From: The INTELST Forum [mailto:INTELST@LISTSERV.ARMY.PENTAGON.MIL] On Behalf Of Krishna Mungur

Sent: Friday, November 28, 2008 9:37 AM

To: INTELST@LISTSERV.ARMY.PENTAGON.MIL

Subject: Cyber-attack on Defense Department computers raises concerns

http://www.latimes.com/news/nationworld/nation/la-na-cyberattack28-2008nov28,0,6441140.story

Cyber-attack on Defense Department computers raises concerns The 'malware' strike, thought to be from inside Russia, hit combat zone computers and the U.S.

Central Command overseeing Iraq and Afghanistan. The attack underscores concerns about computer warfare.

By Julian E. Barnes

November 28, 2008

Reporting from Washington -- Senior military leaders took the exceptional step of briefing President Bush this week on a severe and widespread electronic attack on Defense Department computers that may have originated in Russia -- an incursion that posed unusual concern among commanders and raised potential implications for national security.

Defense officials would not describe the extent of damage inflicted on military networks. But they said that the attack struck hard at networks within U.S.

Central Command, the headquarters that oversees U.S. involvement in Iraq and Afghanistan, and affected computers in combat zones. The attack also penetrated at least one highly protected classified network.

Military computers are regularly beset by outside hackers, computer viruses and worms. But defense officials said the most recent attack involved an intrusive piece of malicious software, or "malware,"apparently designed specifically to target military networks.

"This one was significant; this one got our attention," said one defense official, speaking on condition of anonymity when discussing internal assessments.

Although officials are withholding many details, the attack underscores the increasing danger and potential significance of computer warfare, which defense experts say could one day be used by combatants to undermine even a militarily superior adversary.

Bush was briefed on the threat by Navy Adm. Michael G. Mullen, chairman of the Joint Chiefs of Staff.

Mullen also briefed Defense Secretary Robert M. Gates.

Military electronics experts have not pinpointed the source or motive of the attack and could not say whether the destructive program was created by an individual hacker or whether the Russian government may have had some involvement. Defense experts may never be able to answer such questions, officials said.

The defense official said the military also had not learned whether the software's designers may have been specifically targeting computers used by troops in Afghanistan and Iraq.

However, suspicions of Russian involvement come at an especially delicate time because of sagging relations between Washington and Moscow and growing tension over U.S. plans to develop a missile defense system in Eastern Europe. The two governments also have traded charges of regional meddling after U.S. support for democratic elections in former Soviet states and recent Russian overtures in Latin America.

U.S. officials have worried in recent years about the possibility of cyber-attacks from other countries, especially China and Russia, whether sponsored by governments of those countries or launched by individual computer experts.

An electronic attack from Russia shut down government computers in Estonia in 2007. And officials believe that a series of electronic attacks were launched against Georgia at the same time that hostilities erupted between Moscow and Tbilisi last summer.

Russia has denied official involvement in the Georgia attacks.

The first indication that the Pentagon was dealing with a computer problem came last week, when officials banned the use of external computer flash drives. At the time, officials did not indicate the extent of the attack or the fact that it may have targeted defense systems or posed national security concerns.

The invasive software, known as agent.btz, has circulated among nongovernmental U.S. computers for months. But only recently has it affected the Pentagon's networks. It is not clear whether the version responsible for the cyber-intrusion of classified networks is the same as the one affecting other computer systems.

The malware is able to spread to any flash drive plugged into an infected computer. The risk of spreading the malware to other networks prompted the military to ban the drives.

Defense officials acknowledged that the worldwide ban on external drives was a drastic move. Flash drives are used constantly in Iraq and Afghanistan, and many officers keep them loaded with crucial information on lanyards around their necks.

Banning their use made sharing information in the war theaters more difficult and reflected the severity of the intrusion and the threat from agent.btz, a second official said.

Officials would not describe the exact threat from agent.btz, or say whether it could shut down computers or steal information. Some computer experts have reported that agent.btz can allow an attacker to take control of a computer remotely and to take files and other information from it.

In response to the attack, the U.S. Strategic Command, which oversees the military's cyberspace defenses, has raised the security level for its so-called information operations condition, or "INFOCON," initiating enhanced security measures on military networks.

The growing possibility of future electronic conflicts has touched off debates among U.S. defense experts over how to train and utilize American computer warfare specialists. Some have advocated creating offensive capabilities, allowing the U.S. to develop the ability to intrude into the networks of other countries.

But most top leaders believe the U.S. emphasis in cyberspace should be on improving defenses and gathering intelligence, particularly about potential threats.

On Tuesday, Gen. Norton A. Schwartz, Air Force chief of staff, received a specialized briefing about the malware attack. Officers from the Air Force Network Operations Center at Barksdale Air Force Base in Louisiana outlined their efforts to halt the spread of the malware and to protect military computers from further attack.

Schwartz, praising those efforts, said that the attack and the military's response were being closely monitored by senior military leaders.

The offending program has been cleansed from a number of military networks. But officials said they did not believe they had removed every bit of infection from all Defense Department computers.

"There are lots of people working hard to remove the threat and put in preventive measures to protect the grid," said the defense official. "We have taken a number of corrective measures, but I would be overstating it if I said we were through this."

Barnes is a writer in our Washington bureau.

julian.barnes@latimes.com