Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 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\\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\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 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\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review CLEAN - § 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\\Primary Sources\_Policy\_Strategies\\2015 DOD Cyber Strategy CLEAN - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

capabilities

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 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\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 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\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 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.