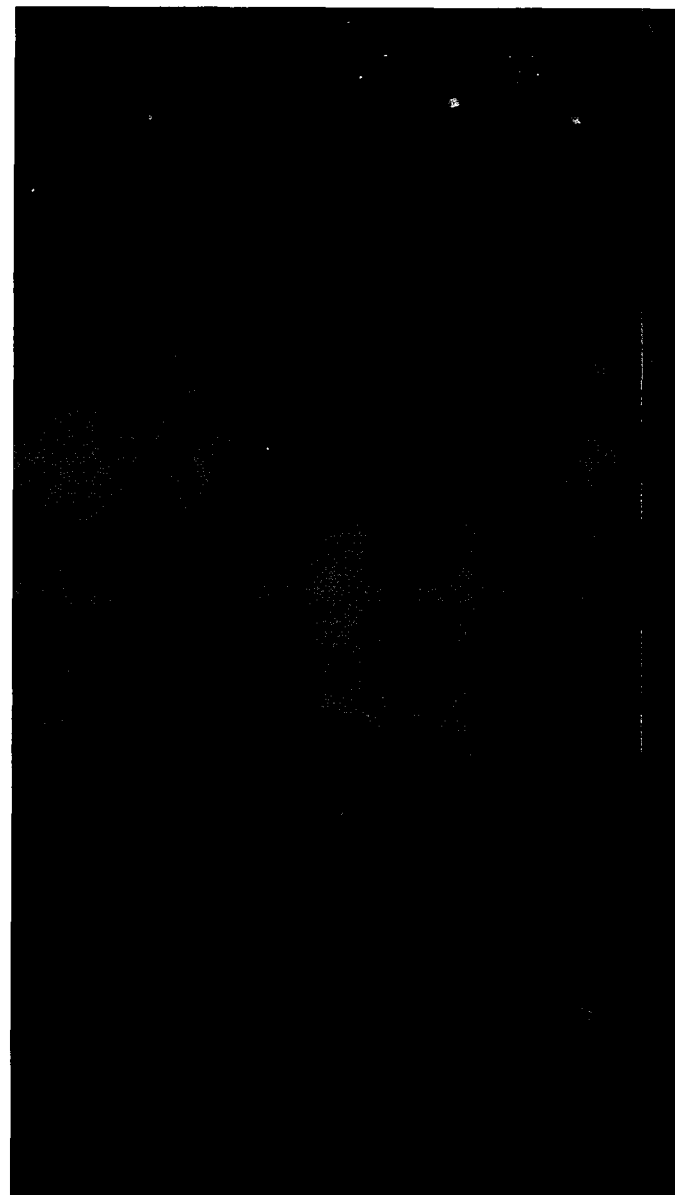
## JOHN B. ROBERTS II

peration Desert Glow began like clockwork at 0900 on the morning of June 6, 1989. Just outside Denver, Colorado, almost a hundred heavily armed federal agents, including seventy special agents from the Federal Bureau of Investigation, descended en masse upon the Rocky Flats Nuclear Weapons Plant.

FBI Agent Jon Lipsky, whose investigative work led to the creation of Operation Desert Glow, was taking no chances that morning. Rocky Flats' senior managers were gathered inside one of the hundred buildings sprawled over four hundred acres at the Department of Energy complex. The cover story the FBI gave them was that they should all assemble for a briefing on a threat from the environmental extremist group Earth First to carry out a terrorist attack on the plant, which produced plutonium triggers for America's atomic weapons arsenal.

---

JOHN B. ROBERTS II is a writer and television producer.



The waiting executives were unaware that the agents who were already descending on them would thoroughly search the Rocky Flats facilities for eighteen days, guard it twenty-four hours a day, and gather more than 104 boxes of evidence. They didn't know that the innocuous-looking airplane that had flown over the complex on three separate nights six months earlier was operated by the FBI and crammed with infrared surveillance equipment.

Assistant U.S. Attorney Ken Fimberg would later recall how strange it seemed, sitting in the airplane next to Agent Lipsky during the nighttime surveillance flights, to be spying on a U.S. facility in Colorado. Fimberg, a self-described liberal Democrat and environmentalist who had clerked for the Environmental Defense Fund, was an ardent advocate of Lipsky's operation. More than anyone else in the federal government, the two thirty-something friends were responsible for the entire probe. Spurred on by Agent Lipsky, Fimberg would eventually take the fight for criminal prosecutions of those indi-