

Pentagon looks for weapons to wage cyber warfare

November 7 2011



Analysts watch monitors in Arlington, VA in 2010. The Pentagon's researchers plan to bolster their efforts to create offensive weapons for use in cyber warfare, reflecting a growing concern over digital threats, US officials said Monday.

The Pentagon's researchers plan to bolster their efforts to create offensive weapons for use in cyber warfare, reflecting a growing concern over digital threats, US officials said Monday.

The US government needed "more and better options" to safeguard the country from assaults on sensitive computer networks and had to invest in both offensive and defensive tools, said Regina Dugan, director of the Pentagon's research arm, the Defense Advanced Research Projects Agency (DARPA).

"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 told a conference.

"To this end, in the coming years we will focus an increasing portion of our cyber research on the investigation of offensive capabilities to address military-specific needs," she said.

DARPA has proposed boosting funding in cyber research in the proposed 2012 budget from \$120 million to \$208 million and the Defense Department leadership has called for \$500 million in funding for cyber security over the next five years, she said.

With other countries pursuing cyber warfare capabilities and the danger from digital attacks growing by the day, the United States had to look at developing "offensive" arms to protect national security, said Dugan, without specifying what weapons could be employed.

"Our first goal must be to prevent war. We do so in part by being prepared for it. Failing prevention, however, we must accept our responsibility to be prepared to respond," she said.

Even while preparing for possible digital war, US policy makers must protect civil liberties and the "peaceful shared use of cyberspace," she added.

A recent DARPA analysis of cyber security over several months concluded that the US government had to rethink how it defends cyberspace to keep up with a threat evolving at lightning speed.

"Why is it that despite billions of dollars in investment and the concerted efforts of many dedicated individuals, it feels like we are losing ground?"

The DARPA study found that security software had grown more and more complex over the past two decades -- involving up to ten million lines of code -- while various viruses and other digital assaults required

an average of 125 lines of code for malware, according to Dugan.

"This is not to suggest that we stop doing what we are doing in cyber security. On the contrary, our existing efforts are necessary," she said. "These efforts represent the wisdom of the moment. But if we continue only down the current path, we will not converge with the threat."

DARPA organized the "cyber colloquium" in the Washington suburb of Arlington to help find better ways to address the digital threat, inviting members of industry, government and academia -- including "white hat" hackers, she said.

At the same event, the head of the National Security Agency, the secretive intelligence agency that carries out eavesdropping on foreign communications, and the US military's newly created cyber command, General Keith Alexander, proposed one way to improve the country's cyber defenses -- cloud computing.

By shifting to a "cloud architecture," the United States would save money and be better placed to protect vital computer networks, Alexander said.

The current complex web of government and military networks is unwieldy and intelligence agencies cannot easily monitor for intrusions or attacks, he said.

(c) 2011 AFP

Citation: Pentagon looks for weapons to wage cyber warfare (2011, November 7) retrieved 19 April 2024 from <https://phys.org/news/2011-11-pentagon-weapons-wage-cyber-warfare.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.