Cyber Terror: Defusing the Timebomb

By Erick Stakelbeck
CBN News
January 10, 2007

CBNNews.com - WASHINGTON - What if terrorists could steal your credit card information online?

Or hack into a U.S. government website to remove their names from a no-fly list?

Even steal U.S. military and national security secrets?

These may sound like scenarios straight out of the hit show *24*, but for a growing number of rogue regimes, third-world economies and terrorist groups, the prospect of attacking America electronically is all too real.

Andrew Colarik is a cyber security expert and author of *Cyber Terrorism: Political and Economic Implications*.

Colarik said, "Countries such as Peru, Iran, United Arab Emirates, Saudi Arabia, Croatia, Vietnam -- there's a large litany of them -- have been actively attacking our power and utility infrastructure, they've been attacking our financial systems -- going after our technology-based companies."

He says a "digital tsunami" is headed for the United States.

"There are some very sophisticated people who work for governments, criminal organizations, syndicates, terrorist organizations, that have exceptional skills that aren't just creating Web sites and uploading video," Colarik warned.

He says they're using this computer savvy to wage information warfare against the United States, especially in lesser developed countries. Those nations know they can't compete with America economically or militarily. So they encourage their populations to weaken the U.S. through cyber attacks.

"Think about it," Colarik said. "We can't operate a business now without using computers and networks. If you want to sabotage, or if you want to gain intelligence, or if you want to see what we are planning, then the best way is to hone skills in this area."

And it's not just the Third World that's discovered the benefits of attacking America's computer systems.

Colarik explained, "Russia is interested in financial gain. So they go after our banking systems, all the support systems that go with that, including brokerage firms…China is really trying to get its economic infrastructure set up to be a world-class world power. And so they're using electronic espionage to take our trade secrets, our technologies, explore our military capabilities."

Islamic radicals have also become adept at cyber terrorism -- or what they call "electronic jihad." One website, Al-Jinan, gives instructions on how to hack into Web sites that supposedly "insult Islam." Experts say the cyber attack is now part of jihadi basic training.

Dr. Walid Phares is a terrorism expert and author of *Future Jihad: Terrorist Strategies against the West*.

He said, "They have concentrated over the past few years on creating a cyber-jihad war room. Many of their affiliates, not just in the Middle East -- including in the West, possibly in the United States -- have been focusing on trying to bring down Web sites, trying to break into security Web sites, and also possibly trying to wreak havoc in the financial part of this international Internet consortium."

He told CBN News of a recent U.S. government warning that al-Qaeda is seeking to attack online stock trading and banking websites.

Al-Qaeda also publishes a monthly magazine devoted to cyber-terrorism techniques.

Phares said, "Al-Qaeda has a web of activists. And those activists want to have access. And access translates into identity, into financial channels, and when this information goes all the way up the ladder to the leadership of al-Qaeda, they will decide how to use this information. It's not only about bringing down economic sites -- it's also having access to information."

So how can the U.S. prevent a massive al-Qaeda cyber attack?

"Number one, is better protection of the most sensitive cyber sites: nervous centers, nuclear, bio sites, and other very important protections and defenses for the West and for the United States," said Phares.

Colarik proposes "a league of cyber communities." The world's 20 largest economies would sign a treaty vowing to manage their own country's cyber activities. Member states would then deny traffic to any nation that refuses to crack down on cyber terrorists.

The U.S. government says it's already taken measures to prevent such attacks. A spokesman from the Cyber-Security Division of the Department of Homeland Security told CBN News:

"We have fostered partnerships with our Federal, state and local governments, the private sector, academia and international entities to respond to, mitigate and deter cyber attacks. We have also raised public awareness of the importance of cyber security. the Department of Homeland Security also maintains a 24/7 secure operations center that identifies and analyzes cyber threats and vulnerabilities."

DHS officials say that American citizens and businesses can do their part as well, by installing and updating anti-virus software and deleting e-mails from unknown sources.

They warn that cyber-terrorist tactics are becoming more sophisticated and frequent -- and with much of America running on computers, everyone has a stake in securing cyberspace.