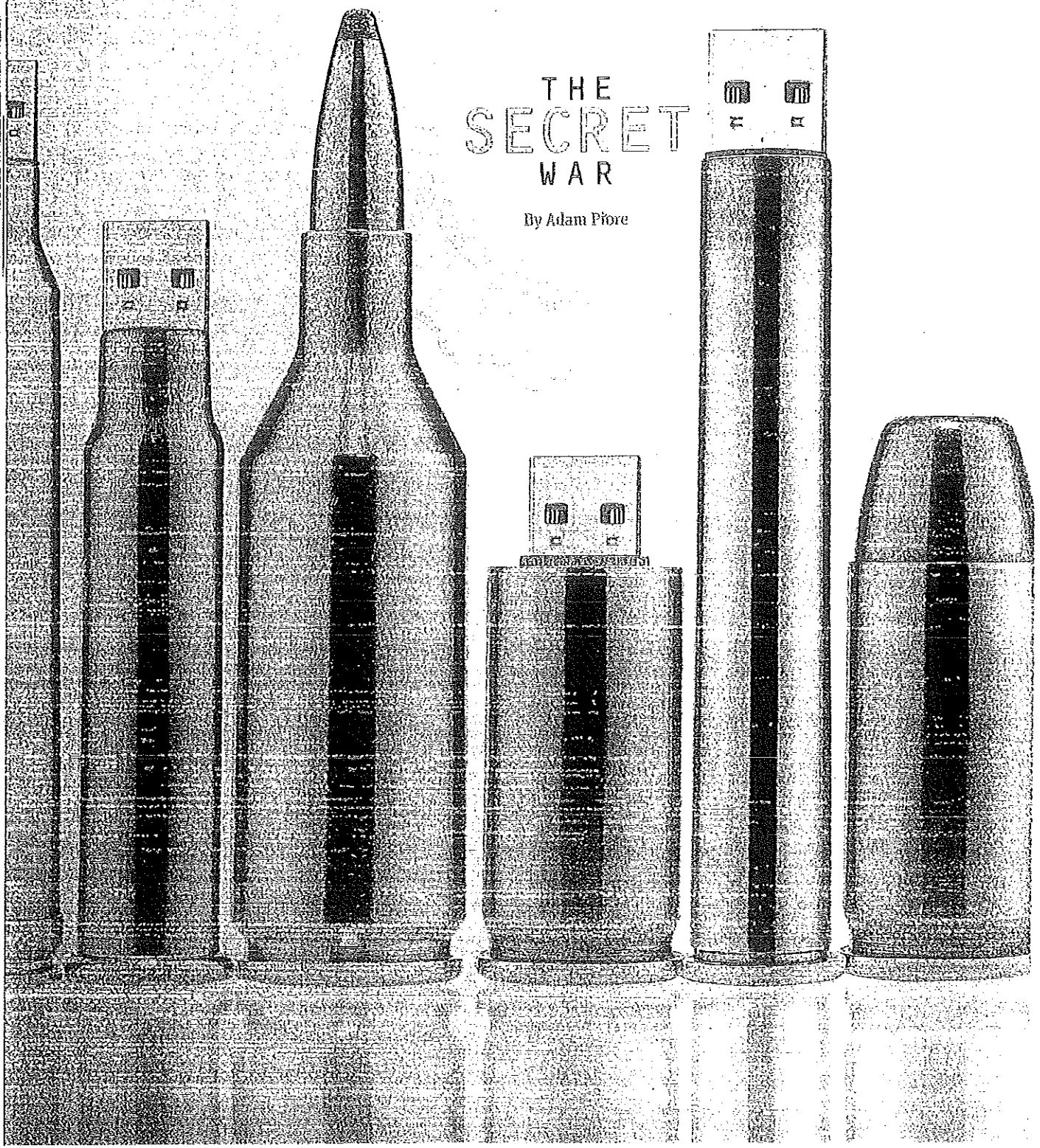
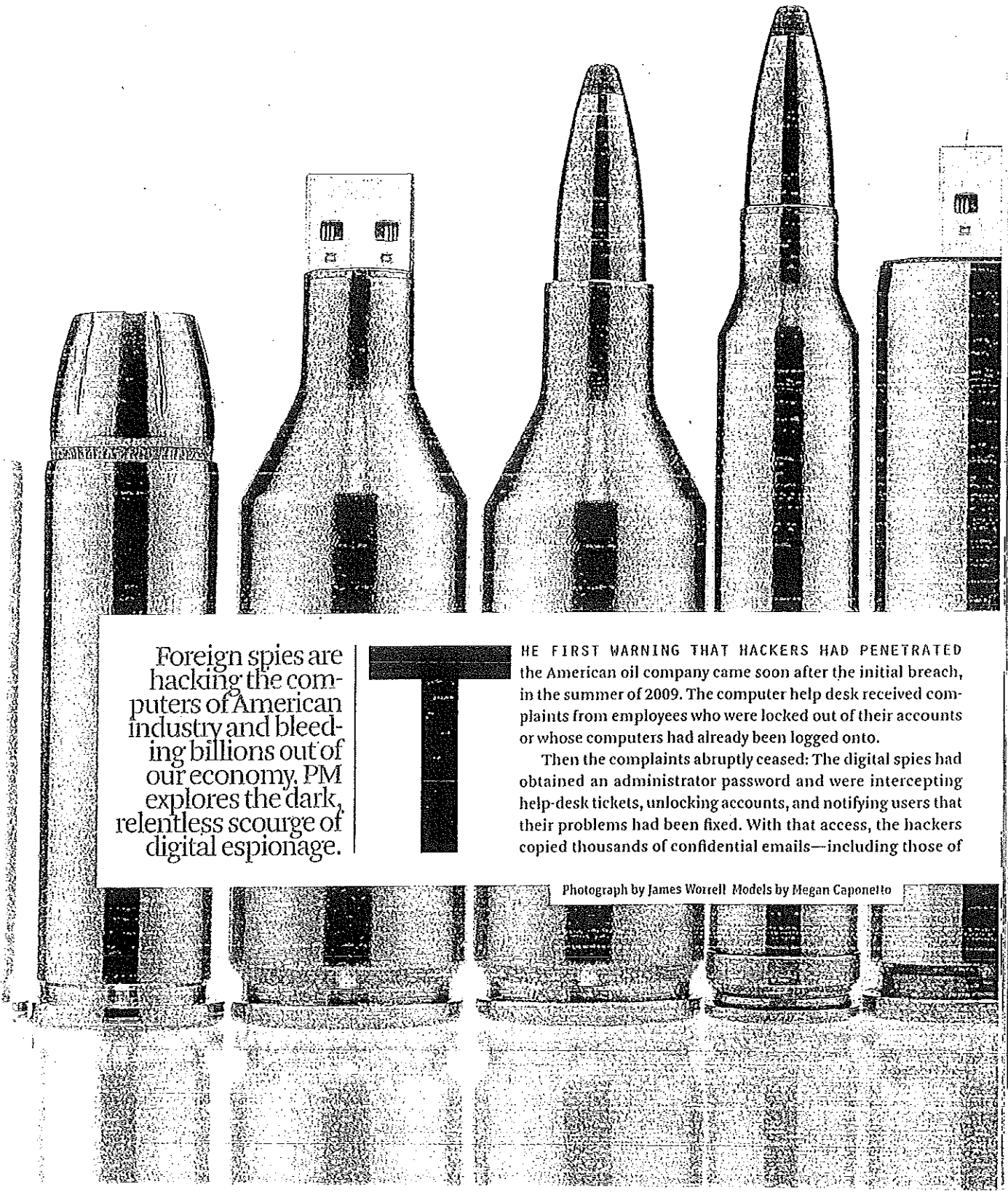
THE SECRET WAR

By Adam Piore



Story



Foreign spies are hacking the computers of American industry and bleeding billions out of our economy. PM explores the dark, relentless scourge of digital espionage.

THE FIRST WARNING THAT HACKERS HAD PENETRATED the American oil company came soon after the initial breach, in the summer of 2009. The computer help desk received complaints from employees who were locked out of their accounts or whose computers had already been logged onto.

Then the complaints abruptly ceased: The digital spies had obtained an administrator password and were intercepting help-desk tickets, unlocking accounts, and notifying users that their problems had been fixed. With that access, the hackers copied thousands of confidential emails—including those of

Photograph by James Worrell Models by Megan Caponetto

top executives—and transmitted them to China in massive files late at night, after the oil company's employees had left for the day.

By the time the FBI informed the company of suspicious network traffic in the summer of 2010, Chinese firms had outbid the oil company on several high-stakes acquisitions by just a few thousand dollars. But it could have been far worse: For months, malware that allowed the hackers to take over terminals had been burrowing deeper into the company's systems and had wormed its way into computers that controlled oil-drilling and pipeline operations.

"People were alarmed that their email was compromised, but the hackers could have crippled the business," says Jonathan Pollet, the founder of Red Tiger Security in Houston. In early 2011, Pollet helped the oil company identify some of the hackers' breaches; he refused to name the company, citing a confidentiality agreement.

The example Pollet cites is just one incident in an ongoing, aggressive campaign of electronic espionage that costs U.S. firms billions of dollars, endangers our military secrets, and threatens to erode our technological edge, as computer hackers—often but not exclusively traced to China—help their clients, and their countries, gain the upper hand in business deals and steal intellectual property. (An October 2011 report prepared for the Director of National Intelligence titled "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace" explicitly accuses China and Russia of hacking U.S. companies, calling Chinese hackers "the world's most active and persistent perpetrators of economic espionage.")

The phenomenon blurs the lines between white-collar crime, international spying, and even acts of war, but the attacks are known in the intelligence community as advanced persistent threats, or APTs. Well-financed, patient teams of hackers that U.S. intelligence agencies believe are backed by foreign governments now constitute a major national security risk. The hackers use tactics that are inherently difficult to trace and choose targets that have deep roots within U.S. infrastructure, government, and military. Recent news accounts have identified APT victims that include Google, ExxonMobil, Royal Dutch Shell, Morgan Stanley, Dow Chemical, Symantec, Northrop Grumman, and Lockheed Martin, to name just a few.

Private industry is understandably reluctant to reveal such breaches, even to the government: If a digital attack strikes fear in the hearts of a company's executives, one can only imagine how it would make shareholders feel. But digital spying is like a cockroach infestation—for every one that you see, thousands thrive out of view. "I can't find an organization, an entity, a business, or a department that hasn't suffered from cyber intrusions," says Gordon M. Snow, assistant director of the FBI's Cyber Division. "If they really believe they haven't, they're just not aware of it yet."

In August 2011, a report by the security firm McAfee detailed hacks into some 72 public and private computer networks in 14 countries and warned of "the biggest transfer of wealth in terms of intellectual property in history."

Technology theft is the most common motive for digital espionage, but China and other nations have used it to squelch internal political dissent as well. Stolen source code from Google was used to hack into the accounts of Chinese dissidents, and after an Iranian hacker broke into Dutch security firm DigiNotar, the stolen technology was used to help his government spy on troublemakers in Iran. These attacks can cause collateral damage that compromises the security of everyone online. Digital security certificates from DigiNotar were part of the basic verification system of the Internet. If you can fake one of those, you can fool a browser into thinking any site is safe.

A History of Hacks

THE UNITED STATES ITSELF IS NO slouch at cyber spying. The National Security Agency and the Pentagon possess the most sophisticated signals intelligence and digital warfare technology in the world. That gives us the ability to spy on foreign cellphone calls, shut down enemy air defenses, or even remotely cause equipment in an adversary's weapons facility to self-destruct.

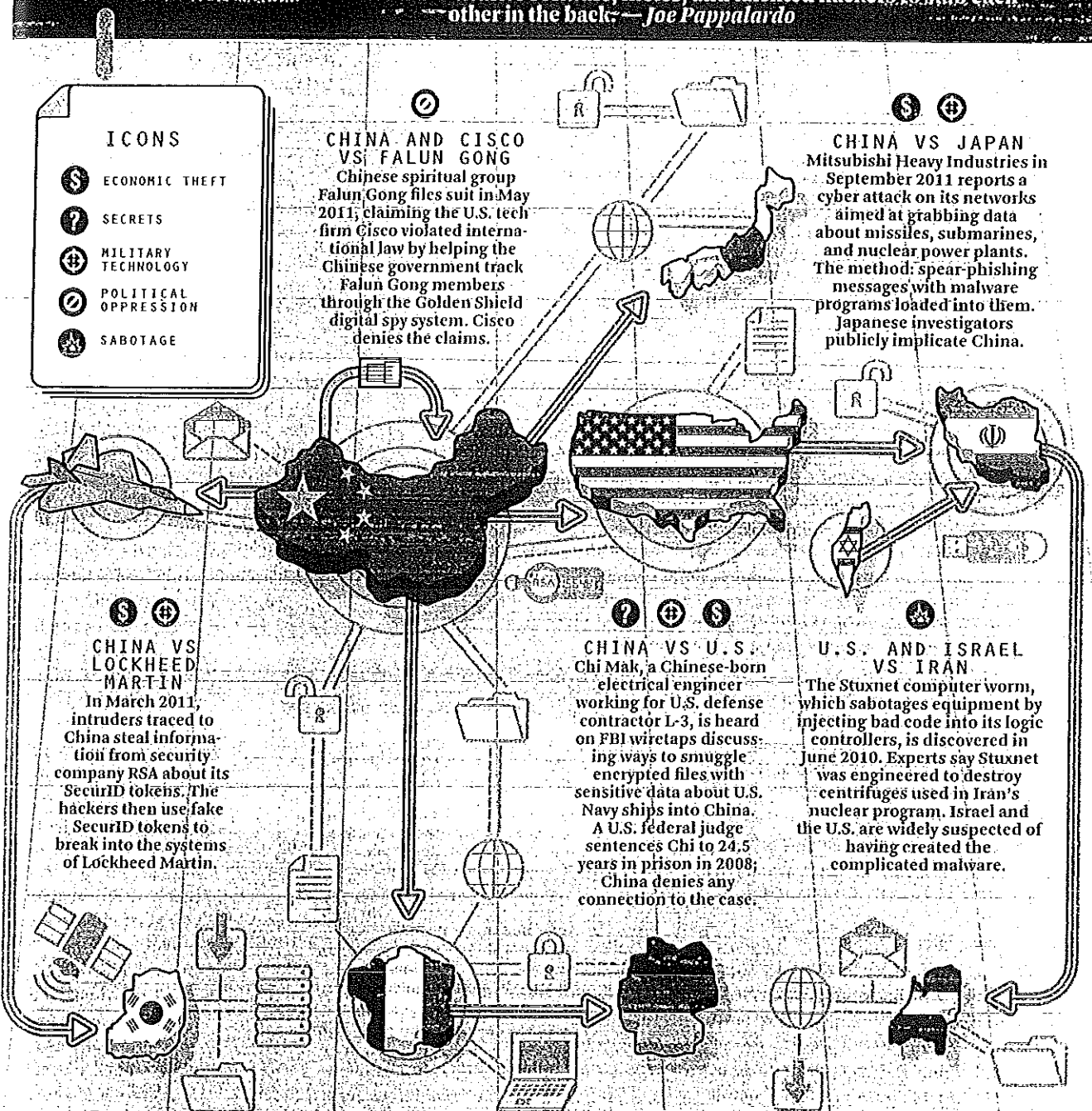
But former U.S. officials insist the government does not engage in economic espionage or intellectual property theft from foreign companies. In part, they contend,

German chancellor Angela Merkel (above) confronted China's premier, Wen Jiabao, during a 2007 state visit to Beijing after the magazine *Der Spiegel* reported that computers in the German chancellery had been infiltrated by Chinese malware. German officials traced the attack back to Trojan programs hidden inside Microsoft Word and PowerPoint files. The officials discovered the software trying to offload 160 gigabytes of data from government computers and send it to a botnet of hijacked computers in South Korea. The Germans believed the botnet was controlled by the People's Liberation Army.

ILLUSTRATION BY JACOPO ROSATI

WHO'S SPYING ON WHOM?

High-tech espionage is a game with no rules. In this secretive world, rival countries and multinational companies use invasive software, moles, and talented hackers to stab each other in the back. —*Joe Pappalardo*



that's because there is little IP we would want to steal, and to do so would undercut our efforts to discourage such theft by other nations. Private U.S. companies, meanwhile, would be breaking U.S. law if they hacked into the servers of state-owned competitors in places like China and Russia—although some U.S. multinationals have been accused of dirty business overseas (see "Who's Spying on Whom?" page 55). "The U.S. has an enormous stake in the integrity of the intellectual property regime," says Joel Brenner, former head of U.S. counterintelligence during the Bush and Obama administrations and the author of *America the Vulnerable*, a book on digital espionage published last September. "Many of our adversaries don't believe we don't do this. But it's really true. We don't." According to James Lewis, a digital security expert at the Washington, D.C.–based Center for Strategic and International Studies, this apparent unwillingness to retaliate presents "an asymmetric disadvantage" that our rivals are exploiting to win an emerging digital cold war.

Computer espionage has a history almost as long as that of the modern Internet. In the late 1980s, the German hacker Markus Hess and several associates were recruited by the KGB to penetrate computers at American universities and military labs. They made off with sensitive semiconductor, satellite, space, and aircraft technologies. Today, China, Israel, and Russia are reportedly the most aggressive about stealing secrets. But China is playing a game of a different magnitude. "The Chinese didn't create this problem," Brenner says. "But there's no question China is the worst offender now. They are all over us. It's just relentless."

Experts believe today's attacks on U.S. industry are an extension of a series of attacks on American military computer networks that took place in the late '90s and early 2000s. The assault has netted the Chinese sensitive military technologies that might one day be used against us. Then, as now, the Chinese government has vehemently denied that it has any state-sponsored hacking program, calling U.S. allegations groundless and irresponsible.

Plausible deniability is precisely what makes digital espionage such an effective tool. It's difficult to detect and impossible to prove—and thus can't be used to justify retaliation. Digital-security experts call this the attribution problem. "At most, you know the immediate computer involved in attacking you or receiving the stolen data—and sometimes you don't even know that," says Columbia University computer scientist Steven Bellovin, who advises the Department of Homeland Security on the issue. "But you don't know who actually controls the computer. It could be another hacked computer someplace that somebody else is controlling from somewhere else."

Still, few buy the Chinese denials. There have simply been too many attacks traced to the mainland. Last spring, secret State Department cables obtained by WikiLeaks and made public by Reuters detailed a widespread digital spying operation, Byzantine Hades, linked to the People's Liberation Army Chengdu Military Region First Technical Reconnaissance Bureau, an electronic espionage unit of the Chinese military. According to the cables, Byzantine Hades targeted not only the U.S. government and indu try, but also high-level European official The Chinese hackers even managed t remotely activate the computer micr phones and Web cameras of French off cials so they could peek in on everythin from office gossip to high-level diplomati planning sessions. In the past, survei lance like that would have required spie to know where their targets were stayin and mic the room—but in the age of cel phones and laptops, spies can listen in o foreign officials half a world away.

Anatomy of an Attack

IN FEBRUARY 2011, MCAFEE released a report detailing a series o hacks called Night Dragon. Emanatin from locations in China and aimed at si global oil, gas, and petrochemical compa nies, the hacks resembled the oil compan attack described by Pollet. The media late identified the victims as ExxonMobil Royal Dutch Shell, BP, Marathon Oil ConocoPhillips, and Baker Hughes, all o which declined to discuss the report wher asked by POPULAR MECHANICS.

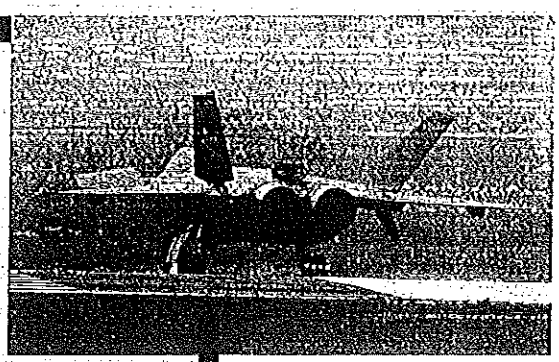
Regardless, the methods described by both Pollet and McAfee are straight out of the playbook of Chinese-based APTs. Instead of trying to identify vulnerabilities in a company's firewall, APTs focus on exploiting the one thing that's impossible to control—the vulnerabilities of company employees.

The hackers Pollet investigated found personal information about the oil company's executives on social-networking sites such as Facebook and Myspace. Then they crafted emails aimed at enticing the executives to click on a poisoned link.

"The initial attack is very subtle," Pollet says. "It no longer says, 'I am a Nigerian prince and need to hide a bank account.' If the hacker can find an executive who likes to restore old cars and can find the names of some of his friends, he will send an email saying 'Hey, I was talk-

DON'T GET HACKED

- Foreign spies aren't after your PC, says Alex Stamos, CTO of security firm iSEC Partners, but the code from their hacks can be quickly mimicked by cyber criminals. "It's like R&D for the broader malware market," he says. Keep your software updated to stay safe.
- Any employee of a large company can become an attack vector for spies looking to steal data. "Be paranoid about what you click on," Stamos says—even emails that seem to be from friends.
- Be careful if you store personal data on your work computer. If the machine becomes infected, your employer can erase everything.
- USB drives are classic tools for getting malware through a firewall. If you don't trust where a drive came from, don't plug it into your computer.



ast year, the Chinese military unveiled the Chengdu J-20 stealth fighter. Some U.S. intelligence experts see the J-20 as the result of a long campaign of technology theft. The Chinese are believed to have inspected and reverse-engineered aspects of an American F-117 Nighthawk downed in Serbia in 1999. Also, in the early 2000s, Chinese spies are suspected of hacking into a U.S. military research facility in China Lake, Calif., and making off with computer files relating to stealth technology.

g to our friend Paul, and
said you were restoring
50s Chevys. I found this
eat website you should
eck out.'"

When the victim clicks
the link, it takes him
a webpage where mal-
are loads onto his com-
ter. It sits there for days
til it wakes up and
ones home.

The malware might post a code to a
witter account or post a comment as
mple as "I'm going skiing on Saturday"
a blog. That beacon alerts hackers
at their malware has taken root and is
ady for instructions. The hackers can
en respond with coded directives by
e same means.

It wasn't until a year into the hack on
e oil company that the FBI contacted
ecutives and informed them they had
otted data traffic leaving their network
d heading to servers in China known to
e used to command and control net-
orks, Pollet says. The FBI's Snow says he
nnot comment on specific cases. But it
as certainly not the first time the FBI
epped in. The current campaign of
ber espionage is so widespread, he says,
at it has forced a "significant cultural
ift" in the way the FBI handles cyber-
trusions. Previously, "the No. 1 priority
as to protect the operational security of
e investigation and the prosecutive
uities on the criminal side." While
ose goals are still important, "it's even
ore important that the victims under-
nd they have been victimized," he says.

mergency Response

TER THE FBI ALERT, THE OIL
mpany brought in security firms Red
ger and Mandiant to expunge the
truders. But expelling an APT isn't as
mple as it sounds. "They are agile,
namic, and, if you defeat them once,
ey're going to change their tactic," says Richard Bejtlich, chief security officer for Mandiant, who also would not comment on the specifics of the oil company attack. The attackers, he notes, are usually in it for the long haul and are likely to return if the company still has intelligence on its networks that the hackers or their employers consider of value.

The best approach once an intrusion is detected is not to tip your hand until you are ready to respond with a serious defense. Countermeasures usually involve first identifying as many infected computers as possible by looking for suspicious software on hard drives and tracking which computers have been contacting suspicious host servers. The response team then attempts to pull as many infected computers as possible off the server at once, "by any means necessary," Bejtlich says. "In some cases it's literally pulling a cable out of the computer."

But often it's impossible to know whether all the malware has been successfully removed. And even if it has, the attacker will often attempt to break in once again, using more sophisticated, perhaps never-before-seen code. That's one of the reasons that many in the intelligence community are calling for a new security paradigm, one that places an emphasis on information sharing and preventive measures.

The government can go only so far to protect the networks of private companies. In the past year, the Department of Defense launched a pilot program with the defense industrial base that helps contractors improve security and share information about emerging forms of malware. Most U.S. companies, however, remain shockingly vulnerable to massive security breaches and naive about the extent of the problem.

Even with cooperation, most security experts believe that keeping a capable and determined adversary out of a system is impossible.

"Perimeter defense is finished," Brenner says. "If you want to talk about really confidential stuff in email, you've got to understand that if you've got a real sophisticated adversary, they're reading it."

The FBI's Snow agrees. "We have to have a cultural shift in the nation where we understand that there is no secure system, that people are going to be hacked," he says.

As for retaliation? Bejtlich says he often gets questions from high-level executives who want to "hack back," even if all that means is retaliating against a Chinese computer with a virus that will disable it.

"There is sufficient resistance from outside counsel because it would violate U.S. law, and in U.S. government agencies, there is no support to do that," Bejtlich says.

When asked if compromised companies might use the knowledge that they have been infiltrated to feed spies false data, Bejtlich scoffed. "Those deception maneuvers are so far beyond the capability of any private corporation that no one could pull that off," he says. "You couldn't protect the planning. The bad guys will see it all and laugh." PM