Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 2 references coded [ 1.39% Coverage]

Reference 1 - 0.33% Coverage

DoD seeks to foster a stronger culture of information assurance within its workforce to assure individual responsibility and deter malicious insiders by shaping behaviors and attitudes through the imposition of higher costs for malicious activity.

Reference 2 - 1.06% Coverage

As malicious cyber activity continues to grow, DoD has employed active cyber defense to prevent intrusions and defeat adversary activities on DoD networks and systems. Active cyber defense is DoD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems.   
As intrusions may not always be stopped at the network   
boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 1 reference coded [ 0.41% Coverage]

Reference 1 - 0.41% Coverage

We will support whole-of-nation deterrence approaches that blend economic, diplomatic, and military tools to influence adversary behavior. Denying an aggressor the benefits of achieving its objectives can be just as effective as in altering its strategic calculus through the threat of retaliation. The most effective deterrence approaches make use of both techniques, while also providing potential adversaries acceptable alternative courses of action.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 7 references coded [ 0.61% Coverage]

Reference 1 - 0.02% Coverage

Defense: Dissuading and Deterring

Reference 2 - 0.11% Coverage

We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options~

Reference 3 - 0.06% Coverage

eserving the right to defend these vital national assets as necessary and appropriate~

Reference 4 - 0.10% Coverage

The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks~

Reference 5 - 0.16% Coverage

For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them~

Reference 6 - 0.10% Coverage

We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense

Reference 7 - 0.05% Coverage

we will exhaust all options before military force whenever we can

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 1 reference coded [ 0.05% Coverage]

Reference 1 - 0.05% Coverage

In the future, as our forces transition into a period of lessintensive sustained operations, the Department’s force planning assumes an ability to undertake a broader and deeper range of prevent-and-deter missions, acting wherever possible as part of a whole-of-government approach and in concert with allies and partners.