

## Cyber-warfare 'the next battlefront,' experts say

### New wave of hackers ready to unleash attacks

**Vito Pilioci**

The Ottawa Citizen

*Thursday, November 06, 2008*

North America needs to work fast if it is to protect itself from a new wave of cyber-warfare.

According to several Internet security experts meeting at the Casino du Lac-Leamy in Gatineau yesterday, terrorists are learning to hack and many countries are gathering people proficient in computer science to unleash lethal attacks on the communications systems of other countries.

"This really represents the next battlefront," said Cornelius Tate, director of the U.S. Department of Homeland Security's National Cyber Security and Communications Division.

"Computers have become a real big part of everyday life. If there is a lesson from 9/11, it's that we have to think pro-actively instead of reactively."

Representatives from the FBI, the RCMP and the North Atlantic Treaty Organization also addressed the Conference Board of Canada's summit on cyber security.

These experts discussed the need for immediate action by businesses and government to address new electronic threats emerging in potentially hostile areas of the world. They focused on recent cyber warfare examples from Estonia and Georgia.

Estonia once was the most wired nation in the European Union, but in May 2007, hackers who overloaded servers shut down communication and forced banks, government institutions and private businesses offline.

At one point, the country was being attacked by more than one million computers from 100 countries. In many cases, the owners of the computers didn't even know they were taking part in the attacks, as hackers remotely controlled the machines.

Georgia's Internet networks were targeted in a similar fashion during its war with Russia in August. The websites were replaced with a slideshow comparing Georgia's president to Adolf Hitler.

The country's Internet networks were crippled, slowing communications to a crawl or preventing them entirely.

Both of the countries were attacked by what are known as "botnets," a remote control network of computers infected with a special virus. The virus allows hackers to activate the network off-site and attack any target they choose.

Scott O'Neal, the chief of the computer intrusion section of the FBI's cyber

division, said one reason cyber warfare is on the rise is that it's a "very low-risk, high-reward business right now."

Many governments do not have laws specifically outlining penalties for hacking or cyber warfare and the FBI doesn't have the manpower to crack down on the hackers.

Botnets, such as the ones used in Estonia and Georgia, can be rented from hackers for \$200 U.S. for a two-hour period, according to Edward Amoroso, senior vice-president and chief security office for AT&T Inc.

Those rogue computer networks can be used to target any business or government a paying customer may choose. Mr. Amoroso said there are more than 2.5 million botnet-infected computers globally.

If used to target a bank or stock exchange, "that can cause a very bad day in the global economy," Mr. Amoroso said.

Speakers at the conference said governments need to collaborate and share information to help catch hired hackers or terrorists before they can instigate a major information breach.

Kurtis Simpson, acting director of policy and programs, chief of defence intelligence for the Department of National Defence, said that to address this issue, governments everywhere must begin updating policies defining what an act of war is and how they should respond.

"Government policy in this area is underdeveloped. If you are attacked ... it is easy for a government to determine it was a missile strike and this is how we respond. A comprehensive strategy for cyber threats does not exist."

Mr. Simpson said NATO is pushing governments to come up with an agreed upon existing framework outlining procedures that should be followed in the event a cyber attack is detected.

The summit on cyber security continues today.

© The Ottawa Citizen 2008

CLOSE WINDOW

---

Copyright © 2008 CanWest Interactive, a division of CanWest MediaWorks Publications, Inc.. All rights reserved.

CanWest Interactive, a division of CanWest MediaWorks Publications, Inc.. All rights reserved.