Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 2 references coded [ 0.02% Coverage]

Reference 1 - 0.02% Coverage

the Department’s prevent-and-deter activities will be focused on ensuring a defense in depth of the United States;

Reference 2 - 0.01% Coverage

DoD must actively defend its networks.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 1 reference coded [ 0.30% Coverage]

Reference 1 - 0.30% Coverage

Joint Forces will secure the ‘.mil’ domain, requiring a resilient DoD cyberspace architecture that employs a combination of detection, deterrence, denial, and multi-layered defense. We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with less cost and lower collateral impact.

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

response and recovery

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 4 references coded [ 0.72% Coverage]

Reference 1 - 0.26% Coverage

DoD conducts network defense operations on an ongoing basis to securely operate the Department of Defense Information Network (DoDIN). If and when DoD detects indications of hostile activity within its networks, DoD has quick-response capabilities to close or mitigate vulnerabilities and secure its networks and systems. Network defense operations on DoD networks constitute the vast majority of DoD’s operations in cyberspace.

Reference 2 - 0.19% Coverage

If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace. The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life.

Reference 3 - 0.18% Coverage

There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary’s militaryrelated networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations.

Reference 4 - 0.09% Coverage

Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 2 references coded [ 0.23% Coverage]

Reference 1 - 0.04% Coverage

could rapidly react to a cyber attack on the nation.

Reference 2 - 0.19% Coverage

These capabilities, matched with the expertise of the Intelligence Community and the Department of Defense, reflect a “whole-of-government” approach to identify, mitigate, and defend against cyber incidents and national-level events

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 1 reference coded [ 0.03% Coverage]

Reference 1 - 0.03% Coverage

U.S. eﬀ orts to counter the exploitation of information by rivals have been tepid and fragmented.