Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 5 references coded [ 0.10% Coverage]

Reference 1 - 0.06% Coverage

Rebalancing the Force In order to successfully protect and advance U.S. interests while balancing the priority objectives outlined above, the QDR makes a series of recommendations aimed at helping to rebalance America’s Armed Forces to better enable success in the following missions critical to protecting and advancing the nation’s interests.

Reference 2 - 0.01% Coverage

Increase the resiliency of U.S. forward posture and base infrastructure;

Reference 3 - 0.01% Coverage

Enhance the presence and responsiveness of U.S. forces abroad.

Reference 4 - 0.02% Coverage

Establish a Joint Task Force Elimination Headquarters to plan, train, and execute WMDelimination operations;

Reference 5 - 0.01% Coverage

10 space and cyberspace wings

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 5 references coded [ 2.26% Coverage]

Reference 1 - 0.22% Coverage

Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential.

Reference 2 - 0.32% Coverage

treating cyberspace as a domain is a critical organizing concept for DoD’s national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests.

Reference 3 - 0.53% Coverage

the Secretary of Defense has assigned cyberspace mission responsibilities to United States Strategic Command (USSTRATCOM), the other Combatant Commands, and the Military Departments.   
effectively in cyberspace and efficiently organize its resources, DoD established U.S. Cyber Command (USCYBERCOM) as a sub-unified command of USSTRATCOM. The establishment of USCYBERCOM reflects DoD’s need to

Reference 4 - 0.73% Coverage

USSTRATCOM has delegated to USCYBERCOM the responsibility for synchronizing and coordinating Service components within each branch of the military, including U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, the 24th Air Force, U.S. Marine Corps Forces Cyber Command, and U.S. Coast Guard Cyber Command. A key organizational concept behind the stand-up of USCYBERCOM is its co-location with the National Security Agency (NSA). Additionally, the Director of the National Security Agency is dual-hatted as the Commander of USCYBERCOM.

Reference 5 - 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.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 2 references coded [ 0.41% Coverage]

Reference 1 - 0.15% Coverage

The QDR also defined the main elements of U.S. force structure and provided a construct for sizing and shaping the Joint Force to accomplish the Nation’s defense objectives.

Reference 2 - 0.26% Coverage

We will carefully review legacy personnel systems, particularly whether we have the appropriate balance between uniformed, civilian, and contract professionals, and active and reserve components. The emerging war-fighting domain of cyberspace requires special attention in this regard.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 14 references coded [ 0.83% Coverage]

Reference 1 - 0.03% Coverage

Doing so will require exceptional agility in how we shape, prepare, and posture the Joint Force.

Reference 2 - 0.06% Coverage

Given this dynamic environment, the 2014 Quadrennial Defense Review (QDR) is principally focused on preparing for the future by rebalancing our defense efforts in a period of increasing fiscal constraint.

Reference 3 - 0.05% Coverage

Second, the QDR describes how the Department is responsibly and realistically taking steps to rebalance major elements of the Joint Force given the changing environment.

Reference 4 - 0.06% Coverage

Third, the QDR demonstrates our intent to rebalance the Department itself as part of our effort to control internal cost growth that is threatening to erode our combat power in this period of fiscal austerity.

Reference 5 - 0.04% Coverage

our updated defense strategy requires that the Department rebalance the Joint Force in several key areas to prepare most effectively for the future.

Reference 6 - 0.01% Coverage

Rebalancing for a broad spectrum of conflict.

Reference 7 - 0.02% Coverage

Rebalancing capability, capacity, and readiness within the Joint Force.

Reference 8 - 0.04% Coverage

The force will become smaller in the next five years but will gradually become more modern as well, with readiness improving over time.

Reference 9 - 0.07% Coverage

Maintaining an Air Force with global power projection capabilities crucial for this updated defense strategy. We will modernize next-generation Air Force combat equipment – including fighters and bombers – particularly against advancing modern air defense systems.

Reference 10 - 0.08% Coverage

Sustaining a world-class Army capable of conducting the full range of operations on land, including prompt and sustained land combat as part of large, multi-phase joint and multinational operations by maintaining a force structure that we can man, train, equip, and keep ready.

Reference 11 - 0.10% Coverage

Preserving Naval capacity to build security globally and respond to crises. Through an aggressive effort to reduce acquisition costs and temporary ship lay-ups, the Navy will modernize its fleets of surface ships, aircraft, and submarines to meet 21st century threats. We must ensure that the fleet is capable of operating in every region and across the full spectrum of conflict.

Reference 12 - 0.06% Coverage

Maintaining the role of the Marine Corps as a vital crisis response force, protecting its most important modernization priorities and ensuring readiness, but planning for an end strength of 182,000 active Marines.

Reference 13 - 0.15% Coverage

Rebalancing tooth and tail. Finally, the Department itself will rebalance internally to control cost growth and generate greater efficiencies in order to prioritize spending on combat power. The Department has previously submitted three packages of budget proposals aimed at achieving efficiencies and now plans to implement additional overhead reduction efforts. Key ongoing activities include reducing the Department’s major headquarters budgets by 20 percent and decreasing the number of direct reports to the Secretary of Defense.

Reference 14 - 0.06% Coverage

Recognizing current   
fiscal realities, the   
Department has made a number of decisions to ensure the Joint Force remains as balanced as possible over time, even as it must begin force structure reductions due to fiscal constraints.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 26 references coded [ 4.33% Coverage]

Reference 1 - 0.02% Coverage

Build and maintain ready forces

Reference 2 - 0.15% Coverage

This strategy builds on previous decisions regarding DoD’s Cyber Mission Force and cyber workforce development and provides new and specific guidance to mitigate anticipated risks and capture opportunities to strengthen U.S. national security.

Reference 3 - 0.13% Coverage

The U.S. military’s dependence on cyberspace for its operations led the Secretary of Defense in 2011 to declare cyberspace as an operational domain for purposes of organizing, training, and equipping U.S. military forces.

Reference 4 - 0.01% Coverage

A New Cyber Mission Force

Reference 5 - 0.10% Coverage

Among DoD’s cyber personnel and forces, the Cyber Mission Force (CMF) has a unique role within the Department. In 2012, DoD began to build a CMF to carry out DoD’s cyber missions.

Reference 6 - 0.10% Coverage

Once fully operational, the CMF will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components.

Reference 7 - 0.19% Coverage

The Cyber Mission Force represents a major investment by the Department of Defense and the United States as whole, and a central aim of this strategy is to set specific goals and objectives to guide the development of the Cyber Mission Force and DoD’s wider cyber workforce to protect and defend U.S. national interests.

Reference 8 - 0.37% Coverage

The Cyber Mission Force will be comprised of cyber operators organized into 133 teams, primarily aligned as follows: Cyber Protection Forces will augment traditional defensive measures and defend priority DoD networks and systems against priority threats; National Mission Forces and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence; and 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 - 0.19% Coverage

Combatant commands integrate Combat Mission Forces and Cyber Protection Teams into plans and operations and employ them in cyberspace, while the National Mission Force operates under the Commander of USCYBERCOM. Outside of this construct, teams can also be used to support other missions as required by the Department.

Reference 10 - 0.17% Coverage

In 2013 the Department began to integrate the CMF into the larger multi-mission U.S. military force to achieve synergy across domains, assure the CMF’s readiness within the force, and restructure the military and civilian workforce and infrastructure to execute DoD’s missions.

Reference 11 - 0.12% Coverage

During the course of implementing this strategy, DoD will continue to build the CMF, and will continue to mature the necessary command, control, and enabling organizations required for effective operations.

Reference 12 - 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 13 - 0.05% Coverage

Build and maintain ready forces and capabilities to conduct cyberspace operations

Reference 14 - 0.26% Coverage

As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.

Reference 15 - 0.06% Coverage

STRATEGIC GOAL I: BUILD AND MAINTAIN READY FORCES AND CAPABILITIES TO CONDUCT CYBERSPACE OPERATIONS.

Reference 16 - 0.19% Coverage

In 2013 DoD initiated a major investment in its cyber personnel and technologies by initiating the CMF; now DoD must make good on that investment by training its people, building effective organizations and command and control systems, and fully developing the capabilities that DoD requires to operate in cyberspace.

Reference 17 - 0.06% Coverage

STRATEGIC GOAL I: BUILD AND MAINTAIN READY FORCES AND CAPABILITIES TO CONDUCT CYBERSPACE OPERATIONS.

Reference 18 - 0.10% Coverage

Assess Cyber Mission Force capacity. Assess the capacity of the projected Cyber Mission Force to achieve its mission   
objectives when confronted with multiple contingencies.

Reference 19 - 0.18% Coverage

Assess and ensure the effectiveness of the Joint Force Headquarters for DoD information network (DoDIN) operations. Operating under USCYBERCOM, the Joint Force Headquarters-DoDIN will coordinate network defense and mitigate cyber risks to DoD operations and missions across the defense enterprise.

Reference 20 - 0.55% Coverage

Define and refine the National Guard’s   
Members of the Ohio National Guard Computer Network Defense Team conduct cyber defense operations during exercise Cyber Shield 2015 at Camp Atterbury, IN. (Ohio National Guard photo by Staff Sgt. George Davis)   
role in supporting law enforcement, Homeland Defense, and Defense Support of Civil Authorities missions. DoD will work with the National Guard to define the coordinate, train, advise, and assist (C/TAA) roles of the National Guard force and refine implementation through Cyber Guard 16-1. Under its existing and planned force structure,   
22   
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   
National Guard forces will exercise to coordinate, train, advise, and assist state and local agencies and domestic critical infrastructure and to provide support to law enforcement, Homeland Defense, and Defense Support of Civil Authorities activities in support of national objectives.

Reference 21 - 0.17% Coverage

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 22 - 0.13% Coverage

Under its existing and planned force structure, DoD will work with key allies and partners to build partner capacity and help secure the critical infrastructure and key resources on which DoD missions and U.S. interests depend.

Reference 23 - 0.10% Coverage

To achieve the goals and objectives outlined in this strategy will require hard choices regarding cyber forces and personnel, organizations, and capabilities.

Reference 24 - 0.14% Coverage

The 2014 NDAA also stipulated that this Principal Cyber Advisor integrate the cyber expertise and perspectives of key organizations to build an intradepartmental team of key players to ensure effective governance of cyber issues within DoD.

Reference 25 - 0.47% Coverage

In coordination with the Principal Cyber Advisor to the Secretary of Defense, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Office of the Director of Coast Assessment and Program Evaluation, USCYBERCOM will provide short- and long-term recommendations through the CIMB to provide to the Secretary of   
30   
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   
Defense regarding organizational structure, command and control mechanism, rules of engagement, personnel, capabilities, tools, and potential operational gaps. The goal of this posture assessment will be to provide a clear understanding of the future operational environment; key stakeholder views; as well as strategic priorities, choices, and resources for planning and operations.

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.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 1 reference coded [ 0.02% Coverage]

Reference 1 - 0.02% Coverage

Cyber Mission Force

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 2 references coded [ 0.44% Coverage]

Reference 1 - 0.23% Coverage

The U.S. Cyber Command, in conjunction with the Service Cyber Components, the National Security Agency, and the Defense Information Systems Agency, monitors the functioning of DOD networks and routinely provides threat and vulnerability information to the operators of those networks.

Reference 2 - 0.21% Coverage

To augment those efforts, the Administration has established the Cyber Threat Intelligence Integration Center (CTIIC) to “connect the dots” regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests.