BusinessWeek

COVER STORY April 10, 2008, 5:00PM EST

The New E-spionage Threat

A *BusinessWeek* probe of rising attacks on America's most sensitive computer networks uncovers startling security gaps

by Brian Grow, Keith Epstein and Chi-Chu Tschang

The e-mail message addressed to a Booz Allen Hamilton executive was mundane—a shopping list sent over by the Pentagon of weaponry India wanted to buy. But the missive turned out to be a brilliant fake. Lurking beneath the description of aircraft, engines, and radar equipment was an insidious piece of computer code known as "Poison Ivy" designed to suck sensitive data out of the $4 billion consulting firm's computer network.

The Pentagon hadn't sent the e-mail at all. Its origin is unknown, but the message traveled through Korea on its way to Booz Allen. Its authors knew enough about the "sender" and "recipient" to craft a message unlikely to arouse suspicion. Had the Booz Allen executive clicked on the attachment, his every keystroke would have been reported back to a mysterious master at the Internet address cybersyndrome.3322.org, which is registered through an obscure company headquartered on the banks of China's Yangtze River.

The U.S. government, and its sprawl of defense contractors, have been the victims of an unprecedented rash of similar cyber attacks over the last two years, say current and former U.S. government officials. "It's espionage on a massive scale," says Paul B. Kurtz, a former high-ranking national security official. Government agencies reported 12,986 cyber security incidents to the U.S. Homeland Security Dept. last fiscal year, triple the number from two years earlier. Incursions on the military's networks were up 55% last year, says Lieutenant General Charles E. Croom, head of the Pentagon's Joint Task Force for Global Network Operations. Private targets like Booz Allen are just as vulnerable and pose just as much potential security risk. "They have our information on their networks. They're building our weapon systems. You wouldn't want that in enemy hands," Croom says. Cyber attackers "are not denying, disrupting, or destroying operations—yet. But that doesn't mean they don't have the capability."

A MONSTER

When the deluge began in 2006, officials scurried to come up with software "patches," "wraps," and other bits of triage. The effort got serious last summer when top military brass discreetly summoned the chief executives or their representatives from the 20 largest U.S. defense contractors to the Pentagon for a "threat briefing." *BusinessWeek* has learned the U.S. government has launched a classified operation called Byzantine Foothold to detect, track, and disarm intrusions on the government's most critical networks. And President George W. Bush on Jan. 8 quietly signed an order known as the Cyber Initiative to overhaul U.S. cyber defenses, at an eventual cost in the tens of billions of dollars, and establishing 12 distinct goals, according to people briefed on its contents. One goal in particular illustrates the urgency and scope of the problem: By June all government agencies must cut the number of communication channels, or ports, through which their networks connect to the Internet from more than 4,000 to fewer than 100. On Apr. 8, Homeland Security Dept. Secretary Michael Chertoff called the President's order a cyber security "Manhattan Project."

But many security experts worry the Internet has become too unwieldy to be tamed. New exploits appear every day, each seemingly more sophisticated than the previous one. The Defense Dept., whose Advanced Research Projects Agency (DARPA) developed the Internet in the 1960s, is beginning to think it created a monster. "You don't need an Army, a Navy, an Air Force to beat the U.S.," says General William T. Lord, commander of the Air Force Cyber Command, a unit formed in November, 2006, to upgrade Air Force computer defenses. "You can be a peer force for the price of the PC on my desk." Military officials have long believed that "it's cheaper, and we kill stuff faster, when we use the Internet to enable high-tech warfare," says a top adviser to the U.S. military on the overhaul of its computer security strategy. "Now they're saying, Oh, shit.'"

Adding to Washington's anxiety, current and former U.S. government officials say many of the new attackers are trained professionals backed by foreign governments. "The new breed of threat that has evolved is nation-state-sponsored stuff," says Amit Yoran, a former director of Homeland Security's National Cyber Security Div. Adds one of the nation's most senior military officers: "We've got to figure out how to get at it before our regrets exceed our ability to react."

The military and intelligence communities have alleged that the People's Republic of China is the U.S.'s biggest cyber menace. "In the past year, numerous computer networks around the world, including those owned by the U.S. government, were subject to intrusions that appear to have originated within the PRC," reads the Pentagon's annual report to Congress on Chinese military power, released on Mar. 3. The preamble of Bush's Cyber Initiative focuses attention on China as well.

Wang Baodong, a spokesman for the Chinese government at its embassy in Washington, says "anti-China forces" are behind the allegations. Assertions by U.S. officials and others of cyber intrusions sponsored or encouraged by China are unwarranted, he wrote in an Apr. 9 e-mail response to questions from *BusinessWeek*. "The Chinese government always opposes and forbids any cyber crimes including hacking' that undermine the security of computer networks," says Wang. China itself, he adds, is a victim, "frequently intruded and attacked by hackers from certain countries."

Because the Web allows digital spies and thieves to mask their identities, conceal their physical locations, and bounce malicious code to and fro, it's frequently impossible to pinpoint specific attackers. Network security professionals call this digital masquerade ball "the attribution problem."

A CREDIBLE MESSAGE

In written responses to questions from *BusinessWeek*, officials in the office of National Intelligence Director J. Michael McConnell, a leading proponent of boosting government cyber security, would not comment "on specific code-word programs" such as Byzantine Foothold, nor on "specific intrusions or possible victims." But the department says that "computer intrusions have been successful against a wide range of government and corporate networks across the critical infrastructure and defense industrial base." The White House declined to address the contents of the Cyber Initiative, citing its classified nature.

The e-mail aimed at Booz Allen, obtained by *BusinessWeek* and traced back to an Internet address in China, paints a vivid picture of the alarming new capabilities of America's cyber enemies. On Sept. 5, 2007, at 08:22:21 Eastern time, an e-mail message appeared to be sent to John F. "Jack" Mulhern, vice-president for international military assistance programs at Booz Allen. In the high-tech world of weapons sales, Mulhern's specialty, the e-mail looked authentic enough. "Integrate U.S., Russian, and Indian weapons and avionics," the e-mail noted, describing the Indian government's expectations for its fighter jets. "Source code given to India for indigenous computer upgrade capability." Such lingo could easily be understood by Mulhern. The 62-year-old former U.S. Naval officer and 33-year veteran of Booz Allen's military consulting business is an expert in helping to sell U.S. weapons to foreign governments.

The e-mail was more convincing because of its apparent sender: Stephen J. Moree, a civilian who works for a group that reports to the office of Air Force Secretary Michael W. Wynne. Among its duties, Moree's unit evaluates the security of selling U.S. military aircraft to other countries. There would be little reason to suspect anything seriously amiss in Moree's passing along the highly technical document with "India MRCA Request for Proposal" in the subject line. The Indian government had just released the request a week earlier, on Aug. 28, and the language in the e-mail closely tracked the request. Making the message appear more credible still: It referred to upcoming Air Force communiqués and a "Teaming Meeting" to discuss the deal.

But the missive from Moree to Jack Mulhern was a fake. An analysis of the e-mail's path and attachment, conducted for *BusinessWeek* by three cyber security specialists, shows it was sent by an unknown attacker, bounced through an Internet address in South Korea, was relayed through a Yahoo! (YHOO) server in New York, and finally made its way toward Mulhern's Booz Allen in-box. The analysis also shows the code—known as "malware," for malicious software—tracks keystrokes on the computers of people who open it. A separate program disables security measures such as password protection on Microsoft (MSFT) Access database files, a program often used by large organizations such as the U.S. defense industry to manage big batches of data.

AN E-MAIL'S JOURNEY

While hardly the most sophisticated technique used by electronic thieves these days, "if you have any kind of sensitive documents on Access databases, this [code] is getting in there and getting them out," says a senior executive at a leading cyber security firm that analyzed the e-mail. (The person requested anonymity because his firm provides security consulting to U.S. military departments, defense contractors, and financial institutions.) Commercial computer security firms have dubbed the malicious code "Poison Ivy."

But the malware attached to the fake Air Force e-mail has a more devious—and worrisome—capability. Known as a remote administration tool, or RAT, it gives the attacker control over the "host" PC, capturing screen shots and perusing files. It lurks in the background of Microsoft Internet Explorer browsers while users surf the Web. Then it phones home to its "master" at an Internet address currently registered under the name cybersyndrome.3322.org.

The digital trail to cybersyndrome.3322.org, followed by analysts at *BusinessWeek*'s request, leads to one of China's largest free domain-name-registration and e-mail services. Called 3322.org, it is registered to a company called Bentium in the city of Changzhou, an industry hub outside Shanghai. A range of security experts say that 3322.org provides names for computers and servers that act as the command and control centers for more than 10,000 pieces of malicious code launched at government and corporate networks in recent years. Many of those PCs are in China; the rest could be anywhere.

The founder of 3322.org, a 37-year-old technology entrepreneur named Peng Yong, says his company merely allows users to register domain names. "As for what our users do, we cannot completely control it," says Peng. The bottom line: If Poison Ivy infected Jack Mulhern's computer at Booz Allen, any secrets inside could be seen in China. And if it spread to other computers, as malware often does, the infection opens windows on potentially sensitive information there, too.

It's not clear whether Mulhern received the e-mail, but the address was accurate. Informed by *BusinessWeek* on Mar. 20 of the fake message, Booz Allen spokesman George Farrar says the company launched a search to find it. As of Apr. 9, says Farrar, the company had not discovered the e-mail or Poison Ivy in Booz Allen's networks. Farrar says Booz Allen computer security executives examined the PCs of Mulhern and an assistant who received his e-mail. "We take this very seriously," says Farrar. (Mulhern, who retired in March, did not respond to e-mailed requests for comment and declined a request, through Booz Allen, for an interview.)

Air Force officials referred requests for comment to U.S. Defense Secretary Robert M. Gates' office. In an e-mailed response to *BusinessWeek*, Gates' office acknowledges being the target of cyber attacks from "a variety of state and non-state-sponsored organizations to gain unauthorized access to, or otherwise degrade, [Defense Dept.] information systems." But the Pentagon declined to discuss the attempted Booz Allen break-in. The Air Force, meanwhile, would not make Stephen Moree available for comment.

The bogus e-mail, however, seemed to cause a stir inside the Air Force, correspondence reviewed by *BusinessWeek* shows. On Sept. 4, defense analyst James Mulvenon also received the message with Moree and Mulhern's names on it. Security experts believe Mulvenon's e-mail address was secretly included in the "blind copy" line of a version of the message. Mulvenon is director of the Center for Intelligence Research & Analysis and a leading consultant to U.S. defense and intelligence agencies on China's military and cyber strategy. He maintains an Excel spreadsheet of suspect e-mails, malicious code, and hacker groups and passes them along to the authorities. Suspicious of the note when he received it, Mulvenon replied to Moree the next day. Was the e-mail "India spam?" Mulvenon asked.

"I apologize—this e-mail was sent in error—please delete," Moree responded a few hours later.

"No worries," typed Mulvenon. "I have been getting a lot of trojaned Access databases from China lately and just wanted to make sure."

"Interesting—our network folks are looking into some kind of malicious intent behind this e-mail snafu," wrote Moree. Neither the Air Force nor the Defense Dept. would confirm to *BusinessWeek* whether an investigation was conducted. A Pentagon spokesman says that its procedure is to refer attacks to law enforcement or counterintelligence agencies. He would not disclose which, if any, is investigating the Air Force e-mail.

DIGITAL INTRUDERS

By itself, the bid to steal digital secrets from Booz Allen might not be deeply troubling. But Poison Ivy is part of a new type of digital intruder rendering traditional defenses—firewalls and updated antivirus software—virtually useless. Sophisticated hackers, say Pentagon officials, are developing new ways to creep into computer networks sometimes before those vulnerabilities are known. "The offense has a big advantage over the defense right now," says Colonel Ward E. Heinke, director of the Air Force Network Operations Center at Barksdale Air Force Base. Only 11 of the top 34 antivirus software programs identified Poison Ivy when it was first tested on behalf of *BusinessWeek* in February. Malware-sniffing software from several top security firms found "no virus" in the India fighter-jet e-mail, the analysis showed.

Over the past two years thousands of highly customized e-mails akin to Stephen Moree's have landed in the laptops and PCs of U.S. government workers and defense contracting executives. According to sources familiar with the matter, the attacks targeted sensitive information on the networks of at least seven agencies—the Defense, State, Energy, Commerce, Health & Human Services, Agriculture, and Treasury departments—and also defense contractors Boeing (BA), Lockheed Martin, General Electric (GE), Raytheon (RTW), and General Dynamics (GD), say current and former government network security experts. Laura Keehner, a spokeswoman for the Homeland Security Dept., which coordinates protection of government computers, declined to comment on specific intrusions. In written responses to questions from *BusinessWeek*, Keehner says: "We are aware of and have defended against malicious cyber activity directed at the U.S. Government over the past few years. We take these threats seriously and continue to remain concerned that this activity is growing more sophisticated, more targeted, and more prevalent." Spokesmen for Lockheed Martin, Boeing, Raytheon, General Dynamics, and General Electric declined to comment. Several cited policies of not discussing security-related matters.

The rash of computer infections is the subject of Byzantine Foothold, the classified operation designed to root out the perpetrators and protect systems in the future, according to three people familiar with the matter. In some cases, the government's own cyber security experts are engaged in "hack-backs"—following the malicious code to peer into the hackers' own computer systems. *BusinessWeek* has learned that a classified document called an intelligence community assessment, or ICA, details the Byzantine intrusions and assigns each a unique Byzantine-related name. The ICA has circulated in recent months among selected officials at U.S. intelligence agencies, the Pentagon, and cyber security consultants acting as outside reviewers. Until December, details of the ICA's contents had not even been shared with congressional intelligence committees.

Now, Senate Intelligence Committee Chairman John D. Rockefeller (D-W. Va.) is said to be discreetly informing fellow senators of the Byzantine operation, in part to win their support for needed appropriations, many of which are part of classified "black" budgets kept off official government books. Rockefeller declined to comment. In January a Senate Intelligence Committee staffer urged his boss, Missouri Republican Christopher "Kit" Bond, the committee's vice-chairman, to supplement closed-door testimony and classified documents with a viewing of the movie *Die Hard 4* on a flight the senator made to New Zealand. In the film, cyber terrorists breach FBI networks, purloin financial data, and bring car traffic to a halt in Washington. Hollywood, says Bond, doesn't exaggerate as much as people might think. "I can't discuss classified matters," he cautions. "But the movie illustrates the potential impact of a cyber conflict. Except for a few things, let me just tell you: It's credible."

"Phishing," one technique used in many attacks, allows cyber spies to steal information by posing as a trustworthy entity in an online communication. The term was coined in the mid-1990s when hackers began "fishing" for information (and tweaked the spelling). The e-mail attacks on government agencies and defense contractors, called "spear-phish" because they target specific individuals, are the Web version of laser-guided missiles. Spear-phish creators gather information about people's jobs and social networks, often from publicly available information and data stolen from other infected computers, and then trick them into opening an e-mail.

DEVIOUS SCRIPT

Spear-phish tap into a cyber espionage tactic that security experts call "Net reconnaissance." In the attempted attack on Booz Allen, attackers had plenty of information about Moree: his full name, title (Northeast Asia Branch Chief), job responsibilities, and e-mail address. Net reconnaissance can be surprisingly simple, often starting with a Google (GOOG) search. (A lookup of the Air Force's Pentagon e-mail address on Apr. 9, for instance, retrieved 8,680 e-mail addresses for current or former Air Force personnel and departments.) The information is woven into a fake e-mail with a link to an infected Web site or containing an attached document. All attackers have to do is hit their send button. Once the e-mail is opened, intruders are automatically ushered inside the walled perimeter of computer networks—and malicious code such as Poison Ivy can take over.

By mid-2007 analysts at the National Security Agency began to discern a pattern: personalized e-mails with corrupted attachments such as PowerPoint presentations, Word documents, and Access database files had been turning up on computers connected to the networks of numerous agencies and defense contractors.

A previously undisclosed breach in the autumn of 2005 at the American Enterprise Institute—a conservative think tank whose former officials and corporate executive board members are closely connected to the Bush Administration—proved so nettlesome that the White House shut off aides' access to the Web site for more than six months, says a cyber security specialist familiar with the incident. The Defense Dept. shut the door for even longer. Computer security investigators, one of whom spoke with *BusinessWeek*, identified the culprit: a few lines of Java script buried in AEI's home page, www.aei.org, that activated as soon as someone visited the site. The script secretly redirected the user's computer to another server that attempted to load malware. The malware, in turn, sent information from the visitor's hard drive to a server in China. But the security specialist says cyber sleuths couldn't get rid of the intruder. After each deletion, the furtive code would reappear. AEI says otherwise—except for a brief accidental recurrence caused by its own network personnel in August, 2007, the devious Java script did not return and was not difficult to eradicate.

The government has yet to disclose the breaches related to Byzantine Foothold. *BusinessWeek* has learned that intruders managed to worm into the State Dept.'s highly sensitive Bureau of Intelligence & Research, a key channel between the work of intelligence agencies and the rest of the government. The breach posed a risk to CIA operatives in embassies around the globe, say several network security specialists familiar with the effort to cope with what became seen as an internal crisis. Teams worked around-the-clock in search of malware, they say, calling the White House regularly with updates.

The attack began in May, 2006, when an unwitting employee in the State Dept.'s East Asia Pacific region clicked on an attachment in a seemingly authentic e-mail. Malicious code was embedded in the Word document, a congressional speech, and opened a Trojan "back door" for the code's creators to peer inside the State Dept.'s innermost networks. Soon, cyber security engineers began spotting more intrusions in State Dept. computers across the globe. The malware took advantage of previously unknown vulnerabilities in the Microsoft operating system. Unable to develop a patch quickly enough, engineers watched helplessly as streams of State Dept. data slipped through the back door and into the Internet ether. Although they were unable to fix the vulnerability, specialists came up with a temporary scheme to block further infections. They also yanked connections to the Internet.

One member of the emergency team summoned to the scene recalls that each time cyber security professionals thought they had eliminated the source of a "beacon" reporting back to its master, another popped up. He compared the effort to the arcade game Whack-A-Mole. The State Dept. says it eradicated the infection, but only after sanitizing scores of infected computers and servers and changing passwords. Microsoft's own patch, meanwhile, was not deployed until August, 2006, three months after the infection. A Microsoft spokeswoman declined to comment on the episode, but said: "Microsoft has, for several years, taken a comprehensive approach to help protect people online."

There is little doubt among senior U.S. officials about where the trail of the recent wave of attacks leads. "The Byzantine series tracks back to China," says Air Force Colonel Heinke. More than a dozen current and former U.S. military, cyber security, and intelligence officials interviewed by *BusinessWeek* say China is the biggest emerging adversary—and not just clubs of rogue or enterprising hackers who happen to be Chinese. O. Sami Saydjari, a former National Security Agency executive and now president of computer security firm Cyber Defense Agency, says the Chinese People's Liberation Army, one of the world's largest military forces, with an annual budget of $57 billion, has "tens of thousands" of trainees launching attacks on U.S. computer networks. Those figures could not be independently confirmed by *BusinessWeek*. Other experts provide lower estimates and note that even one hacker can do a lot of damage. Says Saydjari: "We have to look at this as equivalent to the launch of a Chinese Sputnik." China vigorously disputes the spying allegation and says its military posture is purely defensive.

Hints of the perils perceived within America's corridors of power have been slipping out in recent months. In Feb. 27 testimony before the U.S. Senate Armed Services Committee, National Intelligence Director McConnell echoed the view that the threat comes from China. He told Congress he worries less about people capturing information than altering it. "If someone has the ability to enter information in systems, they can destroy data. And the destroyed data could be something like money supply, electric-power distribution, transportation sequencing, and that sort of thing." His conclusion: "The federal government is not well-protected and the private sector is not well-protected."

Worries about China-sponsored Internet attacks spread last year to Germany, France, and Britain. British domestic intelligence agency MI5 had seen enough evidence of intrusion and theft of corporate secrets by allegedly state-sponsored Chinese hackers by November, 2007, that the agency's director general, Jonathan Evans, sent an unusual letter of warning to 300 corporations, accounting firms, and law firms—and a list of network security specialists to help block computer intrusions. Some recipients of the MI5 letter hired Peter Yapp, a leading security consultant with London-based Control Risks. "People treat this like it's just another hacker story, and it is almost unbelievable," says Yapp. "There's a James Bond element to it. Too many people think, It's not going to happen to me.' But it has."

Identifying the thieves slipping their malware through the digital gates can be tricky. Some computer security specialists doubt China's government is involved in cyber attacks on U.S. defense targets. Peter Sommer, an information systems security specialist at the London School of Economics who helps companies secure networks, says: "I suspect if it's an official part of the Chinese government, you wouldn't be spotting it."

A range of attacks in the past two years on U.S. and foreign government entities, defense contractors, and corporate networks have been traced to Internet addresses registered through Chinese domain name services such as 3322.org, run by Peng Yong. In late March, *BusinessWeek* interviewed Peng in an apartment on the 14th floor of the gray-tiled residential building that houses the five-person office for 3322.org in Changzhou. Peng says he started 3322.org in 2001 with $14,000 of his own money so the growing ranks of China's Net surfers could register Web sites and distribute data. "We felt that this business would be very popular, especially as broadband, fiber-optic cables, [data transmission technology] ADSL, these ways of getting on the Internet took off," says Peng (translated by *BusinessWeek* from Mandarin), who drives a black Lexus IS300 bought last year.

His 3322.org has indeed become a hit. Peng says the service has registered more than 1 million domain names, charging $14 per year for "top-level" names ending in .com, .org, or .net. But cyber security experts and the Homeland Security Dept.'s U.S. Computer Emergency Readiness Team (CERT) say that 3322.org is a hit with another group: hackers. That's because 3322.org and five sister sites controlled by Peng are dynamic DNS providers. Like an Internet phone book, dynamic DNS assigns names for the digits that mark a computer's location on the Web. For example, 3322.org is the registrar for the name cybersyndrome.3322.org at Internet address 61.234.4.28, the China-based computer that was contacted by the malicious code in the attempted Booz Allen attack, according to analyses reviewed by *BusinessWeek*. "Hackers started using sites like 3322.org so that the malware phones home to the specific name. The reason? It is relatively difficult to have [Internet addresses] taken down in China," says Maarten van Horenbeeck, a Belgium-based intrusion analyst for the SANS Internet Storm Center, a cyber threat monitoring group.

TARGET: PRIVATE SECTOR

Peng's 3322.org and sister sites have become a source of concern to the U.S. government and private firms. Cyber security firm Team Cymru sent a confidential report, reviewed by *BusinessWeek*, to clients on Mar. 7 that illustrates how 3322.org has enabled many recent attacks. In early March, the report says, Team Cymru received "a spoofed e-mail message from a U.S. military entity, and the PowerPoint attachment had a malware widget embedded in it." The e-mail was a spear-phish. The computer that controlled the malicious code in the PowerPoint? Cybersyndrome.3322.org—the same China-registered computer in the attempted attack on Booz Allen. Although the cybersyndrome Internet address may not be located in China, the top five computers communicating directly with it were—and four were registered with a large state-owned Internet service provider, according to the report.

A person familiar with Team Cymru's research says the company has 10,710 distinct malware samples that communicate to masters registered through 3322.org. Other groups reporting attacks from computers hosted by 3322.org include activist group Students for a Free Tibet, the European Parliament, and U.S. Bancorp (USB), according to security reports. Team Cymru declined to comment. The U.S. government has pinpointed Peng's services as a problem, too. In a Nov. 28, 2007, confidential report from Homeland Security's U.S. CERT obtained by *BusinessWeek*,

"Cyber Incidents Suspected of Impacting Private Sector Networks," the federal cyber watchdog warned U.S. corporate information technology staff to update security software to block Internet traffic from a dozen Web addresses after spear-phishing attacks. "The level of sophistication and scope of these cyber security incidents indicates they are coordinated and targeted at private-sector systems," says the report. Among the sites named: Peng's 3322.org, as well as his 8800.org, 9966.org, and 8866.org. Homeland Security and U.S. CERT declined to discuss the report.

Peng says he has no idea hackers are using his service to send and control malicious code. "Are there a lot?" he says when asked why so many hackers use 3322.org. He says his business is not responsible for cyber attacks on U.S. computers. "It's like we have paved a road and what sort of car [users] drive on it is their own business," says Peng, who adds that he spends most of his time these days developing Internet telephony for his new software firm, Bitcomm Software Tech Co. Peng says he was not aware that several of his Web sites and Internet addresses registered through them were named in the U.S. CERT report. On Apr. 7, he said he planned to shut the sites down and contact the U.S. agency. Asked by *BusinessWeek* to check his database for the person who registered the computer at the domain name cybersyndrome.3322.org, Peng says it is registered to Gansu Railway Communications, a regional telecom subsidiary of China's Railways Ministry. Peng declined to provide the name of the registrant, citing a confidentiality agreement. "You can go through the police to find out the user information," says Peng.

U.S. cyber security experts say it's doubtful that the Chinese government would allow the high volume of attacks on U.S. entities from China-based computers if it didn't want them to happen. "China has one of the best-controlled Internets in the world. Anything that happens on their Internet requires permission," says Cyber Defense Group's Saydjari. The Chinese government spokesman declined to answer specific questions from *BusinessWeek* about 3322.org.

But Peng says he can do little if hackers exploit his goodwill—and there hasn't been much incentive from the Chinese government for him to get tough. "Normally, we take care of these problems by shutting them down," says Peng. "Because our laws do not have an extremely clear method to handle this problem, sometimes we are helpless to stop their services." And so, it seems thus far, is the U.S. government.

Grow is a correspondent in BusinessWeek's Atlanta bureau . Epstein is a correspondent in BusinessWeek's Washington bureau. Tschang is a correspondent in BusinessWeek's Beijing bureau.

The new bill would update the Official Secrets Act and the laws on treason. He has also appointed Jonathan Hall QC as a watchdog to monitor the new terror laws. A register would act as a deterrent to spying and make it easier to take action against those involved, Mr Javid said. The home secretary said the tempo of terrorist activity was increasing, with 19 plots foiled in the UK in two years. Threat Intelâ€™s â€˜History ofâ€¦â€™ series will look at the origins and evolution of notable developments in cybersecurity. Throughout history, nation states have been trying to undermine each other through clandestine activity, whether its spying, sabotage, or subversion. The rapid growth of the internet during the 1990s opened up a new frontier in the arena of international espionage, and it wasnâ€™t long before we began to read ominous warnings about cyber warfare. Could a countryâ€™s enemies shut down its power grid, take out its telephone system, or even hijack its nuclear missiles? Given the covert The New E-spionage Threat. A BusinessWeek probe of rising attacks on America's most sensitive computer networks uncovers startling security gaps. Chris Usher.Â The e-mail message addressed to a Booz Allen Hamilton executive was mundaneâ€”a shopping list sent over by the Pentagon of weaponry India wanted to buy. But the missive turned out to be a brilliant fake. Lurking beneath the description of aircraft, engines, and radar equipment was an insidious piece of computer code known as "Poison Ivy" designed to suck sensitive data out of the $4 billion consulting firm's computer network. The Pentagon hadn't sent the e-mail at all. Its origin is unknown, but the message traveled through Korea on its way to Booz Allen.