Pentagon to publish strategy for cyberspace wars

July 14 2011, By LOLITA C. BALDOR , Associated Press

(AP) -- Facing escalating risks of cyberattacks by hackers, criminals and other nations, the Pentagon is developing more resilient computer networks so the military can continue to operate if critical systems are breached or taken down.

In a broad new cybersecurity strategy to be released Thursday, the Defense Department lays out its vulnerabilities to attack from both outside and within its own workforce. Formally declaring cyberspace a new warfare domain, much like air, land and sea, the new strategy stresses the need for the military to continue to operate if its computer systems are attacked and degraded.

The Associated Press reviewed a draft copy of the 12-page, unclassified summary of the strategy to be released by The Pentagon.

The strategy is the final step in the administration's effort to map out how to handle the escalating threat of destructive cyberattacks, including potential assaults on critical infrastructure such as the electrical grid, financial networks or power plants.

Details about how the military would respond to a cyberattack or discussion of any offensive cyberspace operations by the U.S. are not included in the summary. That information is in classified documents and directives. The classified version of the Pentagon strategy is about 40 pages.

Earlier this year, President [Barack Obama](#) signed executive orders that lay out how far military commanders around the globe can go in using cyberattacks and other computer-based operations against enemies and as part of routine espionage in other countries.

The orders detail when the military must seek presidential approval for a specific [cyberattack](#) on an enemy, defense officials and cybersecurity experts told the AP.

The orders and the new strategy cap a two-year Pentagon effort to draft U.S. rules of the road for cyberspace warfare, and come as the U.S. begins to work with allies on global ground rules.

Noting that Defense Department systems are vulnerable to attack, the strategy says the Pentagon must develop resilient networks that can detect and fend off attacks. At the same time, the [military](#) must have multiple networks and be able to shift its operations from one system to another in order to keep operating in the event of an attack.

That research is ongoing.

The strategy also warns that theft of intellectual property is the "most pervasive cyber threat." And it calls for more significant efforts to insure the integrity of the supply chain, so that software does not come with vulnerabilities that allow hackers to infiltrate.