

# Pentagon: Military Response To Cyber Attack Possible

By [Global Research](#)

Global Research, May 14, 2010

[AFP](#) 12 May 2010

Region: [USA](#)

Theme: [US NATO War Agenda](#)

WASHINGTON – The Pentagon would consider a military response in the case of a cyber attack against the United States, a U.S. defense official said May 12.

Asked about the possibility of using military force after a cyber assault, James Miller, undersecretary of defense for policy, said: “Yes, we need to think about the potential for responses that are not limited to the cyber domain.”

But he said it remained unclear what constituted an act of war in cyberspace.

“Those are legal questions that we are attempting to address,” Miller said at a conference in Washington, adding that “there are certainly a lot of gray areas in this field.”

He said hostile acts in cyberspace covered a wide range, from digital espionage to introducing false data into a network, that did not necessarily represent full-blown war.

But he said the threat to U.S. networks from terrorists, criminals and others was real and growing.

“Over the past decade, we’ve seen the frequency and the sophistication of intrusions into our networks increase,” he said. “Our systems are probed thousands of times a day.”

The Defense Department has about 90,000 employees and troops using computer networks, with about 7 million computer devices, he said.

The U.S. military recently created a new cyber command that will be led by Army Lt. Gen. Keith Alexander, head of the National Security Agency. Alexander was confirmed in his post by the U.S. Senate last week.

In written testimony to Congress, Alexander said that the cyber command would be prepared to wage offensive operations as well, despite the risk of sustaining damage to U.S. networks.

He told lawmakers that he expected digital operations to take place as part of a wider military campaign, but that special legal authority would be required to respond to a cyber attack staged from a neutral country.

---

## [Comment on Global Research Articles on our Facebook page](#)

## [Become a Member of Global Research](#)

Articles by: [Global Research](#)

**Disclaimer:** The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)

[www.globalresearch.ca](http://www.globalresearch.ca) contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)