NATO plans force to respond to cyber attacks

June 8 2011

NATO Defence ministers during a summit at the NATO headquarters in Brussels. NATO wants to beef up its cyber defence capabilities with the creation of a special task force to detect and respond to Internet attacks, an alliance expert said Wednesday at a conference on cyber security.

NATO wants to beef up its cyber defence capabilities with the creation of a special task force to detect and respond to Internet attacks, an alliance expert said Wednesday at a conference on cyber security here.

"NATO is planning to establish the Cyber Red Team (...) that would provide a significant contribution to the improvement of NATO's cyber defence capability," Luc Dandurand and expert with NATO's C3 Agency told delegates to the alliance's third annual cyber defence conference.

The new NATO cyber force could be involved in simulating threats and controlling readiness to response, gathering and using public information from open sources, scanning and probing networks as well as conducting denial-of-service attacks against specific services or networks, according to Dandurand.

The Symantec cyber security firm recently reported that web-based attacks in 2010 were up 93 percent from 2009.

"The need for such a team is obvious," Dandurand said, adding it would primarily be tasked with detecting, responding to and assessing the "damage cyber attacks can cause in a military sense."

Dandurand also highlighted legal and privacy issues that must be addressed before NATO's cyber force can take shape.

"The two main issues identified at this point are the need to legitimize the Cyber Red Team activities that could otherwise be construed as the malicious or unauthorized use of computer systems, and the potential for invasion of privacy resulting from cyber red team activities," he told experts gathered at NATO's Tallinn-based Cyber Defence Centre.

"Cyber-attacks against Estonia in the Spring of 2007, during Russia's operation in Georgia in 2008, and the many more cyber attacks we have seen worldwide since then have shown us there is a new kind of war that can cause a lot of damage," Major General Jonathan Shaw, a British defence ministry official told delegates.

"We need a response system and we need to learn to respond fast. In the cyber world you have to do lot of homework before the attack in order to be effective," he added.

The three-day conference, which kicked off Tuesday and is attended by

300 international cyber experts, focuses on the legal and political aspects of national and global Internet security.

(c) 2011 AFP