Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 2 references coded [ 0.07% Coverage]

Reference 1 - 0.02% Coverage

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

Reference 2 - 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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 DoD Cyber Strategy Summary - § 1 reference coded [ 0.55% Coverage]

Reference 1 - 0.55% Coverage

Our strategic approach is based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Defense Strategy Summary - § 1 reference coded [ 0.19% Coverage]

Reference 1 - 0.19% Coverage

This unclassified synopsis of the classified 2018 National Defense Strategy articulates our strategy to compete, deter, and win in this environment.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Military Strategy Description - § 1 reference coded [ 1.55% Coverage]

Reference 1 - 1.55% Coverage

As an overarching military strategic framework, this strategy implements the substantial body of policy and strategy direction provided in the 2017 National Security Strategy, the 2018 National Defense Strategy (NDS), the Defense Planning Guidance (DPG), and other documents.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 2 references coded [ 0.08% Coverage]

Reference 1 - 0.04% Coverage

The 2022 NDS advances a strategy focused on the PRC and on collaboration with our growing network of Allies and partners on common objectives.

Reference 2 - 0.04% Coverage

This strategy shifts focus and resources toward the Department’s highest priorities, which will inevitably affect risk profiles in other areas.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 1 reference coded [ 2.37% Coverage]

Reference 1 - 2.37% Coverage

The 2022 NMS is the Chairman of the Joint Chiefs of Staff’s (CJCS) strategic guidance that provides the logic and framework to achieve the 2022 National Defense Strategy (NDS) priorities and build the future Joint Force. This NMS offers guidance for every Active Duty, Reserve, National Guard, and civilian member to take bold and transformative action now to protect the security of the American people and defend the democratic ideals at the heart of the American way of life. This strategy is about the Joint Force obtaining lasting positions of relative advantage in peace and achieving decisive victory in war.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 6 references coded [ 0.32% Coverage]

Reference 1 - 0.01% Coverage

Overview of Our Strategic Approach

Reference 2 - 0.01% Coverage

OUR STRATEGY BY REGION

Reference 3 - 0.04% Coverage

This National Security Strategy lays out our plan to achieve a better future of a free, open, secure, and prosperous world.

Reference 4 - 0.02% Coverage

Implementing a Modern Industrial and Innovation Strategy

Reference 5 - 0.12% Coverage

Our strategy toward the PRC is threefold: 1) to invest in the foundations of our strength at home – our competitiveness, our innovation, our resilience, our democracy, 2) to align our efforts with our network of allies and partners, acting with common purpose and in common cause, and 3) compete responsibly with the PRC to defend our interests and build our vision for the future.1

Reference 6 - 0.13% Coverage

Continuing to implement our first-ever National Strategy for Countering Domestic Terrorism will enable us to better understand and share information regarding the domestic terrorist threat, prevent recruitment and mobilization to violence, and disrupt and deter domestic terrorist activity and any transnational linkages—all while reinforcing respect for civil rights and civil liberties.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 1 reference coded [ 0.36% Coverage]

Reference 1 - 0.36% Coverage

These operations will support the strategic approach outlined in the 2023 National Cybersecurity Strategy, in which the Department’s cyberspace operations may complement concurrent actions by the diplomatic, law enforcement, and intelligence communities, among others.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 7 references coded [ 0.71% Coverage]

Reference 1 - 0.10% Coverage

This strategy will position the United States and its allies and partners to build that digital ecosystem together, making it more easily and inherently defensible, resilient, and aligned with our values.

Reference 2 - 0.04% Coverage

This strategy seeks to build and enhance collaboration around five pillars

Reference 3 - 0.12% Coverage

The pillars organizing this strategy articulate a vision of shared purpose and priorities for these communities, highlight challenges they face in achieving this vision, and identify strategic objectives around which to organize their efforts.

Reference 4 - 0.09% Coverage

This Administration is committed to improving Federal cybersecurity through long-term efforts to implement a zero trust architecture strategy and modernize IT and OT infrastructure.

Reference 5 - 0.14% Coverage

Informed by lessons learned and the rapidly-evolving threat environment, DoD will develop an updated departmental cyber strategy aligned with the National Security Strategy,   
NAT I ONAL CY B E RS E CU RI T Y S T RATEGY 14   
        
National Defense Strategy, and this National Cybersecurity Strategy.

Reference 6 - 0.17% Coverage

United States and its foreign and private sector partners will implement a multi-pronged strategy to preserve technical excellence, protect our security, drive economic competitiveness, promote digital trade, and ensure that the “rules of the road” for technology standards favor principles of transparency, openness, consensus, relevance, and coherence.

Reference 7 - 0.07% Coverage

To address this challenge, ONCD will lead the development and oversee implementation of a National Cyber Workforce and Education Strategy.

**Annotations**

1 PRC strategy has elements of all theoretical paradigms, mixing both sets of LOEs (OBJs and National Interests): competitiveness, resilience, alliance and partnerships, mutual interest/common cause...Building a vision for the future has "World as It Ought to Be" undertones.