AVIATION WEEK

Click to Print

Close

By David A. Fulghum

The denial-of-services cyber attack — attributed to North Korea — that disabled at least three Washington, D.C.-based U.S. government agencies, and is still being cleaned up, appears to have had minor technological effects, but major implications for long-term policy, economics and military training.

"I won't go into great detail about specifics [of the attacks attributed to North Korea]," says the chairman of the Joint Chiefs of Staff, Adm. Mike Mullen. "I'm growing increasingly concerned about the cyber world and the attacks, whether they are from individual attackers or from state entities. There has been a significant investment in [analyzing and preventing] that. It has become a mainstream issue for all of leadership.

"We need to raise more people who are capable in this area," Mullen continued. "The fiscal 2010 budget was a very comprehensive approach to the future, including a significant investment not just in irregular warfare ... but also in the cyber world. We need to have it as a big part of our focus now and in the future."

A senior cyber warfare researcher and practitioner with insight into National Security Agency capabilities as well as network attack and defense characterizes the attacks on government agencies as no surprise and increasingly a fact of daily life in the cyber world.

Asked if it's big news in his world or business as usual, he replied, "As the Dylan song says, 'it happens every day…'"

A Cato Institute specialist was equally dismissive, at least to the perception of the attacks being anything unexpected or unusual.

The cyber attacks were launched against South Korean and U.S. government Web sites. Jim Harper, director of information policy studies at Cato, says that despite cyber fears, most Americans will probably not know about cyber attacks, and those who do will learn about them by reading about them. Only a few people noticed the absence of the violated Web sites, and it illustrates that this type of cyberwar has little strategic value and little capacity to do real damage, he says.

These results illustrate that cyber terrorism doesn't exist because it isn't terrifying. Harper does agree that it is important to secure Web sites, data, and networks against all threats, but this can be done methodically and successfully by the distributed owners and controllers.

The Defense Department was not a target of the North Korean attacks, but it is "constantly probed in the cyber world and has been for some time," Mullin says. "We are alert and recognize probes and are responding."

The Secret Service and Federal Trade Commission Web sites, as well as those of the Treasury and Transportation departments, were down periodically over the July 4th weekend and outages continued into this week.

Immediate effects of the attacks were not considered unusual, but the continuation of disruptions after three days puts them in a relatively unique category of unusually long and sophisticated cyberwarfare.

Photo: Wikipedia