Cyberterrorism: By Whatever Name, It's On The Increase

By Larry Greenemeier, InformationWeek
July 7, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=200900812

Experts say U.S. companies need to take the increasing use of cyberwarfare tactics and tools very seriously.

Security Pros are hesitant to label Web attacks as "cyberterrorism" because of the volatile connotations of that phrase. But recent events in England and Russia point to an increased use of the Web to coordinate or launch such attacks aimed at cultural and political subversion.

A British court last week handed down prison sentences of up to 10 years to three Muslim men it called "cyber-jihadis" and convicted of using the Internet to urge Muslims to wage holy war on non-Muslims. And the U.S. Computer Emergency Readiness Team reported politically motivated cyberattacks in Russia. The Web site for Russia's United Civil Front, which is run by former chess champ turned political activist Garry Kasparov, experienced problems staying online, and malicious hackers tried to break into the main site of the Center for Journalism in Extreme Situations, says director Oleg Panfilo. He added that the sites of several organizations "engaged in the protection of human rights" also were exposed to hacker attacks.

This type of cyberwarfare has been going on for months. The Web sites of Kommersant, a Russian newspaper, and the Echo of Moscow, a radio station, suffered significant denial-of-service attacks in early May for what the editor in chief of Kommersant's Web site speculated might be retaliation for the publication of a police interview with the expatriate billionaire Boris Berezovsky. Estonia's cyberinfrastructure was the target of extended DOS attacks in late April and early May.

These "cyber-jihadis" were convicted of inciting terrorists.

Electronic Jihad

Even the generally neutral Swiss government has found itself in the middle of the emerging struggle against cyberterrorism. Late last month, Swiss prosecutors charged a husband-and-wife team with running Web sites that supported terrorists by providing them with information on how to make bombs.

Similarly, the "Electronic Jihad Program," available via the jihadi Web site Al-jinan.org, is an application that users can install and use to target specific IP addresses for DOS attacks. The application includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and then click on the "attack" button.

The site was down late last week, but Al-jinan has been registered for about 4-1/2 years. Its domain name server registration features a number of contradictions that make tracing its origins difficult. Al-jinan's domain name server is being hosted by Ibtekarat, a Web hosting company

based in Beirut. The site's registration information cites an address with a Los Angeles postal code, while listing the Egyptian city of Al Esmaeiliya as its "registrant city" and Iraq as its "registrant country."

Electronic jihad hasn't yet caused any major Web site disruptions, but the potential is there. "Jihadists are interested in taking down Web sites and disrupting economies that they don't like," says Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School. "It's something to be taken seriously."

U.S. businesses would be greatly affected by large-scale cyberattacks because most of the country's critical infrastructure is run by companies in the private sector. The government and the U.S. business community "are one-in-the-same target," says Andrew Colarik, an information security consultant. Even businesses that don't run critical infrastructure elements would be affected because "there's a cascading effect if you attack the infrastructure," Colarik says.

While companies that operate critical infrastructure must be especially wary of Internet-based attacks, "everyone has to pay attention to security," Denning says. "There may be some businesses that say, 'No one will target us.' But electronic jihad will target anyone if it creates economic disruption. Whoever's vulnerable gets attacked."