US Struggles with How to Retaliate in Cyber Attacks

Lolita C. Baldor, AP Writer

WASHINGTON (AP) - - In the murky world of computer espionage, the U.S. faces hard choices on how to retaliate when government or privately owned networks come under cyber attack, senior military and intelligence officials said Tuesday.

As the administration grapples with how best to defend its computer networks, debate is raging over how far the U.S. can go in pursuit of cyber criminals, and even what constitutes a digital act of war.

The most immediate challenge is identifying the hacker, terrorist or enemy nation that launched the attack in vast and anonymous cyberspace, officials said. That hurdle is complicated by privacy debates over how deeply the government can wade into privately owned systems to investigate threats, and how it should handle attacks against a company, as opposed to a federal agency.

U.S. law allows "hot pursuit" of criminals, said former Air Force Secretary Michael Wynne, so computer users "may have to tolerate some hot pursuit" through their digital world so authorities can track and ultimately respond to cyber crimes.

Speaking to a crowd of corporate and government technology experts at a conference sponsored by Defense Daily, Wynne and others painted a grim picture of the country's cyber security.

"In the face of our almost universal reliance on untrusted systems, the United States currently is facing a grave national security challenge in the form of exploitation of our government and private-sector networks and information," said Steven Chabinsky, assistant deputy director of cyber issues for the Obama administration's director of national intelligence. "This exploitation is occurring on an unprecedented scale by a growing array of state and non-state actors."

Chabinsky said the U.S. needs to figure out what it is prepared to do in the face of a cyber assault, such as an action that takes down the electrical grid. And, since the grid is privately run, officials must also decide how any counterattack should be coordinated with the corporate world.

He added that while other powerful nations have the ability to take down critical U.S. computer systems, they probably don't have the intent, because it would be a declaration of war.

Just last Friday, President Barack Obama announced he would appoint a cyber czar

to work out of the White House and coordinate the nation's cyber security. The country, he said, is not as prepared as it should be to take on cyber threats.

But as the nation tries to police a digital world with no geography and no boundaries, the U.S. must also balance security with the liberties that Americans hold dear, said Brig. Gen. Michelle Johnson, deputy director for cyber issues for the Joint Staff.

She said that while cyberspace is the new war fighting domain that must be defended, officials also must consider privacy questions and set legal boundaries.