'Cybergeddon' fear stalks US: FBI

NEW YORK, Jan 6 (AFP) Jan 07, 2009
Cyber attacks pose the greatest threat to the United States after nuclear war and weapons of mass destruction -- and they are increasingly hard to prevent, FBI experts said Tuesday.

Shawn Henry, assistant director of the FBI's cyber division, told a conference in New York that computer attacks pose the biggest risk "from a national security perspective, other than a weapon of mass destruction or a bomb in one of our major cities."

"Other than a nuclear device or some other type of destructive weapon, the threat to our infrastructure, the threat to our intelligence, the threat to our computer network is the most critical threat we face," he added.

US experts warn of "cybergeddon," in which an advanced economy -- where almost everything of importance is linked to or controlled by computers -- falls prey to hackers, with catastrophic results.

Michael Balboni, deputy secretary for public safety in New York state, described "a huge threat out there" against everything from banking institutions to municipal water systems and dams.

Henry said terrorist groups aim for an online 9/11, "inflicting the same kind of damage on our country, on all our countries, on all our networks, as they did in 2001 by flying planes into buildings."

A web attack of that scale has not yet happened in the United States but computer hacking -- once something of a sport for brilliant delinquents -- is rapidly evolving around the world as a weapon of war.

Russian hackers allegedly mounted huge assaults on Internet networks in Estonia and Georgia last year, while Palestinian sympathizers have orchestrated attacks against hundreds of Israeli websites in the last few days.

Evan Kohlmann, an investigator with Global Terror Alert, based in Washington, said websites and social networking tools already allow underground Islamist leaders and militant organizations to recruit and communicate in safety worldwide.

Jihadist websites can be destroyed, but "you knock one out and another pops up the next day."

More efforts are being made to infiltrate the sites and disrupt the clandestine networks, Kohlmann said.

In response, young militants are learning how to code software, or they are getting help from freelance experts, including those in Russia, who may well have nothing to do with Islamist causes.

"Right now, we're at the cusp of this," Kohlmann said.

Financial cyber criminals, who use the Internet to steal identities, siphon billions of dollars, and sometimes paralyze businesses, are also becoming more sophisticated.

"It used to be we'd chase people around, literally carrying duffel bags of cash," said Donald Codling, the FBI's cyber unit liaison with the Department of Homeland Security.

"Nowadays the guy can use his SIM chip and he can move money all over the world and his confederates can withdraw that money from an ATM in a currency of his or her choice. It's extraordinarily difficult for us to catch them."

Codling, like other cyber crime fighters, expressed grudging admiration for the skills of his foes, who he said are highly motivated and often a step ahead.

"We're seeing that the folks on the cutting edge of this tend to be the bad guys. There's a financial reason for them to be good at this," he said.

Christopher Painter, an FBI specialist focused on building international cooperation, described another basic weakness in the fight for cyber security: the threat is largely invisible and therefore not always taken seriously.

"It's not like a fire," he said. "It's hard to get your head around the threat. We often discover a company has been attacked and we tell them that and they don't know."

http://www.spacewar.com/2006/090107003235.7h48u951.html