Pentagon: All options on table in cyber-attack (Update)

May 31 2011, by Shaun Tandon

A man surfs the web at an Internet cafe. The Pentagon has adopted a new strategy that will classify major cyber attacks as acts of war, paving the way for possible military retaliation, the Wall Street Journal has reported.

The Pentagon said Tuesday that it would consider all options if the United States were hit by a cyber-attack as it develops the first military guidelines for the age of Internet warfare.

President Barack Obama's administration has been formalizing rules on cyberspace amid growing concern about the reach of hackers. Defense contractor Lockheed Martin said it repelled a major cyber-assault a week ago.

The White House on May 16 unveiled an international strategy statement

on cyber-security which said the United States "will respond to hostile acts in cyberspace as we would to any other threat to our country."

"We reserve the right to use all necessary means -- diplomatic, informational, military, and economic -- as appropriate and consistent with applicable international law, in order to defend our nation, our allies, our partners and our interests," the strategy statement said.

Pentagon spokesman Colonel Dave Lapan said Tuesday that the White House policy did not rule out a military response to a cyber-attack.

"A response to a cyber incident or attack on the US would not necessarily be a cyber-response," Lapan told reporters. "All appropriate options would be on the table if we were attacked, be it cyber."

Lapan said that the Pentagon was drawing up an accompanying cyber defense strategy which would be ready in two to three weeks.

The Wall Street Journal, citing three officials who said they had seen the document, reported Tuesday that the strategy would classify major cyber-attacks as acts of war, paving the way for possible military retaliation.

The newspaper said that the strategy was intended in part as a warning to foes that may try to sabotage the US electricity grid, subways or pipelines.

"If you shut down our power grid, maybe we will put a missile down one of your smokestacks," it quoted a military official as saying.

The newspaper said the Pentagon would likely decide whether to respond militarily to cyber-attacks based on "equivalence" -- whether the attack was comparable in damage to a conventional military strike.

Such a decision would also depend on whether the precise source of the attack could be determined.

The US military suffered its worst cyber-attack in 2008. Deputy Secretary of Defense William Lynn said that a malicious flash drive -- likely from a foreign spy agency -- spread and commandeered computers at US Central Command, which runs the war in Afghanistan.

The attack served as a wakeup call, with the Pentagon setting up a Cyber Command and working up the doctrine for a new type of conflict.

In cyber-warfare, aggressors are often mysterious and hence would not fear immediate retaliation -- a key difference from traditional warfare, in which the fear of one's own destruction is considered a deterrent.

While stepping up defenses, some believe the United States may also be pursuing cyber war. Iran has accused the United States and Israel of last year launching Stuxnet, a worm that reportedly wreaked havoc on computers in the Islamic republic's controversial nuclear program.

The United States and Israel both declined to comment on Stuxnet.

A study released Tuesday by the Center for a New American Society identified the United States, Britain, France, Israel, Russia and China as the leaders in cyber-offense, with Moscow and Beijing viewing cyber-attacks as an attractive option in the event of a major conflict.

But while sophisticated attacks take resources, the study noted that the barriers to entering cyberspace are "extraordinarily low."

"To launch a cyber-attack today, all a person needs is a computer, which costs less than $400 in the United States, an Internet connection and limited technical knowhow," it said.

Joseph Nye, the Harvard University professor and theoretician of power, said in a paper for the report that "it makes little sense to speak of dominance in cyberspace as in sea power or air power."

"If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors," he wrote.

Citation: Pentagon: All options on table in cyber-attack (Update) (2011, May 31) retrieved 25 April 2024 from https://phys.org/news/2011-05-view-major-cyber-war.html