

# Time to wake up to cyber threat: experts

June 18 2010

---



Acting senior director for Cyberspace for the National Security and Homeland Security Councils of the US Melissa Hathaway, speaks during the four-day international conference tackling the issue of cyber conflicts in Tallinn on June 17. "Cybercrime and cyberespionage are topics that can't be ignored," Hathaway said.

NATO governments and the public must wake up to the threat of cyberattacks, which could paralyse a nation far more easily than conventional warfare, experts warned Friday.

"[Cybercrime](#) and cyberespionage are topics that can't be ignored," said Melissa Hathaway, a former US cyber tsar, at a conference in Estonia organised by the trans-Atlantic alliance's IT defence unit.

"Key infrastructure, including power stations, have become vulnerable due to their dependence on Internet connections," Hathaway said.

"There is no national [security](#) in the modern world without economic security, and both companies and private citizens should also realise the depth of the problem," she added.

Charlie Miller -- a security expert who launches test assaults on IT systems -- underlined that cyberwar is far easier than a conventional attack.

"It would take two years and cost less than 50 million dollars a year to prepare a cyberattack that could paralyse the United States," Miller warned.

Such an attack could involve fewer than 600 hackers, he added.

Estonia is home to a unit known in NATO jargon as the Cooperative Cyber Defence Centre of Excellence.

Bitter experience taught Estonia -- one of the world's most wired nations and a NATO member since 2004 -- all about cyberattacks.

The Baltic state of 1.3 million people suffered an assault in 2007 that paralysed key business and [government web](#) services for days.

It came as Estonian authorities shifted a Soviet-era war memorial from central Tallinn to a cemetery site.

The monument, erected when Moscow took over after World War II, became a flashpoint following independence in 1991 for rallies by Estonia's ethnic-Russian minority.

Estonia blamed Moscow for stoking riots in Tallinn as the memorial was moved, and said the cyberattacks were traced to Russian official servers.

Russia, however, denied involvement.

Despite Estonia's experience, people elsewhere have not woken up, said British defence ministry expert Gloria Craig.

"It's still hard to convince the public that a cyberattack is an attack, when people don't see a smoking gun," Craig said.

"As of now NATO is not prepared for a global [cyberattack](#)," she added.

US specialist Bruce Schneier, however, said the current threat should not be overplayed.

"Building tanks does not mean you fear you could be overrun by a military force right now. It pays to build tanks and it pays to prepare for cyberwar, but I don't believe that's a fear we should worry about right now," Schneier said.

"It's very easy to invent scare scenarios but this does not mean we should actually be scared by them," he said.

Schneier said, however, that it time to prepare now so that sci-fi style scenarios never become reality.

(c) 2010 AFP

Citation: Time to wake up to cyber threat: experts (2010, June 18) retrieved 19 April 2024 from <https://phys.org/news/2010-06-cyber-threat-experts.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--