



Defense Science Board warns of cyber problems

By [Alice Lipowicz](#)

Published on November 7, 2008

The U.S. military's dependence on sophisticated network-centric information technology has become its "Achilles heel," according to a new report from the Defense Science Board.

Sponsored By

Although cyber threats have grown, there has been limited progress on cybersecurity for national defense and the incoming Obama administration should place the "highest priority" on accelerating and strengthening cybersecurity efforts, said the report, titled "Defense Imperatives for the New Administration," which was published on the Web on Nov. 4.

The 72-page report provides an overview of urgent goals that include the need to maintain capabilities for nuclear power and deterrence, project conventional forces around the world, fight terrorism, and provide support for domestic response and recovery, among others.

The study also recommended an immediate overhaul of the Defense Department's acquisition and business practices to enforce budget discipline and strengthen supply chain security. This includes reforming DOD's acquisition governance.

Although there has been a growing recognition of cyber vulnerabilities, and perimeter system and network defenses have been established, there is "scant real progress" in addressing the scope of the cyber threat, the report said.

Among the immediate actions recommended for improving DOD's cyber posture:

- More aggressive auditing of military information networks.
- Veiled acquisition terms for critical military software to avoid giving information to cyber adversaries.
- More frequent upgrades of military software and hardware elements of critical systems;
- More effective surveillance of military networks to identify data exfiltrations,
- Detailed back-up plans for managing joint forces operations following data or system failures or corruptions;
- Detailed plans for reconstituting networks using an alternative system, following a network failure.
- Encrypting all data stored on mobile devices.

- Minimizing the time to introduce new software and hardware, so cyber adversaries will be less prepared to make successful attacks.
- Removing unnecessary functionality from systems and networks,
- Using government-produced elements in every critical system to complicate attack planning by cyber adversaries.



© 1996-2008 1105 Media, Inc. All Rights Reserved.