Defense official discloses cyberattack

washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html

Now it is official: The most significant breach of U.S. military computers was caused by a flash drive inserted into a U.S. military laptop on a post in the Middle East in 2008.

In an article to be published Wednesday discussing the Pentagon's cyberstrategy, Deputy Defense Secretary William J. Lynn III says malicious code placed on the drive by a foreign intelligence agency uploaded itself onto a network run by the U.S. military's Central Command.

"That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control," he says in the Foreign Affairs article.

"It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary."

Lynn's decision to declassify an incident that Defense officials had kept secret reflects the Pentagon's desire to raise congressional and public concern over the threats facing U.S. computer systems, experts said.

Much of what Lynn writes in Foreign Affairs has been said before: that the Pentagon's 15,000 networks and 7 million computing devices are being probed thousands of times daily; that cyberwar is asymmetric; and that traditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult to identify the instigator of an attack.

But he also presents new details about the Defense Department's cyberstrategy, including the development of ways to find intruders inside the network. That is part of what is called "active defense."

He puts the Homeland Security Department on notice that although it has the "lead" in protecting the dot.gov and dot.com domains, the Pentagon - which includes the ultra-secret National Security Agency - should support efforts to protect critical industry networks.

Lynn's declassification of the 2008 incident has prompted concern among cyberexperts that he gave adversaries useful information. The Foreign Affairs article, Pentagon officials said, is the first on-the-record disclosure that a foreign intelligence agency had penetrated the U.S. military's classified systems. In 2008, the Los Angeles Times reported, citing anonymous Defense officials, that the incursion might have originated in Russia.

The Pentagon operation to counter the attack, known as Operation Buckshot Yankee, marked a turning point in U.S. cyberdefense strategy, Lynn said. In November 2008, the Defense Department banned the use of flash drives, a ban it has since modified.

Infiltrating the military's command and control system is significant, said one former intelligence official who spoke on the condition of anonymity because of the sensitivity of the matter. "This is how we order people to go to war. If you're on the inside, you can change orders. You can say, 'turn left' instead of 'turn right.' You can say 'go up' instead of 'go down.' "

In a nutshell, he said, the "Pentagon has begun to recognize its vulnerability and is making a case for how you've got to deal with it."