US defense programs target of China cyber threat

May 29 2013, by Lolita C. Baldor

New revelations that China used cyberattacks to access data from nearly 40 U.S. weapons programs and almost 30 other defense technologies have increased pressure on American leaders to take more strident action against Beijing to stem the persistent breaches.

The disclosure, which was included in a Defense Science Board report released earlier this year but is only now being discussed publicly, comes as Defense Secretary Chuck Hagel heads to Southeast Asia, where he will discuss the escalating cyberthreat with counterparts from a number of area nations.

While officials have been warning for years about China's cyber espionage efforts aimed at U.S. military and high-tech programs, the breadth of the list underscored how routine the attacks have become. And, as the U.S. looks to grow its military presence in the Asia Pacific, it heightens worries that China can use the information to blunt America's military superiority and keep pace with emerging technologies.

"It introduces uncertainty on how well the weapons may work, and it means we may have to redo weapons systems," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies. "If they know how it works precisely, they will be able to evade it and figure out how to better beat our systems."

A chart included in the science board's report laid out what it called a

partial list of 37 breached programs, which included the Terminal High Altitude Area Defense weapon—a land-based missile defense system that was recently deployed to Guam to help counter the North Korean threat. Other programs include the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet, and the hybrid MV-22 Osprey, which can take off and land like a helicopter and fly like an airplane.

The report also listed another 29 broader defense technologies that have been compromised, including drone video systems and high-tech avionics. The information was gathered more than two years ago, so some of the data is dated and a few of the breaches—such as the F-35—had actually already become public.

The details of the breaches were first reported by The Washington Post.

According to a defense official, the report is based on more than 50 briefings that members of the board's task force received from senior leaders in the Pentagon, the State Department, the intelligence community, national laboratories and business. The official was not authorized to discuss the report publicly so spoke on condition of anonymity.

U.S. officials have been far more open about discussing the China cyberattacks over the past year or two, beginning with a November 2011 report by U.S. intelligence agencies that accused China of systematically stealing American high-tech data for its own national economic gain. The Pentagon, meanwhile, in its latest report on China's military power, asserted publicly for the first time that Beijing's military was likely behind computer-based attacks targeting federal agencies.

"In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese

government and military," said the report, which was released earlier this month.

In Beijing on Wednesday, Assistant Foreign Minister Zheng Zeguang did not directly address the allegations, but said that China opposes all hacking and referred to an agreement with the U.S. to form a cybercrime working group.

Cybersecurity experts have for some time been urging the U.S. government to use sanctions or other punishments against China for the breaches.

The benefits to the cyber espionage are high and the costs are low, said Shawn Henry, former cyber director at the FBI and now president of CrowdStrike Services, a security technology company.

"There is no cost, there are no sanctions, no diplomatic actions, no financial disincentives," said Henry, adding that the U.S. intellectual property losses are in the hundreds of millions of dollars. He said that the U.S. needs to have a discussion with Chinese leaders about "what the red lines are and what the repercussions will be for crossing those red lines."

U.S. leaders, including President Barack Obama, however, have instead been using the bully pulpit to increase pressure on the Chinese to confront the problem. Obama is expected to raise the issue with China's new leader Xi Jinping during a summit next month in Southern California.

Pentagon Press Secretary George Little said Tuesday that the Pentagon maintains "full confidence in our weapons platforms," adding that the department has taken a number of steps to strengthen its network defenses and monitor for threats.

Defense contractors, meanwhile, declined to say whether their systems had been breached. But recent filings to shareholders indicate these companies see intrusions as a serious risk to their business, particularly when they must rely on third-party suppliers.

In its most recent annual report, Lockheed Martin—a primary contractor on missile defense programs—told shareholders that prior cyberattacks "have not had a material impact on our financial results," and that it believed its security efforts were adequate.

However, suppliers and subcontractors have "varying levels of cybersecurity expertise and safeguards and their relationships with government contractors, such as Lockheed Martin may increase the likelihood that they are targeted by the same cyber threats we face," according to the 2012 report.

In a statement emailed to reporters on Tuesday, Lockheed Martin said it has made "significant investments" in cybersecurity and that the company was trying to secure its supply chain given that "program information resides in a large cyber ecosystem."

Similar risk disclosures to shareholders have been made recently by Northrop Grumman, Boeing and Raytheon. For example, Northrop Grumman wrote in its 2012 annual report that cyber intrusions "could damage our reputation and lead to financial losses from remedial actions, loss of business or potential liability."

Company spokesman Randy Belote on Tuesday declined to say whether Northrop Grumman's systems had been breached, citing company policy. But, he added, "the number of attempts to breach our networks (is) increasing at an alarming rate."