Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 4 references coded [ 0.33% Coverage]

Reference 1 - 0.02% Coverage

r exploitation

Reference 2 - 0.11% Coverage

y foreign nations are working to exploit DoD unclassified and classified network

Reference 3 - 0.16% Coverage

The global scope of DoD networks and systems presents adversaries with broad opportunities for exploitation and attack.

Reference 4 - 0.04% Coverage

theft or exploitation of data

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 6 references coded [ 0.24% Coverage]

Reference 1 - 0.07% Coverage

We have also witnessed offline challenges, like exploitation and aggression, move into cyberspace~

Reference 2 - 0.02% Coverage

exploiting our networks

Reference 3 - 0.07% Coverage

Exploitation of these vulnerabilities impairs economic performance and national security

Reference 4 - 0.02% Coverage

exploit online systems,

Reference 5 - 0.05% Coverage

exploit the Internet for operational planning, financing, or attacks

Reference 6 - 0.01% Coverage

exploit our networks

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 DOD Cyber Strategy CLEAN - § 1 reference coded [ 0.10% Coverage]

Reference 1 - 0.10% Coverage

Without strong investments in cybersecurity and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 3 references coded [ 0.38% Coverage]

Reference 1 - 0.09% Coverage

Malicious actors employ various tactics for attacking, exploiting, or disrupting networks, systems, and data.

Reference 2 - 0.09% Coverage

Supply-chain operations seek to exploit access to products and services provided to the intended victim.

Reference 3 - 0.20% Coverage

Shared situational awareness of cyber threats and indicators of malicious cyber activity – including information on those responsible – provides network defenders the opportunity to close known vulnerabilities before they can be fully exploited.