US Cyberwarfare Prep Includes Offense

Apr 6 01:35 PM US/Eastern
By ANICK JESDANUN
AP Internet Writer
http://www.breitbart.com/article.php?id=D8VSGL800&show_article=1

NEW YORK (AP) - U.S. military officials seeking to boost the nation's cyberwarfare capabilities are looking beyond defending the Internet: They are developing ways to launch virtual attacks on enemies.

But first the military will have to figure out the proper boundaries.

"What do we consider to be an act of war in cyberspace?" asked Lt. Gen. Robert J. Elder Jr., who heads the Air Force's cyberoperations command. "The military is not going to tend to do that (use virtual strike capabilities) until you cross some line that constitutes an act of war."

Elder said initial uses likely would be limited to diverting or killing data packets that threaten the nation's systems, the way the military may intercept a foreign ship carrying arms in international waters.

The remarks came late Friday during a New York chapter meeting of the Association For Intelligence Officers, a nonprofit group for current and former intelligence agents and their supporters.

In an interview afterward, Elder said that in the future, the military might rely upon network warfare to disrupt an enemy's communications system, replacing the need for conventional weapons like bombs.

In any such scenario, Elder said the military would be restricted by the same rules of engagement—such as requirements for a formal declaration of war—that apply to conventional attacks.

Elder said that during the early days of the Iraq war, rudimentary forms of cyberattacks were used by the United States, including electronically jamming Iraqi military systems and using network attacks to hinder Iraqi ground units from communicating with one another.

The military's offensive capabilities have improved since then, he said.

As the military increasingly relies on networks and computer systems to communicate and coordinate conventional operations, the U.S. Air Force is planning to establish by October a Cyber Command for waging a future war that is fought not only by land, sea and air but also in cyberspace.

Hackers with a foreign government or terrorist group potentially could bring down military and civilian Web sites using what's known as a denial-of-service attack—flooding the computer servers with fake traffic such that legitimate visitors can't get through.

Enemies also could look for security vulnerabilities to break into key systems that run power plants, refineries and other infrastructure.

Already, the Chinese government has been suspected of using the Web to break into computers at the Defense Department and other U.S. agencies in what was dubbed Operation Titan Rain. Since 2001, Chinese "hacktivists" have organized attacks on and defaced U.S. Web sites to oppose what

they call the imperialism of the United States and Japan.

Elder outlined several defensive initiatives aimed at deterring cyberattacks on the United States.

The military, for instance, needs to demonstrate that its conventional operations still could function even if the network is disrupted. To do that, he said, the military has been identifying "what if" loss scenarios and figuring out the backup capabilities needed to overcome them.

Forensics capabilities also are being developed, he said, to identify who is attacking, even if the attacker tries to hide by spoofing the identity of packets and rerouting them through intermediary computer servers. That way, the United States can make a credible threat of retribution.