Too much hysteria over cyber attacks: US experts

15 February 2011

Analysts at the National Cybersecurity & Communications Integration Center (NCCIC) during a media session at their headquarters in Arlington, VA in 2010. Overblown talk of a full-on cyber war between nations fueled by recent attacks like the computer worm Stuxnet could hamper Internet security efforts, officials and experts warned Tuesday.

Overblown talk of full-on cyber war between nations fueled by recent attacks like the computer worm Stuxnet could hamper Internet security efforts, officials and experts warned Tuesday.

Serious attention should be paid to threats of cyber attacks from hackers, spies and terrorist groups but not to the extent of mass hysteria, speakers at the premier RSA computer security conference in San Francisco said.

"Cyber war is a terrible metaphor," said White House cybersecurity czar Howard Schmidt. "Don't make it something it's not."

Online espionage and hacking are not new, and hyping incidents as warfare distracts computer security champions from critical jobs such as safeguarding power grids, financial systems, and medical networks, he contended.

"We are in the midst of a cyber war of words," Schmidt said. "Let's quit pointing fingers and start cleaning up the infrastructure."

Renowned computer security specialist Bruce Schneier of BT Group said that use of warlike tactics in online conflicts is fueling hysteria that has the world on the brink of a "cyber arms race."

"We are not necessarily seeing cyber war, but increasing use of warlike tactics in more general cyber conflicts," Schneier said. "I think that is what's confusing us."

He cited a Stuxnet computer virus evidently crafted to find and disrupt an Iranian nuclear facility as an Internet Age attack that smacks of warfare but arguably falls short.

"It is not war," Schneier said. "It is in the middle somewhere."

Fears of cyber war are driving a needless cyber arms race that brings with it the danger that software weapons might accidentally be released, he argued.

"We haven't seen offensive cyber weapons companies, but they are coming," Schneier said. "Big defense contractors are working on this; you know they would be dumb not to."

The most prevalent cyber threat has been theft of information from networks, US Deputy Secretary of Defense William Lynn said in a keynote address to the gathering.

Foreign spy agencies have accessed military plans and weapons systems designs, while source codes and intellectual property have been swiped from businesses and universities, according to Lynn.

Attacks on computer networks have thus far been "relatively unsophisticated" and short in duration, the defense official said.

An emerging threat is that cyber tools will cause real-world damage, according to Lynn.

"The threat is moving up a ladder of escalation, from exploitation to disruption to destruction," he said.

Foreign spies have focused on mining US networks instead of disrupting them, according to Lynn.

"Although we cannot dismiss the threat of a rogue state lashing out, most nations have no more interest in conducting a destructive cyber attack against us than they do a conventional military attack," Lynn said.

"The risk for them is too great."

US defense officials are more worried about an accidental release of "toxic malware," he explained.

"Perhaps the greatest concern in our judgment is a terrorist group that gains the level of disruptive and destructive capability currently possessed by nation-states," Lynn said.

Terrorist groups could craft their own cyber weapons or buy them on the black market, he added.

"As you know better than I, a couple dozen talented programmers wearing flip-flops and drinking Red Bull can do a lot of damage," Lynn told the gathering of software savants.

"We have to assume that if they have the means to strike, they will do so."

Cyber commandos are being trained in the military, and the US is reaching out to allies to form collective online defenses, he said.

Lynn called on specialists in the computer security industry to team with the military to defend the nation's networks.

"The government cannot protect our nation alone," Lynn said. "It is going to take a public-private partnership to secure our networks."