Cyber spying a threat, and everyone is in on it

April 10 2009, By PAUL HAVEN , Associated Press Writer

(AP) -- Ghost hackers infiltrating the computers of Tibetan exiles and the U.S. electric grid have pulled the curtain back on 21st-century espionage as nefarious as anything from the Cold War - and far more difficult to stop.

Nowadays, a hacker with a high-speed Internet connection, knowledge of computer security and some luck can pilfer information thought to be safely ensconced in a digital locker. And the threat is growing, with countries - including the U.S. - pointing fingers at each other even as they ramp up their own cyber espionage.

The Pentagon this week said it spent more than $100 million in the last six months responding to damage from cyber attacks and other computer network problems. And the White House is wrapping up a 60-day review of how the government can better use technology to protect everything from the nation's electrical grid and stock markets to tax data, airline flight systems and nuclear launch codes.

In 2008, there were 5,499 known breaches of U.S. government computers with malicious software, according to the Department of Homeland Security. That's up from 3,928 the previous year, and just 2,172 in 2006.

Serious breaches by what are described as "unknown foreign entities" have occurred in recent years in computers at the Departments of Defense, Homeland Security and Commerce, as well as NASA,

according to a report by the Center for Strategic and International Studies, a nonpartisan organization in Washington.

The electrical grid might already have been compromised by spies who left behind computer programs that would let them disrupt service, a former U.S. government official told The Associated Press. The official said the sophistication of the attack meant it was almost certainly state-sponsored, but the government does not know its extent because federal officials lack the authority to monitor the entire grid.

"The vulnerability may be bigger than we think," said the official, who asked not to be identified because he was not authorized to discuss details.

It's not just the United States. In 2007, Russian hackers crippled computer networks in Estonia for nearly three weeks. In response, NATO set up an Estonia-based cyber defense center, and announced in April that cyber defense is being incorporated into NATO exercises.

"NATO takes this threat very seriously," Carmen Romero, a NATO representative in Brussels, told the AP. "NATO has to be ready for the new security challenges, and cyber attacks are one of them."

In Germany, experts have been monitoring Chinese cyber espionage since the 1990s. A counterespionage official with Germany's domestic intelligence agency said the country has verified "many hundreds of attacks per year," and that others had likely gone undetected.

"We expect that the attacks we've seen are only the tip of the iceberg," said the official, who spoke on condition of anonymity because of the sensitive nature of the subject. "We follow the attacks to their source, and many come from China."

Governments are not the only targets.

David Livingstone, author of a report on cyber threats by the London-based Chatham House think tank, said cyber espionage is a problem in all sectors - businesses, government and individuals.

"Anywhere there is attractive intellectual property and anything that is valuable and useful to someone else will be a target," he said.

In fact, the ubiquity of computers and the need to spread information electronically leaves us all vulnerable. Joel Brenner, head of the U.S. Office of the National Counterintelligence Executive, has warned that skilled cyber attackers can remotely turn on the camera on your home computer, convert your cell phone into a listening device, and even convert the earphones of your iPod into microphones.

Gone are the days when spies like American Whittaker Chambers hid microfilm in a hollowed-out pumpkin or Christopher Boyce spirited classified documents away inside a potted plant. Even Aldrich Ames, perhaps the CIA's most notorious double agent, used both hard documents and disks to betray U.S. secrets to Russia.

"Now, you can walk into many corporate and government offices, slip a thumb drive into an open USB port and download in seconds more information than all these traitors stole together," Brenner said in a recent speech on cyber espionage.

You don't even need a thumb drive. By infiltrating the Dalai Lama group's e-mail system with malware, cyber invaders saw nearly everything his monks did, from discussions of protest plans to documents that could have put activists at risk. And the Chinese hackers went even further, infiltrating 1,295 computers in 103 countries.

The information was used to warn foreign officials against meeting with the Dalai Lama, and to stop at least one Tibetan activist at the airport, according to researchers from the Ottawa-based think tank SecDev Group and the University of Toronto's Munk Centre for International Studies.

"People in Tibet may have died as a result," concluded a bleak assessment by computer engineers at Cambridge University in Britain also involved in the case. The Cambridge security experts recommended the exiles keep any sensitive information on computers that are never used to connect to a network, or better yet, use pen and paper.

"We have seen all sorts of attempts to computerize things that should never have been computerized," Ross Anderson, lead author of the Cambridge report, told the AP. "It takes a professor of computer science to have the confidence to say that some things simply should never be put on a computer."

While China's name pops up most in headlines about cyber espionage, experts say Russian hackers are at least as dangerous.

Last summer, in the weeks leading up to the war between Russia and Georgia, Georgian government and corporate Web sites began to see "denial of service" attacks, in which sites are deluged with traffic so as to effectively take them off-line. The Kremlin denied involvement, but a group of independent Western computer experts traced domain names and Web site registration data to conclude that the Russian top security and military intelligence agencies were involved.

"It is, quite simply, implausible that the parallel attacks by land and by cyberspace were a coincidence - official denials by Moscow notwithstanding," Eka Tkeshelashvili, the head of the Georgia's National Security Council, said in a speech in Washington last month.

China has denied any involvement in the Tibetan attacks and in cyber espionage. Chinese officials note that cyber invaders can use technology to bounce their identities off IP addresses around the world, making it difficult to pinpoint their whereabouts. And they claim the United States maintains a wide technological superiority in cyberspace.

Chen Wenguang, a Chinese computer expert, said any American accusations of Chinese cyber spying are "just another case of a robber crying 'Stop, thief!'"

"I believe that it is the Americans that steal the most secrets," said Chen, assistant director of the computer science department at Beijing's Tsinghua University. Chinese Foreign Ministry spokeswoman Jiang Yu said Tuesday the recent headlines were an attempt to sully the country's image.

U.S. officials acknowledge that even as they step up the nation's digital defense, they are quietly moving forward with an offense. Military officials in Washington said they had established rules for any offensive cyber strike, but would not say if the Pentagon already has pursued cyber warfare operations.

"A good defense also depends on a good offense," said Air Force Gen. Kevin Chilton, who heads U.S. Strategic Command.