NATO's cyber-brains gaze at the future of war

April 24 2010, by Jonathan Fowler

In Tallinn, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) has a high-security lab where the North Atlantic Treaty Organisation's top cyber-minds are trying to predict the evolution of conflict in an Internet-dependent world.

Behind the walls of a high-security lab, the North Atlantic Treaty Organisation's top cyber-minds are trying to predict the evolution of conflict in an Internet-dependent world.

While they play down disaster-movie scenarios of total meltdown, experts warn cyber-attacks will be part and parcel of future fighting.

Tallinn is home to a cutting-edge unit known in NATO-speak as the Cooperative Cyber Defence Centre of Excellence. The city is the capital

of Estonia, whose flourishing hi-tech industry has earned it the label "E-Stonia".

"Definitely from the cyber-space perspective, I think we've gone further than we imagined in science fiction," said Ilmar Tamm, the Estonian colonel at its helm.

Its base is a 1905 building where military communications experts have toiled away since the days of carrier pigeons and the telegraph.

The centre's dozens of experts second-guess potential adversaries, gazing into what they dub the "fifth battlespace", after land, sea, air and space.

"The whole myriad and complex area makes it a very difficult problem to solve, and at the same time it keeps a very convenient grey area for the bad guys," explained Tamm.

"Many states have realised that this is really something that can be used as a weapon... That we should not ignore. It will have a future impact," he said.

"I'm not so naive that I'd say conventional warfare will go away. But we should expect it to be more combined," he added.

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

The minnow country of 1.3 million people suffered blistering attacks in 2007 which took down business and government web-based services for days.

"It clearly heralded the beginning of a new era," its Defence Minister Jaak Aaviksoo told AFP.

"It had all the characteristics of cyber-crime growing into a national security threat. It was a qualitative change, and that clicked in very many heads," he added.

The assault came as Estonian authorities controversially shifted a Soviet-era war memorial from central Tallinn to a military cemetery.

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

Tallinn was rocked by riots as the memorial was moved. Estonia blamed Russia for stoking the strife, and also claimed the cyber-offensive had been traced to official servers in Moscow.

Russia, whose relations with Estonia are rocky, denied involvement.

For Aaviksoo, cyber-attacks may "present a stand-alone security threat or a combined security threat".

An example of the latter, he noted, came during Russia's 2008 war with ex-Soviet Georgia, as hackers hit Georgian websites while Moscow's troops moved in.

"Cyber-security, cyber-defence and cyber-offence are here to stay. This is a fact of life," Aaviksoo said.

In a report this month, Canadian researchers said a China-based network had stolen Indian military secrets, hacked the Dalai Lama's office and hit computers around the world.

A University of Toronto team traced the attacks to servers in Chengdu, China, but could not identify the culprits. Chengdu is home to Chinese

military communications intelligence units.

"Some reports have, from time to time, been heard of insinuating or criticising the Chinese government... I have no idea what evidence they have or what motives lie behind," Chinese Foreign Ministry spokeswoman Jiang Yu said.

Proving a formal state role in cyber-attacks is close to impossible, because of their fluid nature.

"We're seeing opportunism in terms of citizens bandwagoning on these big events. The role of the state in this is all rather mysterious," said Rex Hughes of the Chatham House think-tank in London.

"I'm sceptical that we'll see an actual cyber-war, where countries will exclusively attack one another over the Internet," he said.

"It remains to be seen if the great cyber Pearl Harbor or 9/11 comes," he added.

(c) 2010 AFP

Citation: NATO's cyber-brains gaze at the future of war (2010, April 24) retrieved 3 May 2024 from https://phys.org/news/2010-04-nato-cyber-brains-future-war.html

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.