VANITY FAIR

National Security

Enter the Cyber-dragon

Hackers have attacked America's defense establishment, as well as companies from Google to Morgan Stanley to security giant RSA, and fingers point to China as the culprit. The author gets an exclusive look at the raging cyber-war—Operation Aurora! Operation Shady rat!—and learns why Washington has been slow to fight back.

Lying there in the junk-mail folder, in the spammy mess of mortgage offers and erectile-dysfunction drug ads, an e-mail from an associate with a subject line that looked legitimate caught the man's eye. The subject line said "2011 Recruitment Plan." It was late winter of 2011. The man clicked on the message, downloaded the attached Excel spreadsheet file, and unwittingly set in motion a chain of events allowing hackers to raid the computer networks of his employer, RSA. RSA is the security division of the high-tech company EMC. Its products protect computer networks at the White House, the Central Intelligence Agency, the National Security Agency, the Pentagon, the Department of Homeland Security, most top defense contractors, and a majority of Fortune 500 corporations.

The parent company disclosed the breach on March 17 in a filing with the Securities and Exchange Commission. The hack gravely undermined the reputation of RSA's popular SecurID security service. As spring gave way to summer, bloggers and computer-security experts found evidence that the attack on RSA had come from China. They also linked the RSA attack to the penetration of computer networks at some of RSA's most powerful defense-contractor clients—among them, Lockheed Martin, Northrop Grumman, and L-3 Communications. Few details of these episodes have been made public.

The RSA and defense-contractor hacks are among the latest battles in a decade-long spy war. Hackers from many countries have been exfiltrating—that is, stealing—intellectual property from American corporations and the U.S. government on a massive scale, and Chinese hackers are among the main culprits. Because virtual attacks can be routed through computer servers anywhere in the world, it is almost impossible to attribute any hack with total certainty.

> **"The difference with cyber is there are people trying to fly planes into buildings every day now.**
>
> **And everybody just looks the other way."**

Dozens of nations have highly developed industrial cyber-espionage programs, including American allies such as France and Israel. And because the People's Republic of China is such a massive entity, it is impossible to know how much Chinese hacking is done on explicit orders from the government. In some cases, the evidence suggests that government and military groups are executing the attacks themselves. In others, Chinese authorities are merely turning a blind eye to illegal activities that are good for China's economy and bad for America's. Last year Google became the first major company to blow the whistle on Chinese hacking when it admitted to a penetration known as Operation Aurora, which also hit

Intel, Morgan Stanley, and several dozen other corporations. (The attack was given that name because the word “aurora” appears in the malware that victims downloaded.) Earlier this year, details concerning the most sweeping intrusion since Operation Aurora were discovered by the cyber-security firm McAfee. Dubbed “Operation Shady rat,” the attacks (of which more later) are being reported here for the first time. Most companies have preferred not to talk about or even acknowledge violations of their computer systems, for fear of panicking shareholders and exposing themselves to lawsuits—or for fear of offending the Chinese and jeopardizing their share of that country’s exploding markets. The U.S. government, for its part, has been fecklessly circumspect in calling out the Chinese.

Most companies have preferred not to talk about or even acknowledge violations of their computer systems, for fear of panicking shareholders and exposing themselves to lawsuits—or for fear of offending the Chinese and jeopardizing their share of that country’s exploding markets.

A scattered alliance of government insiders and cyber-security experts are working to bring attention to the threat, but because of the topic’s extreme sensitivity, much of their consciousness-raising activity must be covert. The result in at least one case, according to documents obtained by *Vanity Fair,* has been a surreal new creation of American bureaucracy: government-directed “hacktivism,” in which an intelligence agency secretly provides information to a group of private-sector hackers so that truths too sensitive for the government to tell will nevertheless come out.

This unusual project began in March, when National Security Agency officials asked a private defense contractor to organize a cadre of elite non-government experts to study the RSA cyber-attacks. The experts constituted a SEAL Team Six of cyber-security and referred to their work as Operation Starlight. “This is the N.S.A. outsourcing the finger-pointing to the private sector,” says one person who was invited to join the group and has been privy to its e-mail logs. The N.S.A. provided Operation Starlight with the data it needed for its forensic analysis.

Operation Starlight’s secret “Working Draft Version 0.2” report, dated April 4, 2011, has a cover page that bears a galactic image resembling a meteor-pockmarked moon. The source who provided *Vanity Fair* with the document emphasized that the draft is just that—a draft—and said that Starlight’s provisional conclusions are subject to change. (The source also says that Operation Starlight’s analysis will continue for a matter of months, and possibly as long as a year.) As of April, however, the draft report argued that the RSA hacks represent an “organized, concerted campaign on behalf of China.” It also suggested that RSA had been under attack, perhaps by different groups, for months prior to the attack that the company acknowledged in March. In July, in the lengthiest interview RSA officials have given since their troubles began, executive chairman Art Coviello and EMC chief security officer Dave Martin resisted those suggestions. Coviello admitted that the SecurID hack was preceded in March by “pretty heavy-duty reconnaissance.” He refused to say specifically when the attack began or ended, but described the duration as “a matter of days, not weeks.” He agreed that the evidence suggested that the SecurID attack had come from a nation-state, but declined to accuse a specific country.

"The Adversary"

If you were designing a new jetfighter for Lockheed Martin, sooner or later you would have to travel to an air-force base to talk to military personnel about what they want the new jetfighter to do. Meetings over, you'd go back to your hotel room, fire up your laptop, and log on to Lockheed's remote network to get some work done. In order to log on, you'd have to glance down at an inch-long red-white-blue-and-gray plastic key-chain fob, shaped vaguely like a key, on which a little L.E.D. screen displays strings of six to eight digits that change every minute or so. Adding those numbers to the basic password that you'd memorized, you would type the whole hybrid string of characters into the Lockheed-network log-in box—and then you would be in. That key fob, called a SecurID token, is RSA's best-known product. The strings of numbers on its screen are generated by a microchip using the SecurID algorithm and a unique cryptographic seed.

Each numeric string is called a "one-time password," and, when entered in combination with your own chosen password, it bumps up your network's security by means of "two-factor authentication." As of March 2011, RSA commanded 70 percent of the market for this form of security. More than 25 million of these tokens are in circulation, and for years they have been used by most U.S. intelligence and military officers, defense contractors, White House officials, and Fortune 500 executives.

> ***Within two months, the impossible had come to pass. Attackers … had broken into Lockheed Martin's network using SecurID information stolen from RSA.***

So it was of great concern to many of the world's most powerful people when, on the same day the company alerted the S.E.C., executive chairman Coviello posted an open letter to customers on RSA's Web site, announcing that the company's security system had identified "an extremely sophisticated cyber attack in progress," an attack that "resulted in certain information being exported from RSA's systems," some of which was "specifically related to RSA's SecurID two-factor authentication products."

The letter was so vague and judiciously bland that many readers assumed what the later Lockheed hack seemed to suggest: that SecurID's seed-key algorithm and some, if not all, of its seed-key database may have been stolen. RSA executives have consistently refused to say precisely what the company lost. Coviello did say in an interview that "the information taken, in and of itself, would not allow a direct attack." An attacker, he went on, "would have had to get other information that only the customer had in their possession." To weaponize the stolen SecurID information would require a strategy of coordinated intrusions, involving attacks not just on RSA but also preliminary attacks on every other target company—something that seemed so complicated as to be almost impossible. Yet within two months, the impossible had come to pass. Attackers, whom security experts often refer to in the satanic singular as "the Adversary," had broken into Lockheed Martin's network using SecurID information stolen from RSA.

On April 1, the RSA Web site published a blog posting titled "Anatomy of an Attack" by the company's head of new technologies, Uri Rivner. Chatty and anecdotal, it described the "2011 Recruitment Plan" e-mail, one of two e-mails sent to low-level employees. ("You wouldn't consider these users particularly high profile or high value targets," Rivner wrote.) The post said nothing about when the attack began, how long it lasted, or what was taken, but some of Rivner's language seems intended to suggest that the intrusion was short-lived: "Since RSA detected this attack in progress, it is likely the attacker had to move very quickly to accomplish anything." Rivner wrote that the RSA hackers used a Flash zero-day vulnerability—that is, a flaw in the code that is unknown to the program's developers and has not been used in prior attacks—to install an extremely common downloader called Poison Ivy. But he gave no details about the malware that Poison Ivy downloaded into RSA's system.

Rivner characterized the attackers' technique as a form of "Advanced Persistent Threat," or A.P.T.—security lingo for "Pretty sure it came from China," in the words of Brian Krebs, a leading cyber-security blogger. According to Operation Starlight's draft report, some of the malware that was used to attack RSA was "compiled," or written, in December of 2010—a full three months before the SecurID hack. "APT attack groups typically launch their attacks within hours of compilation, providing a useful date indicator for the targeted intrusion," the draft says. The draft acknowledges that "these compile dates are easily modified," but it goes on: "The earliest compile date [of malware used in the RSA hack] that has not been materially modified is 12/22/2010, potentially providing at least three months of persistent access into RSA operations." One prominent cyber-security analyst with firsthand knowledge of the RSA intrusions confirms that RSA appeared to be under attack by other A.P.T. groups prior to the SecurID hack. These groups "were not going after seed values," the analyst says, though "we don't know whether they were doing advanced reconnaissance" for the later attacks. In addition, RSA was being hit by "drive-by malware," meant to harvest run-of-the-mill kinds of data. Coviello, for his part, says "we have no evidence" of intrusions beginning earlier than March.

> "The Adversary stayed under the radar by making an ingeniously malevolent move: taking control of the companies' virtual Help Desks, impersonating their IT help-desk staff, and answering employees' service complaints themselves."

The SecurID hack, whenever it began and however long it lasted, was a sophisticated intrusion. Though RSA has not said how the Adversary managed to stay undetected inside its network, previous examples of stealth techniques used by A.P.T. attackers illustrate how resourceful they can be. Jonathan Pollet, the head of Red Tiger Security, based in Houston, Texas, was hired in 2010 by three Fortune 100 companies to clean up after a spate of cyber attacks that came from servers in China. (These intrusions were similar in many ways to the attacks known as Night Dragon, which targeted various energy industries at about the same time.) Pollet says the victims knew that something strange was going on because they kept getting locked out of their e-mail accounts for no apparent reason. But the Adversary stayed under the radar by making an ingeniously malevolent move: taking control of the companies' virtual I.T. help desks, impersonating their I.T. help-desk staff, and answering employees' service complaints themselves. "Attackers want to be a parasite, want to make sure the host is happy," says Pollet. "So if they know the help desk is going to get overwhelmed with complaints, they decide, 'Let's just solve these problems ourselves.' "

Body Count

China's aggressive campaign of cyber-espionage began about a decade ago, with attacks on U.S. government agencies. (The details have still not been divulged.) Then China broadened the scope of its efforts, infiltrating the civilian sector in order to steal intellectual property and gain competitive advantage over Western companies. Dmitri Alperovitch, vice president of threat research at McAfee, who gave Aurora and Night Dragon their names and has written definitive studies of A.P.T. attacks, says that "today we see pretty much any company that has valuable intellectual property or trade secrets of any kind being pilfered continually, all day long, every day, relentlessly."

> **"Today we see pretty much any company that has valuable intellectual property or trade secrets of any kind being pilfered continually, all day long, every day, relentlessly."**

Some of China's intellectual-property thefts are like virtual cat burglaries; others are inside jobs; and many combine elements of both. Dongfan "Greg" Chung, a former Boeing and Rockwell engineer, was convicted in 2009 of acting as an agent of the P.R.C. in stealing secrets related to the Space Shuttle program and the Delta IV rocket. In March of this year, a man named Sixing "Steve" Liu, a Chinese engineer who worked for a division of L-3 Communications, was arrested on charges of illegally exporting military data to China. (Liu has pleaded not guilty and the case is pending.) A former Google executive told me, "The party is very aggressive in enforcing loyalty among Chinese employees of American companies. This creates a dilemma of divided loyalties. Google's response was to take the risk and plow ahead. Google did not hire private investigators. There may have been a cost for that." Early news coverage of Operation Aurora, against Google, indicated that some Google China employees had been denied access to internal networks and others had been put on leave or reassigned in the wake of the attacks. According to a Google spokesperson, the company "ran some tests … internally to ensure that the network was safe and secure and we gave Googlers in China a holiday on the Tuesday we made the announcement."

The vulnerability of corporations to attack stems in part from ignorance, in part from denial. Google executives reportedly believed that the American government monitors this country's Internet infrastructure the same way it monitors foreign military threats to keep the geographic homeland secure. A former White House official told me, "After Google got hacked, they called the N.S.A. in and said, 'You were supposed to protect us from this!' The N.S.A. guys just about fell out of their chairs. They could not believe how naïve the Google guys had been." (In response to detailed questions regarding Operation Aurora and the company's response to it, Google declined to comment.)

Martin Libicki, a Rand Corporation analyst and the author of *Cyberdeterrence and Cyberwar,* says that the 2007 hack of Defense Secretary Robert Gates's computer finally made some in Washington take the cyber-espionage problem seriously. The Pentagon has admitted that in June of that year it had to shut down part of the computer system in Gates's office after the attack, which senior U.S. officials attributed to the People's Liberation Army. "It got personal at that point," Libicki says. Other Western nations started talking publicly about the problem at around the same time. In August of that same year, German chancellor Angela Merkel reportedly confronted Chinese premier Wen Jiabao after hackers from his country gained access to the computers in her office, as well as those in the German foreign, economic, and research ministries. In December, M.I.5 sent a letter to 300 British C.E.O.'s and security chiefs warning them that state-sponsored Chinese organizations may have been spying on their computer systems.

Public awareness of cyber-espionage was dramatically heightened in January 2010 when Google started talking about Operation Aurora. Operation Aurora gathered source code, the virtual equivalent of Coca-Cola's secret formula, from a broad array of U.S. corporations. Because source code is so valuable, and because the manner of its theft was so innovative, many experts were puzzled by the way that Google announced the attacks, emphasizing Aurora's secondary goal (reconnaissance of "human-rights activists" in China) rather than its primary one (stealing Google's virtual DNA).

Access to source code makes it relatively easy to discover new vulnerabilities in a Web application. For malware writers, these vulnerabilities are the keys to the kingdom, the open windows in the house that let them get inside to steal the furniture—or, depending on their goals, to move the furniture around, by altering the code and therefore potentially changing the functions of the company's product.

It was eventually revealed that intruders had made off with source code for a Google password-management program called Gaia. The company's losses are widely rumored to have been much greater, however. New information from security experts who were personally briefed by Google's security chief, Heather Adkins, while Operation Aurora unfolded, offers a far more comprehensive picture of the attack than Google publicly told.

Access to source code makes it relatively easy to discover new vulnerabilities in a Web application.

For malware writers, these vulnerabilities are the keys to the kingdom.

Three people who visited Google's Mountain View, California, headquarters while the attacks were in progress describe dramatic scenes of a company under siege. Google "built a physically separate area for the security team," one of them says. Sergey Brin, one of the company's cofounders, was deeply involved in the cyber-defense. “He moved his desk to go sit with the Aurora responders every day. Because he grew up in the Soviet Union, he personally has a real hard-on for the Chinese now. He is pissed.” Caught unawares and shorthanded, the company made a list of the world’s top security professionals, and Brin personally called to offer them jobs—with $100,000 signing bonuses for some, according to one person who received such an offer—and quickly built Google’s small, pre-Aurora security operation into a group of more than 200.

Meanwhile, representatives of other companies hit by Aurora were invited to the Googleplex for private meetings with Adkins. She told two of the visitors that the attackers had made a beeline for Google’s “legal-discovery portals,” the system the company uses to evaluate requests for information from law-enforcement agencies and foreign governments. “The activity on those portals is closely monitored,” one visitor says. “Someone noticed that a bunch of Chinese names were queried on one woman’s computer [in the legal-discovery department] and asked her, ‘Why did you query all these people?’ She said, ‘I didn’t.’ ”

Security took her laptop to analyze it, and “that was the string they started pulling” that unraveled the Aurora attack.

Much more significant, however—and previously unreported—is that the intruders used Google’s internal search engine to look for words related to the company’s signing certificates: virtual credentials that verify the identity of the source of any software before it can be downloaded to a computer. This part of the attack was foiled because Google keeps its signing certificates offline, in an “air-gapped” network—a network that is not connected to the Internet.

In both Operation Aurora and the RSA hack, not only did the attackers seek to steal proprietary information, they sought to steal the digital identities that would allow them to impersonate the companies.

The search for signing certificates is a disturbing new piece of information about Operation Aurora’s intentions. It also suggests a link to the SecurID theft. In both Operation Aurora and the RSA hack, not only did the attackers seek to steal proprietary information, they sought to steal the digital identities that would allow them to impersonate the companies.

Google’s initial announcement of Operation Aurora stated that “at least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media and chemical sectors”—had been affected, and early news reports named Yahoo and Symantec as among the other victims. As the year wore on, the body count grew: Adobe, Juniper Networks, and Rackspace admitted that they’d been attacked, then Intel. Before long a cache of e-mails written by analysts at the security firm HBGary and its sister company HBGary Federal were made public, after the companies were caught in the crosshairs of the hacktivist group Anonymous, a loose coalition of individuals who perform coordinated cyber-attacks, sometimes with the stated goal of advancing Internet freedom. The e-mails revealed that Aurora or similar attacks had also hit Baker Hughes, ExxonMobil, Royal Dutch Shell, BP, Conoco Phillips, Marathon Oil, Lockheed, Northrop Grumman, Symantec, Juniper, Disney, Sony, Johnson & Johnson, General Electric, General Dynamics, the law firm King & Spalding, and DuPont. DuPont was hit so intensely that, one HBGary analyst wrote, "their hair is on fire."

Not only did the HBGary e-mails provide new details about Aurora, they also described similar attacks that had been going on for much longer than the public knew. "Many of the leading defense contractors … all had … aurora-type attacks as far back as 2005," one analyst wrote. "So a search engine makes a big media stink about one intrusion, and that leads to a bunch of hype? I think the discussion needs to be on why it's taken 5+ years for the rest of the industry to catch on."

> **"Many of the leading defense contractors … all had … aurora-type attacks as far back as 2005."**

Pointing Fingers

From the start, Google openly asserted its view that the attack originated in China, and Hillary Clinton, after being "briefed by Google on these allegations," issued a statement that pointedly said, "We look to the Chinese government for an explanation." A report by Verisign iDefense, a security-intelligence service based in Dulles, Virginia, went further, stating that Aurora was directed by "agents of the Chinese state or proxies thereof." The Chinese government made no official, public response to Clinton's statement. But shortly thereafter, a spokesman for China's Ministry of Industry and Information Technology told Xinhua, the official news agency, about the allegations regarding Google, that the "accusation that the Chinese government participated in [any] cyber attack, either in an explicit or inexplicit way, is groundless and aims to denigrate China."

Yet, in the case of Aurora, there is evidence of involvement. After researchers found similarities between the tools used in the Aurora attacks and malware tools that were posted on open Chinese hacker forums, many analysts speculated that Beijing had employed civilian hackers as proxies to launch the attacks. A leading security-intelligence analyst says he received several dozen tips from sources in China suggesting that, "in point of fact, it was the P.R.C. government taking or demanding access to some of the research that the hackers had been doing, and then using it themselves."

The analyst goes on: "The Chinese government has employed this same tactic in numerous intrusions. Because their internal police and military have such a respected or feared voice among the hacking community, they can make use of the hackers' research with their knowledge and still keep the hackers tight-lipped about it. The hackers know that if they step out of line they will find themselves quickly in a very unpleasant prison in western China, turning large rocks into smaller rocks." In an undated cable made public by WikiLeaks, one American diplomat in Beijing reported to Washington that Aurora was an act of revenge ordered by a Chinese politburo member who had Googled himself and found a raft of unflattering articles.

The SecurID hack used the same basic technique as Operation Aurora and many other recent intrusions, though it made use of different specific tools. The technique, called "spear-phishing," begins with reconnaissance to find personal information about a company's employees. The Adversary may troll social-networking sites, including Facebook and Twitter, or may research e-mail archives exfiltrated in previous attacks to diagram its victims' social situations. Then the Adversary writes e-mails or sends instant messages individually tailored to the recipients and sends them, with malicious attachments, from identities that the victim is likely to trust. If the recipient clicks on the attachment, the malware, called a remote-access tool, or "rat," hooks itself into the user's Windows operating system inside the company's firewall. The rat is manually operated by the Adversary—an actual person, sitting at a computer, waiting to take over the victim's machine.

> *"The initial machine is just a beachhead. From that point, the (hacker) will move into document repositories, e-mail archive servers, proceed to take the data and ship it out of the company."*

"The initial machine is just a beachhead," explains McAfee's Dmitri Alperovitch. "From that point, the Adversary will move into document repositories, e-mail archive servers, proceed to take the data and ship it out of the company through another mechanism, typically by setting up a second, command-and-control server that they will exfiltrate data to. From the moment you've clicked on the malware, there is another individual on the other end adapting to your network eco-system, your security system, and trying various things until they succeed in getting what they want. It's like a Predator drone in Pakistan that's being controlled by a joystick in Nevada."

Some of the types of tools that the RSA hackers used—the rat , the command-and-control-server infrastructure, and the remote domains—had previously been employed in a persistent series of attacks on the Department of Defense and other U.S.-government systems. These attacks were originally code-named Titan Rain. After Titan Rain was made public, it was re-christened with the code name Byzantine Hades, and after that name, too, was made public, Byzantine Hades was re-dubbed with at least three more new classified code names, according to a former N.S.A. analyst. Some top intrusion specialists attribute this series of attacks to a group in China called the Red Hacker Alliance, which has suspected ties to the People's Liberation Army. (The particular malware and command-and-control servers used in the SecurID hack, however, were unique, and had not been used in previous attacks.)

Act of War?

On May 21, the computer systems of America's largest military contractor, Lockheed Martin, detected an intruder. A week later, Lockheed acknowledged the breach in a statement. The company called the attack "significant and tenacious" but also said that it had been detected "almost immediately," at which point the company took "aggressive" actions to stop it. "Our systems remain secure; no customer, program or employee personal data has been compromised," the statement said—leaving open the questions of how an intrusion could be both "tenacious" and detected "almost immediately," and how it could be "significant" without compromising any data. The event was noteworthy enough that President Obama was briefed on the situation. An unnamed Lockheed executive told *The New York Times* investigators "cannot rule out" a connection to the RSA breach. RSA said that it was "premature to speculate" on the cause of the attack.

On May 31, news broke that L-3 Communications, which provides intelligence, surveillance, and reconnaissance technology to the U.S. government, had also been attacked, according to an e-mail to L-3 employees dated April 6. The e-mail said that L-3 had been "actively targeted with penetration attacks leveraging the compromised information" from the RSA breach. When asked whether intruders had gained the ability to clone SecurID key fobs, an RSA spokeswoman said, "That's not something we had commented on and probably never will."

The next day, June 1, Fox News reported that Northrop Grumman had cut off remote access to its network without warning, resetting domain names and passwords, and causing "chaos" across the company, according to an unnamed Northrop executive. The company's official response to Fox's questions on the matter was, verbatim, the same as its response to my questions about previous reported hacks, going back several years: "We do not comment on whether or not Northrop Grumman is or has been a target for cyber intrusions."

That same day, Google made its first allegation of Chinese hacking since Operation Aurora, announcing that it had thwarted an attempt from China to steal the Gmail passwords of senior U.S. government officials. The next week, on June 7, RSA's Art Coviello gave a mea culpa interview to *The Wall Street Journal,* admitting that the entire SecurID system was compromised, offering to replace practically all of the millions of tokens on the market—and infuriating many of its customers, some of whom were reported to be sundering their relationship with RSA and hiring new security companies. Coviello says that he made the replacement offer because, "post-Lockheed, customers had a lower tolerance for risk," and he says that "less than 10 percent of our customers have requested replacement tokens."

This onslaught of revelations was all the more extraordinary because American industry has so few incentives to come clean about its losses, and so many incentives to cover them up.

This onslaught of revelations was all the more extraordinary because American industry has so few incentives to come clean about its losses, and so many incentives to cover them up. Was it a coincidence that, only hours before Northrop's and Google's alleged hacks became public, the Pentagon provided an element of its forthcoming cyber-war strategy to *The Wall Street Journal,* declaring that the U.S. will consider some cyber-attacks to be the equivalent of physical acts of war?

Like so many Rip Van Winkles, most of Washington has been asleep while cyber-attacks proliferated. But a few voices have been trying to wake the town up. One belongs to Scott Borg, director and chief economist of the U.S. Cyber-Consequences Unit, whose research indicates that China, to sustain economic growth, “is relying increasingly on large-scale information theft. This means that cyber attacks are now a basic part of China’s national development strategy.”

Another voice is that of James A. Lewis, a former diplomat who now leads the Technology and Public Policy Program at the Center for Strategic and International Studies. He says, “The thing we have to work through is, how do we want to work with the Chinese on this issue? This administration has decided they want to cooperate, not have a confrontation.” A senior State Department official elaborates: “One of the core things we’re trying to do diplomatically is to build a consensus internationally to build norms of behavior, rules of the road,” as described in the president’s “International Strategy for Cyberspace.” (The norms include “Upholding Fundamental Freedoms,” “Respect for Property,” and “Right of Self-Defense.”) James A. Lewis goes on: “This is what we did on missile proliferation. Our allies showed up and we all said, ‘Here are the norms.’ But how do we get a flow of countries to show up and say, ‘You’re crossing a line. Back off, or there will be consequences’? What is the cost to the Chinese right now? Until there is some cost, they’re not going to stop.”

Another White House document, the “Comprehensive National CyberSecurity Initiative,” as well as several bills in Congress, propose ways of protecting critical infrastructure, such as electrical grids, from cyber-intrusions. China has so thoroughly probed and mapped our power system that former director of national intelligence Dennis Blair once publicly admitted that “a number of nations, including Russia and China, can disrupt elements of the U.S. information infrastructure.”

Still others are trying to address the economic impact of cyber-espionage. On May 11, Senator Jay Rockefeller and several of his colleagues sent a letter to Mary Schapiro, chair of the U.S. Securities and Exchange Commission, asking the S.E.C. to issue interpretive guidance for companies about disclosing material risk due to cyber-breaches. The morning Rockefeller sent his letter, Tom Kellermann, a former cyber-security specialist at the World Bank, told me that the S.E.C. would force companies to make significant disclosures. “The dragon lady’s gonna rain down fire,” he said.

Security Budget Request

CFO: “What’s the worst that can happen if we don’t fix these (65 network vulnerabilities)?”

CIO: “We have large exposure.”

CFO: “No. No. What’s the financial impact?”

CIO: “We’re not regulated or audited, so there won’t be any fines.”

CFO: “You get no budget.”

The dragon lady has her work cut out for her. One industrial-control-systems security specialist recalls a conversation with a chief financial officer and a chief information officer of a major corporation after finding 65 vulnerabilities in the company’s networks, which would have required a huge investment to fix. “What’s the worst that can happen if we don’t fix any of these?” the C.F.O. asked.

“We have large exposure,” answered the C.I.O. “We could potentially be attacked—”

“No, no, no. What is the financial impact if we don’t do any of these?”

“We’re not regulated or audited, so there won’t be any fines.”

The C.F.O. answered, “You get no budget,” and the topic was closed.

The persistent culture of secrecy surrounding all things cyber compounds the difficulty of taking practical steps against Chinese hacking. Much, perhaps most, information about cyber-conflict of all types is classified, which creates tremendous practical problems of communication. Sometimes, when the F.B.I. learns of an intrusion through classified channels, the Bureau has to find other, unclassified evidence of the intrusion in order to be able to tell the victim what is happening. “If it’s a defense contractor being hacked, then the victim company includes people with clearances, so communication is easy. But if you’re talking about a company where no one has clearances, that presents a significant problem”—and can create a significant time delay between the discovery of a hack and the victim’s awareness of exposure, according to one cyber-security analyst.

Playing the Fool

Yet the deeper I delved into the Chinese hacking problem, the more I discovered a network of individuals in government and the private sector who are serving as a semi-official Resistance in this secret war. A handful of influential congressional staffers who shape Hill debate on these matters put me in touch with top intrusion specialists who are former hackers, military personnel, or National Security Agency officials. These analysts are the civilian, cyber-equivalent of special-ops forces. When my phone rang very late one night this spring, I was surprised to see the name of one of these analysts on the screen. In the mood to talk, he spent most of an hour describing his work to me, naming names and counting losses with shocking precision, though forbidding me to repeat the details of his disclosures.

In this conversation—the first of several that took place over the following months—the man said that he had started his career protecting government networks against foreign attacks. On that job, he became so preoccupied with the scale of Chinese hacking that a senior military officer told him to stop talking about it, with the gruff explanation that “the reason this is still going on is that the Chinese government now owns us.” Frustrated, the analyst eventually left government service for the private sector.

The problem may be reaching a boil that will take significant willpower to ignore. In mid-July, the security firm McAfee shared exclusively with *Vanity Fair* the results of its latest cyber-

“There are only two types of companies—those that know they’ve been compromised, and those that don’t know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised.”

espionage investigation. McAfee reports that, over a period of five years, a single Adversary penetrated more than 70 organizations, from giant multi-national corporations to tiny nonprofits, representing more than 30 industries around the world, and exfiltrated intellectual property—including e-mail archives, legal contracts, negotiation plans for business activities, design schematics, and government secrets—as soon as its spear-phishing victims clicked on a link to a Web page. One country’s Olympic committee was compromised for a full 28 months; many other organizations were compromised for two whole years. McAfee has given the name Operation Shady rat to this set of intrusions. Dmitri Alperovitch, who discovered Operation Shady rat, draws a stark lesson: “There are only two types of companies—those that know they’ve been compromised, and those that don’t know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised.”

The full list of Operation Shady rat’s victims includes government agencies and corporations worldwide. The vast majority of victims—more than two-thirds of the total—are in the U.S. Among the other countries targeted are Taiwan, South Korea, Japan, Hong Kong, Singapore, India, Germany, and the U.K. In 2007, the year before the Beijing Olympics, one international athletics organization and the Olympic committees of three different countries were breached by this intruder. Alperovitch believes the targeting of the Olympic committees and of American political nonprofits suggests the intrusions were state-sponsored, explaining, “There’s no economic gain to compromising them.” When asked if the People’s Republic of China was conceivably behind Shady rat —given that China was not itself attacked—Alperovitch noted that McAfee’s policy was not to comment on attribution. He added, “If others want to draw that conclusion, I certainly wouldn’t discourage them.”

Another security researcher who was on the front lines during Operation Aurora says, “Those of us who are hands-on-keyboard want this story to be told, because we feel like the top corporate managers—following the advice of their lawyers—are reflexively keeping breach information secret from other companies that are trying to defend themselves. In the big picture, a little bit of short-term embarrassment is worth it, to get the American people to understand that there’s a low-level Cold War going on.”

“…the top corporate managers—following the advice of their lawyers—are reflexively keeping breach information secret from other companies that are trying to defend themselves.

Despite—and also because of—the extreme secrecy surrounding industrial cyber-espionage, this phenomenon is gradually effecting a fundamental re-arrangement of the relationship between state and corporate power.

Michael Hayden was the director of the N.S.A. and then the C.I.A. during the period when the problem of Chinese cyber-espionage developed. In a conversation with him about Operation Aurora, I asked what he believed to be the most significant fact about those intrusions.

He answered, "You see Google acting in some ways as nation-states used to act, exercising to the best of their ability some attributes traditionally associated with sovereign states. 'We're going to break relationship'—cease doing business there, you know. It's something I dwell on a lot. The cyberworld is so new that the old structures, you know—state, non-state, public, private—they all break down …

The last time we had such a powerful discontinuity is probably the European discovery of the Western Hemisphere. At that point, we had some big, multi-national corporations—East India Company and Hudson's Bay—that acted as states. And I see elements of that with the big Microsofts and Googles of the world. Because of their size, they actually are making decisions that have the impact of the kinds of decisions made in the halls of government. Google is not a state. But what constitutes Google's inherent right of self-defense in this new environment against this kind of attack? I'm not accusing anyone of doing anything wrong. These situations are just so different. What do we believe would be legitimate for Google to do in response to this? Now, I don't have answers. I really don't know, but it's a really good question."

Operation Starlight has an old-fashioned answer to that question: Find the culprits and put them to shame. Its draft report declares: "The attacker's name, telephone number records, and other pertinent information should be divulged to the public in order to support attacker attribution and assist in tracking back to the source."

But no one believes that this tactic by itself will solve the problem—or that corporations will embrace their long-term best interest anytime soon. *Rather, so long as executives and politicians are guided by short-term self-interest, they will continue to play the fool to the country that would be king.*

"You need to consider: What are the subconscious assumptions that companies bring to the issue of foreign cyber-attacks on their networks?" a senior Senate staffer who works on cyber-issues asked me.

> **"The difference with cyber is there are people trying to fly planes into buildings every day now.**
>
> **And everybody just looks the other way."**

"They assume that if something bad happens government will take care of the losses. They act like they don't really believe that a bank could get completely taken out, or that a tech giant could get its whole lunch eaten, because it sounds as fictional as 9/11 would have sounded before it happened. But terrorism is not the best analogy here. Who could have imagined that people would have flown airplanes into buildings? The difference with cyber is there are people trying to fly planes into buildings every day now. And everybody just looks the other way."