US military prepares new rules for cyber war: Panetta

October 12 2012

File picture shows a US military command center. The United States faces a growing threat of a "cyber-Pearl Harbor" and has drafted new rules for the military that would enable it to move aggressively against digital attacks, Defense Secretary Leon Panetta said.

The United States faces a growing threat of a "cyber-Pearl Harbor" and has drafted new rules for the military that would enable it to move aggressively against digital attacks, Defense Secretary Leon Panetta said late Thursday.

The amended rules of engagement underline the need to defend Defense Department computer networks, "but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace," he said.

Citing a mounting cyber danger that could cripple the country's vital infrastructure, Panetta told an audience in New York: "We won't succeed in preventing a cyber attack through improved defenses alone."

"If we detect an imminent threat of attack that will cause significant physical destruction or kill American citizens, we need to have the option to take action to defend the nation when directed by the president," he said.

"For these kinds of scenarios, the department has developed the capability to conduct effective operations to counter threats to our national interests."

Although he avoided the word "offensive" to describe operations or capabilities, Panetta's speech clearly implied that the military would be empowered to take the initiative in the cyber realm.

Officials offered no further details, but as former CIA director, Panetta reportedly helped oversee an unprecedented cyber sabotage campaign that targeted Iran's uranium enrichment program.

President Barack Obama's administration has not publicly acknowledged the operation, dubbed "Olympic Games," which was detailed in a book by New York Times reporter David Sanger, based on interviews with officials.

"All of those who want to do us harm must know that the Department of Defense will take all action necessary to defend the nation," a senior defense official, who spoke on condition of anonymity, told reporters.

Panetta warned of a "significant escalation of the cyber threat," with foreign actors targeting "critical infrastructure networks," including systems that operate chemical, electricity and water plants, as well as

transport.

He laid out dire scenarios in which hostile states or groups could seize control of vital networks.

The result could be "'cyber-Pearl Harbor': an attack that would cause physical destruction and loss of life, paralyze and shock the nation, and create a profound new sense of vulnerability," he said.

"An aggressor nation or extremist group could gain control of critical switches and derail passenger trains, or trains loaded with lethal chemicals.

"They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country," he said.

Panetta used the speech to press for passage of stalled cyber security legislation, arguing that major firms would not share information with the US government to thwart digital threats without legal protections.

"Companies should be able to share specific threat information with the government without the prospect of lawsuits hanging over their head," said Panetta, adding that the administration would safeguard civil liberties.

With a proposed budget of $3.4 billion, the US military's newly created Cyber Command is increasingly able to trace the origin of digital assaults, he said.

The new capability will serve as a deterrent to any potential cyber adversary, as the Pentagon will be able to track down the authors of an attack and "hold them accountable," he added.

The Defense Department has the job of safeguarding military computer networks and supporting efforts by the Department of Homeland Security and the FBI to protect civil networks.

Speaking to an audience of business executives, Panetta cited an alarming "Shamoon" virus that recently hit networks at Saudi Arabia's state oil company Aramco, disabling more than 300,000 computers.

He called the sophisticated virus "the most destructive attack that the private sector has seen to date."

(c) 2012 AFP