Military Computer Attack Confirmed

nytimes.com/2010/08/26/technology/26cyber.html

Brian Knowlton August 25, 2010

Continue reading the main story

WASHINGTON — A top Pentagon official has confirmed a previously classified incident that he describes as "the most significant breach of U.S. military computers ever," a 2008 episode in which a foreign intelligence agent used a flash drive to infect computers, including those used by the Central Command in overseeing combat zones in Iraq and Afghanistan.

Plugging the cigarette-lighter-sized flash drive into an American military laptop at a base in the Middle East amounted to "a digital beachhead, from which data could be transferred to servers under foreign control," according to William J. Lynn 3d, deputy secretary of defense, writing in the latest issue of the journal Foreign Affairs.

"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," Mr. Lynn wrote.

The incident was first reported in November 2008 by the Danger Room blog of Wired magazine, and then in greater detail by The Los Angeles Times, which said that the matter was sufficiently grave that President George W. Bush was briefed on it. The newspaper mentioned suspicions of Russian involvement.

But Mr. Lynn's article was the first official confirmation. He also put a name — Operation Buckshot Yankee — to the Pentagon operation to counter the attack, and said that the episode "marked a turning point in U.S. cyber-defense strategy." In an early step, the Defense Department banned the use of portable flash drives with its computers, though it later modified the ban.

Mr. Lynn described the extraordinary difficulty of protecting military digital communications over a web of 15,000 networks and 7 million computing devices in dozens of countries against farflung adversaries who, with modest means and a reasonable degree of ingenuity, can inflict outsized damage. Traditional notions of deterrence do not apply.

"A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States's global logistics network, steal its operational plans, blind its intelligence capabilities or hinder its ability to deliver weapons on target," he wrote.

Security officials also face the problem of counterfeit hardware that may have remotely operated "kill switches" or "back doors" built in to allow manipulation from afar, as well as the problem of software with rogue code meant to cause sudden malfunctions.

Against the array of threats, Mr. Lynn said, the National Security Agency had pioneered systems — "part sensor, part sentry, part sharpshooter" — that are meant to automatically counter intrusions in real time.

His article appeared intended partly to raise awareness of the threat to United States cybersecurity — "the frequency and sophistication of intrusions into U.S. military networks have increased exponentially," he wrote — and partly to make the case for a larger Pentagon role in cyberdefense.

Various efforts at cyberdefense by the military have been drawn under a single organization, the U.S. Cyber Command, which began operations in late May at Fort Meade, Maryland, under a four-star general, Keith B. Alexander.

But under proposed legislation, the Department of Homeland Security would take the leading role in the defense of civilian systems.

Though the Cyber Command has greater capabilities, the military operates within the United States only if ordered to do so by the president.

Another concern is whether the Pentagon, or government in general, has the nimbleness for such work. Mr. Lynn acknowledged that "it takes the Pentagon 81 months to make a new computer system operational after it is first funded." By contrast, he noted, "the iPhone was developed in 24 months."