Threat of next world war may be in cyberspace: UN

Oct 6 12:47 PM US/Eastern

"The next world war could happen in cyberspace and that would be a catastrophe. We have to make sure that all countries understand that in that war, there is no such thing as a superpower," Hamadoun Toure said.

"Loss of vital networks would quickly cripple any nation, and none is immune to cyberattack," added the secretary-general of the International Telecommunications Union during the ITU's Telecom World 2009 fair in Geneva.

Toure said countries have become "critically dependent" on technology for commerce, finance, health care, emergency services and food distribution.

"The best way to win a war is to avoid it in the first place," he stressed.

As the Internet becomes more linked with daily lives, cyberattacks and crimes have also increased in frequency, experts said.

Such attacks include the use of "phishing" tools to get hold of passwords to commit fraud, or attempts by hackers to bring down secure networks.

Individual countries have started to respond by bolstering their defences.

US Secretary for Homeland Security Janet Napolitano said Thursday that she has received the green light to hire up to 1,000 cybersecurity experts to ramp up the United States' defenses against cyber threats.

South Korea has also announced plans to train 3,000 "cyber sheriffs" by next year to protect businesses after a spate of attacks on state and private websites.

Warning of the magnitude of cybercrimes and attacks, Carlos Solari, Alcatel-Lucent's vice-president on central quality, security and reliability, told a forum here that breaches in e-commerce are now already running to "hundreds of billions."

But one of the most prominent victims in recent years has been the small Baltic state of Estonia, which has staked some of its post Cold War development on new technology.

In 2007 a spate of cyber attacks forced the closure of government websites and disrupted leading businesses.

Estonian Minister for Economic Affairs and Communications Juhan Parts said in Geneva that "adequate international cooperation" was essential.

"Because if something happens on cyberspace... it's a border crossing issue. We have to have horizontal cooperation globally," he added.

To this end, several countries have joined forces in the International Multilateral Partnership against Cyber Threats (IMPACT), set up this year to "proactively track and defend against cyberthreats."

Some 37 ITU member states have signed up, while another 15 nations are holding advanced discussions, said the ITU.

Experts say that a major problem is that the current software and web infrastructure has the same weaknesses as those produced two decades ago.

"The real problem is that we're putting on the market software that is as vulnerable as it was 20 years ago," said Cristine Hoepers, general manager at Brazilian National Computer Emergency Response Team.

"If you see the vulnerabilities that are being exploited today, they are still the same," she underlined.

She suggested that professionals needed to be trained to "design something more resilient."

"Universities are not teaching students to think about that. We need to change the workforce, we need to go to the universities..., we need to start educating our professionals," she said.

Pointing out the infrastructure weakness, Carlos Moreira, who founded and runs the Swiss information security firm Wisekey, said legislation is needed to bring cybersecurity up to international standards.