Stuxnet worm brings cyber warfare out of virtual world

October 1 2010, by Pascal Mallet

An aerial view of Brokdorf nuclear power plant in Germany. Stuxnet, a mysterious computer worm that targets control systems used to manage water supplies, oil rigs and power plants has raised the spectre of a cyber attack as a new weapon of war -- a danger NATO identifies as a key threat.

A mysterious computer worm that has struck Iran has raised the spectre of a cyber attack as a new weapon of war, a danger NATO identifies as a key threat, experts say.

The 28-nation transatlantic alliance will highlight the cyber menace in its new "strategic concept" that will be adopted at a NATO summit in Lisbon next month, according to diplomats.

The danger became all too real with the emergence of Stuxnet in recent weeks, dubbed the world's "first cyber superweapon" by experts, and

which has wreaked havoc on computerised industrial equipment in Iran.

"Are we armed against similar operations? We can ask ourselves on the security of control systems for industries, energy distribution networks or transport," said Daniel Ventre, author of the book "Information Warfare."

"This operation aims to destroy key computer networks, it is not a more common action such as hacking, spying or the dissemination of false information," said Ventre, of the National Scientific Research Centre in Paris.

The virus targets control systems made by German industrial giant Siemens commonly used to manage water supplies, oil rigs, power plants and other industrial facilities.

Chinese media reported this week that Stuxnet had spread to China, infecting millions of computers around the country.

The source of the worm strike on Iran remains unknown, although suspicion has fallen on Israel and the United States, which fear that Tehran is using its nuclear programme to build an atomic bomb, a charge denied by Iran.

Axel Dyevre, a director at the European Company for Strategic Intelligence, said Stuxnet represented "an escalation towards the potential military or political use" of vulnerable computer systems.

The next major conflict could indeed be launched with a traditional bombing campaign in tandem with a cyber blitz, an electronic Pearl Harbor paralysing the enemy.

NATO, which was lightly hassled by Serbian hackers during the Kosovo

war in 1999, has gradually stepped up efforts to protect its own networks since 2002.

The United States urged the alliance last month to build a cyber fortress around its vital military and economic infrastructures.

"NATO has a nuclear shield, it is building a stronger and stronger defence shield, it needs a cyber shield as well," US Deputy Defence Secretary William Lynn said in Brussels on September 15.

An Iranian worker, seen here in 2007, types from a book in Tehran. Stuxnet, a mysterious computer worm that has struck Iran, has raised the spectre of a cyber attack as a new weapon of war -- a danger NATO identifies as a key threat.

The US government kicked off an exercise dubbed "Cyber Storm III" on Tuesday to simulate a large-scale cyber attack on critical infrastructure, with the participation of 60 private companies and 12 international partners.

Stephan De Spiegeleire, a defence expert at the Hague Centre for Strategic Studies, said it was critical for civilians to prepare for the prospect of a computer invasion as well.

"It wouldn't be like the exodus of May 1940, when millions of French and Belgian citizens fled their towns on the road during World War II. This time populations would suddenly be left without electricity, hot water, heating and television," he said.

Aware of the growing danger, the European Union's executive arm proposed new regulations on Thursday to boost the 27-nation bloc's computer defences by improving cooperation against cyber threats.

Several EU states were the target of a botnet, a network of computers infected by malicious software, called 'Conficker' in early 2009, which affected the computers of armed forces in France, Germany and Britain.

A cyber attack against Estonia in 2007 cost the Baltic states between 19 million and 28 million euros.