Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 15 references coded [ 0.43% Coverage]

Reference 1 - 0.06% Coverage

The QDR directs a series of enhancements, including:  Improve the responsiveness and flexibility of consequence management response forces;  Enhance capabilities for domain awareness;  Accelerate the development of standoff radiological/nuclear detection capabilities; and  Enhance domestic capabilities to counter improvised explosive devices (IEDs).

Reference 2 - 0.04% Coverage

 Increase the availability of rotary-wing assets;  Expand manned and unmanned aircraft systems (UASs) for intelligence, surveillance, and reconnaissance (ISR);   
 Increase key enabling assets for special operations forces (SOF);

Reference 3 - 0.01% Coverage

Expand future long-range strike capabilities;

Reference 4 - 0.01% Coverage

Enhance the robustness of key ISR capabilities;

Reference 5 - 0.02% Coverage

Operate effectively in cyberspace: The security environment demands improved capabilities to counter threats in cyberspace.

Reference 6 - 0.01% Coverage

DoD is taking several steps to strengthen capabilities in cyberspace:

Reference 7 - 0.02% Coverage

continued focus   
on capabilities to conduct effective and sustained counterinsurgency, stability, and counterterrorist operations

Reference 8 - 0.01% Coverage

add capabilities and capacity

Reference 9 - 0.02% Coverage

U.S. air forces will become more survivable as large numbers of fifth-generation fighters join the force.

Reference 10 - 0.03% Coverage

The United States will continue to increase the capacity of its special operations forces and will enhance their capabilities through the growth of organic enablers and key support assets in the general purpose forces.

Reference 11 - 0.05% Coverage

 The capabilities, flexibility, and robustness of U.S. forces across the board will be improved by fielding more and better enabling systems, including ISR, electronic attack capabilities, communications networks, more resilient base infrastructure, and enhanced cyber defenses.

Reference 12 - 0.02% Coverage

The QDR report describes some of the tradeoffs that DoD’s leaders have identified to enable the rebalancing of U.S. military capabilities.

Reference 13 - 0.05% Coverage

Where it has not been possible to set in motion initiatives to meet certain future operational needs, the Secretary has identified vectors for the evolution of the force, calling on DoD components to devote sustained efforts toward developing new concepts and capabilities to address those needs

Reference 14 - 0.02% Coverage

providing context and recommendations regarding capability development and investment portfolios

Reference 15 - 0.07% Coverage

Taking into account the demands of a dynamic and complex security environment, the requirements of U.S. defense strategy, the need for enhancements to key capabilities across a wide range of missions, and the need for forces with sufficient aggregate capacity to meet the criteria laid out above, DoD has determined that U.S. forces, for the duration of the FY 2011–15 Future Years Defense Program (FYDP), will conform to the general parameters outlined below.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 18 references coded [ 4.37% Coverage]

Reference 1 - 0.26% Coverage

The quality of the United States’ human capital and knowledge base in both the public and private sectors provides DoD with a strong foundation on which to build current and future cyber capabilities.

Reference 2 - 0.24% Coverage

As directed by the National Security Strategy, DoD must ensure that it has the necessary capabilities to operate effectively in all domains- air, land, maritime, space, and cyberspace

Reference 3 - 0.31% Coverage

Ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most

Reference 4 - 0.15% Coverage

Third, DoD will employ an active cyber defense capability to prevent intrusions onto DoD networks and systems.

Reference 5 - 0.33% Coverage

Therefore, DoD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to share ideas, develop new capabilities, and support collective efforts to meet the crosscutting challenges of cyberspace.

Reference 6 - 0.25% Coverage

Technological innovation is at the forefront of national security, and DoD will foster rapid innovation and enhance its acquisition processes to ensure effective cyberspace operations.

Reference 7 - 0.21% Coverage

DoD will invest in its people, technology, and research and development to create and sustain the cyberspace capabilities that are vital to national security.

Reference 8 - 0.25% Coverage

To replicate the dynamism of the private sector and harness the power of emerging computing concepts, DoD’s acquisition processes for information technology will adopt five principles.

Reference 9 - 0.25% Coverage

DoD’s acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years

Reference 10 - 0.15% Coverage

DoD will employ incremental development and testing rather than a single deployment of large, complex systems.

Reference 11 - 0.14% Coverage

DoD will be willing to sacrifice or defer some customization to achieve speedy incremental improvements.

Reference 12 - 0.31% Coverage

DoD’s information technology needs—from modernizing nuclear command and control systems to updating word-processing software—will adopt differing levels of oversight based on the Department’s prioritization of critical systems.

Reference 13 - 0.15% Coverage

DoD will take a security in depth approach to design, acquisition, and implementation of trustworthy systems.

Reference 14 - 0.37% Coverage

DoD will explore game changing approaches, including new architectures, to strengthen DoD’s defense capabilities and make DoD systems more resistant to malicious activity.   
DoD will   
pursue revolutionary technologies that rethink the technological foundations of cyberspace.

Reference 15 - 0.23% Coverage

DoD will partner with leading scientific institutions to develop new, safe, and secure cyberspace capabilities that are significantly more resistant to malicious activity.

Reference 16 - 0.35% Coverage

The development of the National Cyber Range will enable the success of these and other efforts, allowing DoD, other U.S. government entities, and potentially non-U.S. government partners to test and evaluate new cyberspace concepts, policies, and technologies.

Reference 17 - 0.27% Coverage

DoD will continue to develop robust cyberspace capabilities, and the Department will support interagency efforts to actively engage public and private institutions to encourage cybersecurity innovation.

Reference 18 - 0.17% Coverage

DoD will invest in future personnel and capabilities to achieve its cyberspace objectives and support U.S. national security.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 4 references coded [ 0.38% Coverage]

Reference 1 - 0.09% Coverage

We must grow capabilities that enable operations when a common domain is unusable or inaccessible.

Reference 2 - 0.04% Coverage

sustains and develops the right capabilities,

Reference 3 - 0.13% Coverage

We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with less cost and lower collateral impact.

Reference 4 - 0.12% Coverage

Long-term modernization efforts will improve readiness by developing essential capabilities and capacity to outpace emerging threats.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 11 references coded [ 0.82% Coverage]

Reference 1 - 0.05% Coverage

The President’s Budget provides the resources to build and sustain the capabilities to conduct these operations, although at increased levels of risk for some missions.

Reference 2 - 0.07% Coverage

The Department is taking steps to ensure that progress continues in areas most critical to meeting future challenges such as full-spectrum cyberspace capabilities and where the potential for game-changing breakthroughs appears most promising.

Reference 3 - 0.02% Coverage

while making sure that our military capabilities evolve to meet new threats.

Reference 4 - 0.08% Coverage

Cyber. We will invest in new and expanded cyber capabilities and forces to enhance our ability to conduct cyberspace operations and support military operations worldwide, to support Combatant Commanders as they plan and execute military missions, and to counter cyberattacks against the United States.

Reference 5 - 0.11% Coverage

Missile Defense. We are increasing the number of Ground-Based Interceptors and deploying a second radar in Japan to provide early warning and tracking. We will make targeted investments in defensive interceptors, discrimination capabilities, and sensors; and we are studying the best location for an additional missile defense interceptor site in the United States if additional interceptors are needed.

Reference 6 - 0.07% Coverage

Nuclear Deterrence. We will continue to invest in modernizing our essential nuclear delivery systems; warning, command and control; and, in collaboration with the Department of Energy, nuclear weapons and supporting infrastructure.

Reference 7 - 0.07% Coverage

Space. We will move toward less complex, more affordable, more resilient systems and system architectures and pursue a multi-layered approach to deter attacks on space systems while retaining the capabilities to respond should deterrence fail.

Reference 8 - 0.07% Coverage

Air/Sea. We will continue to invest in combat aircraft, including fighters and long-range strike, survivable persistent surveillance, resilient architectures, and undersea warfare to increase the Joint Force’s ability to counter A2/AD challenges.

Reference 9 - 0.08% Coverage

Precision Strike. We will procure advanced air-to-surface missiles that will allow fighters and bombers to engage a wide range of targets and a long-range anti-ship cruise missile that will improve the joint ability of U.S. air forces to engage surface combatants in defended airspace.

Reference 10 - 0.10% Coverage

Intelligence, Surveillance, and Reconnaissance (ISR). We will rebalance investments toward systems that are operationally responsive and effective in highly contested environments, while sustaining capabilities appropriate for more permissive environments in order to support global situational awareness, counterterrorism, and other operations.

Reference 11 - 0.10% Coverage

Counter Terror and Special Operations. We will grow overall Special Operations Forces end strength to 69,700 personnel, protecting our ability to sustain persistent, networked, distributed operations to defeat al Qa’ida, counter other emerging transnational threats, counter WMD, build the capacity of our partners, and support conventional operations.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 42 references coded [ 6.44% Coverage]

Reference 1 - 0.01% Coverage

capabilities

Reference 2 - 0.19% Coverage

To this end the Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.

Reference 3 - 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 4 - 0.09% Coverage

DoD helps U.S. allies and partners to understand the cyber threats they face and to build the cyber capabilities necessary to defend their networks and data.

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 - 0.18% 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 7 - 0.05% Coverage

Build and maintain ready forces and capabilities to conduct cyberspace operations

Reference 8 - 0.14% Coverage

Although DoD has prioritized the allocation of resources in its budget to develop cyber capabilities, continued fiscal uncertainty requires that DoD plan to build its cyber capabilities under a declining overall defense budget.

Reference 9 - 0.08% Coverage

DoD must continue to prioritize its cyber investments and develop the capabilities required to defend U.S. interests at home and overseas.

Reference 10 - 0.16% Coverage

Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors’ behavior.

Reference 11 - 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 12 - 0.10% Coverage

The Defense Department will support the Justice Department and other agencies in exploring new tools and capabilities to help deter such activity in cyberspace.

Reference 13 - 0.06% Coverage

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

Reference 14 - 0.11% Coverage

To operate effectively in cyberspace, DoD requires forces and personnel that are trained to the highest standard, ready, and equipped with best-in-class technical capabilities.

Reference 15 - 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 16 - 0.14% Coverage

DoD must raise the bar on technology and innovation to stay ahead of the threat by enhancing its cyber defense capabilities, including by building and employing a more defendable network architecture in the Joint Information Environment (JIE).

Reference 17 - 0.07% Coverage

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

Reference 18 - 0.09% Coverage

DoD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property.

Reference 19 - 0.06% Coverage

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

Reference 20 - 0.08% Coverage

assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks.

Reference 21 - 0.19% Coverage

Build technical capabilities for cyber operations. In 2013, DoD developed a model for achieving CMF readiness and for developing viable cyber military options to present to the President and Secretary of Defense. DoD must have the technical tools available to conduct operations in support of combatant command missions.

Reference 22 - 0.21% Coverage

Develop the Unified Platform. On the basis of planning requirements, DoD will develop the detailed requirements for integrating disparate cyber platforms and building an interoperable and extendable network of cyber capabilities. This Unified Platform will enable the CMF to conduct full-spectrum cyberspace operations in support of national requirements.

Reference 23 - 0.39% Coverage

Accelerate research and development. The Defense Department will continue to accelerate innovative cyber research and development to build cyber capabilities. The   
18   
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   
DoD research and development community as well as established and emerging private sector partners can provide DoD and the nation with a significant advantage in developing leap-ahead technologies to defend U.S. interests in cyberspace. In addition to supporting current and planned investments, DoD will focus its basic and applied research agenda on developing cyber capabilities to expand the capacity of the CMF and the broader DoD cyber workforce.

Reference 24 - 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 25 - 0.18% Coverage

Establish an enterprise-wide cyber modeling and simulation capability. DoD will work in collaboration with the intelligence community to develop the data schema, databases, algorithms, and modeling and simulation (M&S) capabilities necessary to assess the effectiveness of cyber operations.

Reference 26 - 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 27 - 0.36% Coverage

The Joint Staff, with support from USCYBERCOM and other DoD components, will propose, collect, analyze, and report a set of appropriate metrics to the Principal Cyber Advisor to measure the operational capacity of the CMF. These metrics will include updates on the status of USCYBERCOM contingency capabilities, to include capability development and proficiency as well as accesses and tools that may be required in a contingency. In response to this analysis, DoD will develop a plan for ensuring that the CMF has the appropriate capacity and flexibility available to respond to changes in the strategic environment.

Reference 28 - 0.34% Coverage

Build the Joint Information Environment (JIE) single security architecture. The Defense Department will build DoD information networks to meet the JIE’s single security   
19   
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   
architecture. The single security architecture will adapt and evolve to mitigate cyber threats; it will help DoD to develop and follow best-in-class cybersecurity practices, and its small network footprint will allow USCYBERCOM, combatant commands, and DoD components to maintain comprehensive situational awareness of network threats and mitigations.

Reference 29 - 0.24% Coverage

The JIE’s single security architecture will enable a robust network defense and shift the focus from protecting service-specific networks and systems to securing the DoD enterprise in a unified manner. The JIE’s single security architecture must be developed with enhanced cyber situational awareness, deployed in response to validated requirements, and able to accommodate future defensive measures.

Reference 30 - 0.17% Coverage

As a part of JIE planning DoD will develop a framework for developing and integrating new defensive techniques into DoD’s cybersecurity architecture, to include anomalybased detection capabilities, data analytics to identify vulnerabilities and threats, and advanced encryption methods.

Reference 31 - 0.10% Coverage

Mitigate known vulnerabilities. The Defense Department will implement a capability to mitigate all known vulnerabilities that present a high risk to DoD networks and data.

Reference 32 - 0.16% Coverage

The DoD Chief Information Officer (CIO) will lead an effort to implement an automated patch management capability to distribute software and configuration patches, updates, and fixes to mitigate known, major vulnerabilities on DoD networks and systems against threats.

Reference 33 - 0.08% Coverage

To safeguard critical programs and technologies DoD will work with companies to develop alert capabilities and build layered cyber defenses.

Reference 34 - 0.26% Coverage

Use DoD counterintelligence capabilities to defend against intrusions. The Military Departments and the Under Secretary of Defense for Intelligence, in consultation with the Principal Cyber Advisor, will develop a strategy for the Secretary of Defense’s approval that maximizes the capabilities and authorities of the military departments’ counterintelligence agencies to identify, attribute, and defend against cyber intruders.

Reference 35 - 0.22% Coverage

Continue to develop intelligence and warning capabilities to anticipate threats. To defend the nation against cyberattacks of significant consequence, DoD will work with the broader intelligence community to develop intelligence capabilities about adversary activities and prepare to disrupt cyberattacks before they can impact the U.S. homeland and U.S. interests.

Reference 36 - 0.03% Coverage

Develop and exercise capabilities to defend the nation.

Reference 37 - 0.05% Coverage

Conduct an annual comprehensive review of DoD’s defend the nation capabilities.

Reference 38 - 0.12% Coverage

Throughout the course of this strategy, DoD will strengthen its international alliances and partnerships to develop combined capabilities to achieve cyber effects in support of combatant command plans.

Reference 39 - 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 40 - 0.09% Coverage

Conduct an end-to-end assessment of DoD’s cyber capabilities. U.S. Cyber Command will lead a comprehensive operational assessment of its posture.

Reference 41 - 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 42 - 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 - § 5 references coded [ 0.59% Coverage]

Reference 1 - 0.16% Coverage

sustain the capabilities, capacity, and readiness required to prevail in conflicts that may differ significantly in scope, scale, and duration.

Reference 2 - 0.06% Coverage

develop partner capabilities for self-defense,

Reference 3 - 0.06% Coverage

Developing flexible, interoperable capabilities

Reference 4 - 0.11% Coverage

We are in the process of defining the next set   
of interoperability standards for future capabilities.

Reference 5 - 0.20% Coverage

As we develop new capabilities to counter threats along the continuum of conflict, we   
also must procure sufficient capacity and readiness to sustain our global responsibilities.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 3 references coded [ 0.25% Coverage]

Reference 1 - 0.11% Coverage

We will protect our investment in foundational capabilities like the nuclear deterrent, and we will grow our investment in crucial capabilities like cyber; space; and intelligence, surveillance, and reconnaissance.

Reference 2 - 0.06% Coverage

We will safeguard our science and technology base to keep our edge in the capabilities needed to prevail against any adversary.

Reference 3 - 0.08% Coverage

Therefore, we will continue to promote rules for responsible behavior while making sure we have the capabilities to assure access to these shared spaces.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 11 references coded [ 1.57% Coverage]

Reference 1 - 0.05% Coverage

Building Capabilities to Defend the Nation in Cyberspace

Reference 2 - 0.07% Coverage

Bolstering “Whole-of-Government” and “Whole of Nation” Response Capabilities

Reference 3 - 0.20% Coverage

In taking this approach, the Administration will continually refine current capabilities and develop new ones that will raise the costs and reduce the benefits of conducting malicious cyber activity against the United States and its interests.

Reference 4 - 0.24% Coverage

The Federal government continues to improve the security of its information and systems through broad implementation of cybersecurity capabilities and services designed to detect and prevent malicious cyber activities as well as manage internal networks and systems more effectively and securely.

Reference 5 - 0.19% Coverage

The United States is helping other countries develop these capabilities through U.S.-led training programs on subjects as varied as developing cyber-related legal frameworks and using computer forensics to investigate crimes.

Reference 6 - 0.05% Coverage

Building Capabilities to Defend the Nation in Cyberspace

Reference 7 - 0.15% Coverage

To support this operational requirement, the Department of Defense established U.S. Cyber Command in October 2010 to consolidate U.S. military cyber capabilities to meet cyber threats.

Reference 8 - 0.11% Coverage

Developing these capabilities does not mean the United States is militarizing cyberspace, any more than having a navy militarizes the oceans.

Reference 9 - 0.24% Coverage

Conducting research and development to reduce and ultimately eliminate adversaries’ asymmetric advantage over network defenders, to develop new capabilities to monitor and detect adversary activity, to pursue adversaries in cyberspace, and to counter adversary activity in a measurable way.

Reference 10 - 0.07% Coverage

Bolstering “Whole-of-Government” and “Whole of Nation” Response Capabilities

Reference 11 - 0.22% Coverage

A credible U.S. cyber deterrent will require sustained efforts by all elements of the government to pursuing policies and capabilities that improve network defenses, bolster the Nation’s cyber resiliency, and provide options for imposing costs on malicious cyber actors.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 1 reference coded [ 0.28% Coverage]

Reference 1 - 0.28% Coverage

Further, as recommended in the   
E.O. 13800 Report to the President on Federal IT Modernization,   
the Administration will support   
N AT I O N A L C Y BE R S T R AT E G Y   
adoption of consolidated acquisition strategies to improve cybersecurity and reduce overhead costs associated with using inconsistent contract provisions across the Federal Government.