

Defense Secretary Leon Panetta has acknowledged for the first time that US military forces are able to carry out retaliatory or preemptive acts of cyber warfare.

Panetta's comment at a conference in New York marked a significant shift in the Department of Defense (DOD) long-standing position that US forces are focused only on defensive measures in cyberspace.

"Our mission is to defend this nation. We defend. We deter. And if called upon, we take decisive action," he told delegates.

Pentagon officials have previously remained almost silent on the US ability to wage cyber war against nations or non-state actors.

"If a crippling cyber attack were launched against our nation, the American people must be defended," Panetta said. "And if the commander in chief orders a response, the Defense Department must be ready to act."

Pentagon cyber warfare specialists are currently drawing up new rules of engagement in the arena.

The rules will include clear guidance on when, where and how US forces can carry out a cyber attack, Panetta emphasised.

US officials have previously argued that the biggest problem in carrying out offensive cyber warfare was the difficulty in pinpointing where an attack had originated.

Significant technology investment apparently now allows the Pentagon's cyber specialists to track attacks in real time and launch counter-measures.

Defense Secretary Panetta warned that certain foreign countries, non-state actors and a disparate array of hackers had the ability to strike at the country's power grid, financial networks and transport system.

He was careful not to identify any specific country or group, but officials have previously identified China, Russia, Iran and numerous militant groups as the major sources of danger in cyberspace.

Panetta highlighted the Shamoon virus, which knocked out 30,000 computers at Saudi Arabia's state oil company, ARAMCO, in the summer, as a sign of what could happen in the US without adequate defences.

He also spoke of denial-of-service attacks against major US banks earlier in the year, which delayed or disrupted services on customer websites.

Arguing that improved defences alone might not prevent a catastrophic cyber-attack, Panetta made it abundantly clear the US would strike first if threatened.

"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.