Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 2 references coded [ 0.83% Coverage]

Reference 1 - 0.60% Coverage

These efforts will be supported by the development of increasingly resilient networks and systems. In the case of a contingency involving network failure or significant compromise, DoD must be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations.

Reference 2 - 0.23% Coverage

To foster resiliency and smart diversity in its networks and systems, DoD will explore new and innovative approaches and paradigms for both existing and emerging challenges.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 3 references coded [ 0.31% Coverage]

Reference 1 - 0.08% Coverage

maintain joint assured access to the global commons and cyberspace should they become contested

Reference 2 - 0.14% Coverage

Joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint Force.

Reference 3 - 0.08% Coverage

Joint Forces will secure the ‘.mil’ domain, requiring a resilient DoD cyberspace architecture

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 4 references coded [ 0.13% Coverage]

Reference 1 - 0.03% Coverage

resilient to arbitrary or malicious disruption

Reference 2 - 0.03% Coverage

national and international network resilience

Reference 3 - 0.05% Coverage

Ensuring the resilience of our networks and information systems

Reference 4 - 0.02% Coverage

enhance overall resilience