Davos call for global action against cybercrime

January 26 2012, by Hui Min Neo

File photo of French police working in an anti-cybercrime unit in Villeneuve-d'Ascq. International action to snuff out cybercrime is desperately needed, officials and business leaders said here, warning that criminals move at Internet speed while countries drag their feet.

International action to snuff out cybercrime is desperately needed, officials and business leaders said here, warning that criminals move at Internet speed while countries drag their feet.

Many hackers are no longer just mischievous individuals.

Instead well-funded organisations do it for profit, along with spies and terrorists, but many governments are struggling to fight it.

"Many countries don't have laws to criminalise cyber crime, they don't

have means and tools to investigate, to share information," said Yury Fedotov, who heads the United Nations office on drugs and crime.

Cybercrime is "interconnected in terms of crime, but not interconnected in collaboration" against it, he added, noting that there is not even an agreement on what constitutes cybercrime.

Fedotov said his greatest wish would be "to get a clear definition of cybercrime -- to be clear about what should be rejected by member states and what should be allowed."

A World Economic Forum (WEF) logo is seen on January 25, 2012 at the Congress Center in Davos. Some 1,600 economic and political leaders, including 40 heads of states and governments, will be asked to urgently find ways to reform a capitalist system that has been described as "outdated and crumbling as they converge at eastern Switzerland's chic ski station of Davos.

"Criminals move at the speed of Internet and countries move at speed of democracy -- that's the discrepancy," warned Moises Naim, senior associate at the Carnegie Endowment for International Peace.

In one of the major recent attacks in January, a hacker brought down the

websites of Israel's national carrier El Al and the Tel Aviv Stock Exchange.

It marked the latest incident in a series of attacks only days into 2012, which saw details of tens of thousands of Israeli credit cards posted online and websites defaced by hackers claiming to be from Saudi Arabia or Gaza.

Sami Abu Zuhri, a spokesman for Gaza's Hamas rulers, has hailed the action, describing it as "a sign of the Arab youth's creativity in inventing new forms of Arab and Islamic resistance against the Israeli occupation."

The Israeli market was not the only one subject to such attacks.

US exchange Nasdaq's general counsellor Edward Knight told delegates in Davos that the world's largest exchange company is also "subject to constant attacks, a million or more ... intrusions into our systems."

He complained that there is no clarity on "where is public responsibility and where is private responsibility" on clamping down on such crime.

Unlike real world attacks, the private sector is required to provide its own defence system, even if virtual attacks are coming from foreign governments.

Kevin Johnson, chief executive officer at the US-based Internet infrastructure provider Juniper Networks, urged state authorities to work with private organisations to clamp down on such crime.

"The challenge is that the Internet is a global resource but there are no geographic boundaries on the Internet, yet laws are established by nation states, they are established by geography," he said.

"One recommendation is any solution... is going to require a much higher degree of public, private partnership," Johnson stressed.

(c) 2012 AFP