Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 2 references coded [ 0.72% Coverage]

Reference 1 - 0.15% Coverage

denial of access or service that affects the availability of networks, information, or network-enabled resources

Reference 2 - 0.57% Coverage

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.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 2 references coded [ 0.13% Coverage]

Reference 1 - 0.05% Coverage

Denying an aggressor the benefits of achieving its objectives

Reference 2 - 0.08% Coverage

employs a combination of detection, deterrence, denial, and multi-layered defense.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 2 references coded [ 0.11% Coverage]

Reference 1 - 0.02% Coverage

deny criminals safe havens,

Reference 2 - 0.09% Coverage

Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

U.S. capabilities to deny adversaries’ objectives