Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 3 references coded [ 0.10% Coverage]

Reference 1 - 0.03% Coverage

Key steps include more effectively ensuring alignment of resources with our national security strategy

Reference 2 - 0.02% Coverage

We are pursuing these objectives with a strategy that has three core components.

Reference 3 - 0.05% Coverage

Our mutual interests must be underpinned by bilateral, multilateral, and global strategies that address underlying sources of insecurity and build new spheres of cooperation

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 4 references coded [ 2.47% Coverage]

Reference 1 - 0.95% Coverage

FIVE STRATEGIC INITIATIVES   
Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential   
Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems   
Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy   
Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity   
Strategic Initiative 5: Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation

Reference 2 - 0.22% Coverage

The Department of Defense Strategy for Operating in Cyberspace assesses these challenges and opportunities and sets a strategic approach for DoD’s cyber mission.

Reference 3 - 0.53% Coverage

The Department’s five strategic initiatives offer a roadmap for DoD to operate effectively in cyberspace, defend national interests, and achieve national security objectives. Each initiative is distinct, yet necessarily connected with the other four. Across the strategy, activities undertaken in one initiative will contribute to DoD’s strategic thinking and lead to new approaches in the others.

Reference 4 - 0.77% Coverage

By pursuing the activities in this strategy, DoD will capitalize on the opportunities afforded to the Department by cyberspace; defend DoD networks and systems against intrusions and malicious activity; support efforts to strengthen cybersecurity for interagency, international, and critical industry partners; and develop robust cyberspace capabilities and partnerships. This strategy will guide the Department’s defense of U.S. interests in cyberspace so that the United States and its allies and partners may continue to benefit from the innovations of the information age.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 1 reference coded [ 0.27% Coverage]

Reference 1 - 0.27% Coverage

The President’s FY2015 Budget provides a realistic alternative to sequester-level cuts, supporting the Department’s ability to achieve our updated defense strategy and beginning an efficient transition to a smaller force over time. Resumption of sequestration-level cuts would lead to more immediate and severe risks to the strategy. Ultimately, with sequestration-level cuts, by 2021 the Joint Force would be too small and too outdated to fully implement our defense strategy. As a global leader, the United States requires a robust national defense strategy to protect and advance its interests and to ensure the security of its allies and partners with a   
EXEC UTIV E SUMMA R Y XIV   
military and civilian workforce that can implement that strategy effectively. This can only be achieved by the strategic balance of reforms and reductions that the Department is presenting to Congress and will require Congress to partner with the Department of Defense in making politically difficult choices.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 3 references coded [ 0.53% Coverage]

Reference 1 - 0.15% Coverage

In the face of an escalating threat, the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests.

Reference 2 - 0.12% Coverage

To mitigate risks and defend U.S. interests in the current and future security environment, the Defense Department outlines five strategic goals and specific objectives for its activities and missions.

Reference 3 - 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.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 3 references coded [ 0.50% Coverage]

Reference 1 - 0.14% Coverage

This National Military Strategy describes how we will employ our military forces to   
protect and advance our national interests.

Reference 2 - 0.32% Coverage

This integrated strategy requires us to conduct synchronized operations around the globe, implement institutional reforms at home, and sustain the capabilities, capacity, and readiness required to prevail in conflicts that may differ significantly in scope, scale, and duration.

Reference 3 - 0.04% Coverage

An Integrated Military Strategy

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 1 reference coded [ 0.29% Coverage]

Reference 1 - 0.29% Coverage

The Administration seeks to shape the future of cybersecurity through a comprehensive plan and investment strategy to develop the tools, techniques, and national workforce necessary to continue to improve the resilience of U.S. computers, networks, and critical infrastructure and provide new technological options for deterring malicious cyber activities.