Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 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,

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 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\\CS1\_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\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 1 reference coded [ 0.13% Coverage]

Reference 1 - 0.13% Coverage

Future conflicts could range from hybrid contingencies against proxy groups using asymmetric approaches, to a high-end conflict against a state power armed with WMD or technologically advanced anti-access and area-denial (A2/AD) capabilities. Reflecting this diverse range of challenges, the U.S. military will shift focus in terms of what kinds of conflicts it prepares for in the future, moving toward greater emphasis on the full spectrum of possible operations.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 27 references coded [ 4.01% Coverage]

Reference 1 - 0.02% Coverage

conduct cyberspace operations.

Reference 2 - 0.24% Coverage

This new strategy sets prioritized strategic goals and objectives for DoD’s cyber activities and missions to achieve over the next five years. It focuses on building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans.

Reference 3 - 0.11% Coverage

In addition to sharing information, DoD partners with other agencies of the U.S. government to synchronize operations and to share lessons-learned and cybersecurity bestpractices.

Reference 4 - 0.07% Coverage

The Defense Department engages in a broad array of activities to improve cybersecurity and cyber operations capacity abroad.

Reference 5 - 0.20% Coverage

The President has established principles and processes for governing cyber operations. The purpose of these principles and processes is to plan, develop, and use U.S. capabilities effectively, and to ensure that cyber operations occur in a manner consistent with the values that the United States promotes domestically and internationally.

Reference 6 - 0.10% Coverage

Third, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans.

Reference 7 - 0.18% Coverage

There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary’s militaryrelated networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations.

Reference 8 - 0.12% Coverage

Combat Mission Forces and their associated support teams will support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations.

Reference 9 - 0.18% Coverage

DoD will focus on ensuring that its forces are trained and ready to operate using the capabilities and architectures they need to conduct cyber operations, continue to build policy and legal frameworks to govern CMF employment, and integrate the CMF into DoD’s overall planning and force development.

Reference 10 - 0.12% Coverage

To defend the nation, DoD must build partnerships with other agencies of the government to prepare to conduct combined cyber operations to deter and if necessary defeat aggression in cyberspace.

Reference 11 - 0.07% Coverage

The Defense Department is focused on building the capabilities, processes, and plans necessary to succeed in this mission.

Reference 12 - 0.10% Coverage

STRATEGIC GOAL IV: BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES.

Reference 13 - 0.10% Coverage

To ensure unity of effort, DoD will enable combatant commands to plan and synchronize cyber operations with kinetic operations across all domains of military operations.

Reference 14 - 0.08% Coverage

This Unified Platform will enable the CMF to conduct full-spectrum cyberspace operations in support of national requirements.

Reference 15 - 0.30% Coverage

Validate and continually refine an adaptive command and control mechanism for cyber operations. DoD has made significant progress in recent years in developing command and control for all three of its missions, but its command and control model must be finalized, resourced, and tested to ensure effectiveness. The command and control model must support USCYBERCOM and the combatant commands. It must be efficient and practical, and must promote unity of effort of effort across all three cyber missions.

Reference 16 - 0.20% Coverage

The Defense Department will assess its cyber defense forces’ ability to conduct integrated, adaptive, and dynamic defensive operations. Enterprise-level and Cyber Protection Team (CPT) network defenders must be able to discover, detect, analyze, and mitigate threats and vulnerabilities to defend the DoD information network.

Reference 17 - 0.27% Coverage

Build and exercise continuity plans. All DoD components will identify and build resiliency plans to maintain continuity of their most critical operations in the event of network disruption and degradation. Military campaign plans must fully incorporate the ability to operate in a degraded cyber environment; military forces must exercise and be able to conduct military campaigns in a degraded cyber environment where access to networks and data is uncertain.

Reference 18 - 0.22% Coverage

Exercise to provide Defense Support of Civil Authorities. Under its existing and planned force structure, DoD will develop a framework and exercise its Defense Support of Civil Authorities (DSCA) capabilities in support of DHS and other agencies and with state and local authorities to help defend the federal government and the private sector in an emergency if directed.

Reference 19 - 0.10% Coverage

To operate effectively in cyberspace DoD requires cyber intelligence and warning and shared situational awareness through all phases of a potential operation.

Reference 20 - 0.19% Coverage

Develop and exercise capabilities to defend the nation. The National Mission Force and other relevant DoD components will train and partner with key interagency organizations   
24   
Th e De pa r tme n t o f De f e n s e Cy be r S t r a t e g y   
to prepare to conduct cyber operations to defend the nation from cyberattacks of significant consequence.

Reference 21 - 0.10% Coverage

STRATEGIC GOAL IV: BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES.

Reference 22 - 0.20% Coverage

Integrate cyber options into plans. To meet strategic end-states as defined by the Guidance for the Employment of the Force, combatant command plans, and other strategic guidance documents, DoD will work with agencies of the U.S. government as well as U.S. allies and partners to integrate cyber options into combatant command planning.

Reference 23 - 0.31% Coverage

Accelerate the integration of cyber requirements into plans. The Defense Department will accelerate the integration of cyber requirements into combatant command plans. Plans must outline and define specific cyberspace effects against targets. To facilitate this work, the Joint Staff will work with USSTRATCOM to synchronize and integrate requirements into planning and provide recommendations to the Chairman of the Joint Chiefs of Staff on the alignment, allocation, assignment, and apportionment of Cyber Mission Forces.

Reference 24 - 0.05% Coverage

Work with capable international partners to plan and train for cyber operations.

Reference 25 - 0.15% Coverage

This effort will help translate national and departmental guidance and policy into tactical operations. It is essential to clarifying conflicts in existing documentation that currently complicate cyber operations and cybersecurity governance.

Reference 26 - 0.16% Coverage

Since developing its first cyber strategy in 2011, the Defense Department has made significant progress in building its cyber capabilities, developing its organizations and plans, and fostering the partnerships necessary to defend the country and its interests.

Reference 27 - 0.08% Coverage

We must anticipate emerging threats, identify new capabilities to build, and determine how to enhance our partnerships and planning.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 7 references coded [ 1.13% Coverage]

Reference 1 - 0.10% Coverage

This integrated strategy requires us to conduct synchronized operations around the globe

Reference 2 - 0.11% Coverage

These NMOs support the force planning guidance prescribed in the 2014 Quadrennial   
Defense Review.

Reference 3 - 0.17% Coverage

Timely interagency planning and coordination also will be leveraged to develop holistic options that serve to integrate all elements of national power.

Reference 4 - 0.54% Coverage

As detailed in the “Capstone Concept for Joint Operations: Joint Force 2020,” globally integrated operations emphasize eight key components: employing mission command; seizing, retaining, and exploiting the initiative; leveraging global agility; partnering; demonstrating flexibility in establishing joint forces; improving crossdomain synergy; using flexible, low-signature capabilities; and being increasingly discriminate to minimize unintended consequences.

Reference 5 - 0.05% Coverage

execute globally   
integrated operations

Reference 6 - 0.12% Coverage

We are revising operational plans to be more flexible, creative, and integrated across Combatant Commands.

Reference 7 - 0.03% Coverage

improving campaign planning

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 1 reference coded [ 0.13% Coverage]

Reference 1 - 0.13% Coverage

Finally, Federal departments and agencies are also making cybersecurity an increasingly prominent component of their continuity of operations planning.