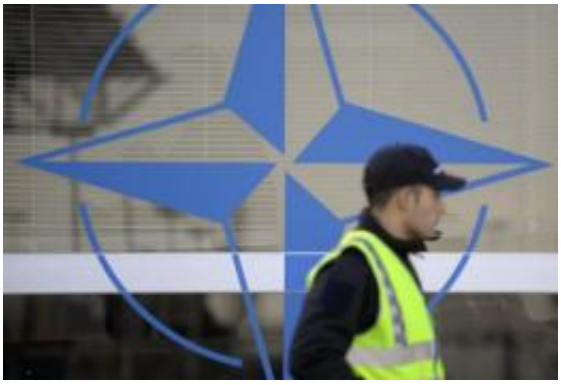
NATO mobilises for cyber warfare

November 18 2010, by Pascal Mallet



A policeman stands guard at a NATO summit in Lisbon, Portugal. There are as many as 100 attempted cyber attacks on the military force every day, IT experts have said.

In 1989, before the Internet revolution, Suleyman Anil was the lone man in charge of the security of NATO's IT system, armed with a single computer.

Two decades later, with the threat of cyber attacks on the rise, Anil oversees two teams tasked with protecting the networks of the alliance's political headquarters in Brussels and operations command in Mons, Belgium.

The threat is constant, with as many as 100 attempted cyber attacks on NATO every day, but it could take just "one in a day to be dangerous," said Anil, a Turkish IT expert who heads NATO's Cyber Defence and

Countermeasures Branch.

NATO leaders meeting at a summit in Lisbon on Friday and Saturday will enshrine cyber security as one of the 28-nation alliance's priorities when they endorse a "strategic concept" to guide its strategy for the next decade.

A message seen on a computer in a NATO office makes the threat clear: "Computer viruses pose a risk to our organisation, varying from anonymous to outright dangerous."

The warning seeks to discourage employees from using USB keys, which can serve as a Trojan horse to plant viruses. But such worms are not the only threat.

The vulnerability of its servers to "professional" and "amateur" hackers was highlighted in 1999 when Serbs flooded NATO with thousands of emails to protest the alliance's bombing campaign in Kosovo, Anil said.

The turning point for NATO came at a summit in Prague in 2002, when leaders asked NATO to improve the security of its computer networks, he told AFP in an interview.

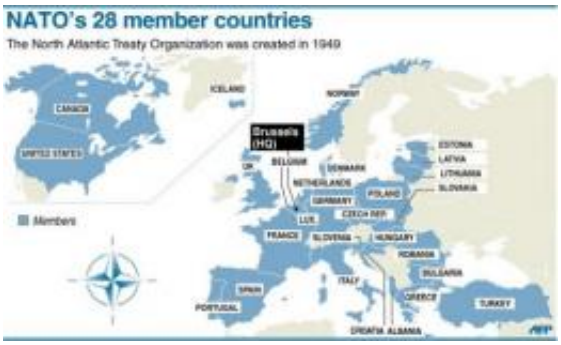
Cyber warfare is one of five sections within a new NATO division against emerging security threats that was created in August.

A costly cyber strike against Estonia in 2007 and the Stuxnet computer worm attack in Iran this year gave new urgency to the need to protect networks.

Following the attack on the Baltic NATO member, the alliance established a research and development centre in Tallin called the Cooperative Cyber Defence Centre of Excellence.

It also decided to establish a rapid reaction team that would be deployed to help any NATO member following a cyber attack.

Although NATO has taken huge strides towards cyber security, it still has work to do.



Map locating the 28 member states of the North Atlantic Treaty Organization.

The transatlantic military organisation will have to wait until 2013 to have 100 percent protection coverage for all its structure following a programme that was launched five years ago.

"We are not yet at the level where we would like to be," Anil said.

There are also legal challenges to linking up cyber defences between allied nations.

Since last year, NATO has signed a memorandum of understanding with seven alliance members on data sharing and procedures to follow in case of a cyber attack. Four other nations will follow suit.

US Admiral James Stavridis, the Supreme Allied Commander Europe,

noted earlier this year the difficulty of governing cyberspace, comparing it to the 10 years it took to establish an international law of the sea.

Meanwhile, the alliance is gearing up for cyberwarfare.

Last year, the United States created its own Cyber Command to respond to computer threats and launch its own offensives.

NATO is in the midst of its third cyber defence exercise since 2008 which began Tuesday and ends Thursday. It involves 24 of 28 alliance members plus Austria.

The "Cyber Coalition 2010" exercise simulates "multiple simultaneous cyber attacks" against NATO and alliance members to test their strategic decision-making process.

(c) 2010 AFP