Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 9 references coded [ 2.15% Coverage]

Reference 1 - 0.21% Coverage

The U.S. military’s ability to use cyberspace for rapid communication and   
information sharing in support of operations is a critical enabler of DoD missions.

Reference 2 - 0.24% Coverage

Manage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and creating secure and resilient network environments

Reference 3 - 0.46% Coverage

Co-location and dual-hatting of these separate and distinct   
Given its need to ensure the ability to operate Department of Defense Strategy for Operating in Cyberspace 5   
organizations allow DoD, and the U.S. government, to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD’s mission.

Reference 4 - 0.35% Coverage

DoD will fully integrate a complete spectrum of cyberspace scenarios into exercises and training to prepare U.S. Armed Forces for a wide variety of contingencies. A cornerstone of this activity will be the inclusion of cyber red teams throughout war games and exercises.

Reference 5 - 0.14% Coverage

Strategic Initiative 2: DoD will employ new defense operating concepts to protect DoD networks and systems.   
~

Reference 6 - 0.19% Coverage

The implementation of constantly evolving defense operating concepts is required to achieve DoD’s cyberspace mission today and in the future.

Reference 7 - 0.12% Coverage

Fourth, DoD is   
developing new defense operating concepts and computing architectures.

Reference 8 - 0.21% Coverage

DoD will strengthen and go beyond the current information assurance paradigm, including the exploration of new operating concepts to reduce vulnerabilities.

Reference 9 - 0.23% Coverage

To foster resiliency and smart diversity in its networks and systems, DoD will explore new and innovative approaches and paradigms for both existing and emerging challenges.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 5 references coded [ 0.92% Coverage]

Reference 1 - 0.17% Coverage

Combatant Commanders shall conduct prudent planning and be prepared to eliminate sources of WMD, providing the President with an array of options for military action when and where necessary.

Reference 2 - 0.10% Coverage

Cyberspace – Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains

Reference 3 - 0.12% Coverage

maintains a sustainable tempo to effectively mitigate operational, institutional, force management, and future challenges risk.

Reference 4 - 0.23% Coverage

Joint Forces must become more expeditionary in nature and will require a smaller logistical footprint in part by reducing large fuel and energy demands. Additionally, Joint Forces must train and exercise in degraded air, sea, cyber, and space environments.

Reference 5 - 0.31% Coverage

Cyberspace – Joint Forces will secure the ‘.mil’ domain, requiring a resilient DoD cyberspace architecture that employs a combination of detection, deterrence, denial, and multi-layered defense. We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with less cost and lower collateral impact.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 5 references coded [ 0.06% Coverage]

Reference 1 - 0.02% Coverage

Increase counterinsurgency, stability operations, and counterterrorism competency and capacity in general purpose forces;

Reference 2 - 0.01% Coverage

Exploit advantages in subsurface operations;

Reference 3 - 0.01% Coverage

Develop a more comprehensive approach to DoD operations in cyberspace;

Reference 4 - 0.01% Coverage

Centralize command of cyber operations; and

Reference 5 - 0.01% Coverage

U.S. ground forces will remain capable of full-spectrum operations,