U.S. says will boost its cyber arsenal

Jim Wolf, Reuters

The Pentagon's advanced research arm said Monday it is boosting efforts to build offensive cyber arms for possible keyboard-launched U.S. military attacks against enemy targets.

The military needs "more and better options" to meet cyber threats to a growing range of industrial and other systems controlled by computers vulnerable to penetration, including cars, Regina Dugan, director of the Defense Advanced Research Projects Agency, told a first-of-its kind conference.

"Modern warfare will demand the effective use of cyber, kinetic and combined cyber and kinetic means," she said. Kinetic is military parlance for traditional ways of fighting such as dropping bombs, firing missiles and rolling tanks in.

Dugan's agency, known as DARPA, opened the session to what it called "visionary hackers" as well as academics and others in an effort to "change the dynamic of cyber defense" amid mounting U.S. concern over vulnerabilities of networks and computer-controlled hardware.

The Office of the National Counterintelligence Executive, a U.S. government body, said in a report to Congress last week that China and Russia are using cyber espionage to steal U.S. trade and technology secrets to bolster their fortunes at U.S. expense.

DARPA officials told the session that a recent in-house analysis had found that layered U.S. defenses alone, as currently configured, were a losing proposition because of a cyber attacker's lopsided advantage.

The cost of creating software security packages, some now involving up to 10 million lines of code, has soared in the past 20 years, the agency's survey found, while malicious software still requires only 125 lines on average.

"This is not to suggest that we stop doing what we are doing in cyber security," Dugan told an audience of about 700 in a hotel ballroom outside Washington. "But if we continue only down the current path, we will not converge with the threat," meaning deal effectively with it.

DARPA's mission is to maintain the U.S. military's technology edge and prevent a high-tech surprise by sponsoring high-payoff research with military applications.

REAL THREAT

"Malicious cyber attacks are not merely an existential threat to our bits and bytes. They are a real threat to our physical systems, including our military systems," Dugan said.

U.S. officials stepped up warnings about possible destructive cyber attacks after the computer virus Stuxnet emerged in 2010, disrupting centrifuges that Iran uses to enrich uranium for what the United States and some European nations have charged is a covert nuclear weapons program.

Daniel Roelker, a DARPA project manager dressed in faded jeans and T-shirt who works on offensive cyber weapons, said the Pentagon needed technological breakthroughs to be able to fight at the speed of light in cyberspace.

The United States and unspecified "adversaries" are locked in a struggle in cyberspace, said another program manager, Timothy Fraser. "Their costs are very low, and our costs are very high," he said.

Modern cars' brakes, accelerators and steering were among the systems that "we need to worry about" because they could be hacked by tapping into their diagnostic boards, even remotely, Kathleen Fisher, a third program manager said.

The DARPA budget request for fiscal 2012, which began October 1, called for its cyber research funding to jump more than 73 percent to $208 million from $120 million.

The agency plans to boost its investment in cyber research over the next five years to 12 percent of its budget from 8 percent even as overall U.S. military-related spending is set to decline As part of deficit cutting.

DARPA "has a special responsibility to explore the outer bounds of such capabilities so that our nation is well prepared for future challenges," Dugan said, citing its role in creating Arpanet in the 1960s, forerunner of the Internet.

U.S. officials have declined to discuss publicly U.S. offensive capabilities in cyberspace. One key concern is whether the United States can defend against possible retaliatory cyber attacks that might target such things as transportation, banking systems and power grids.

James Miller, principal deputy undersecretary of Defense for policy, told a separate event hosted by the Center for Strategic and International Studies that the United States had a "full spectrum of cyber capabilities," by implication including existing cyber weapons.

(Additional reporting by Andrea Shalal-Esa; editing by Anthony Boadle)