Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 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\\CS1\_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\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 2 references coded [ 0.21% 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.

Reference 2 - 0.11% Coverage

In addition to zero-day vulnerabilities, one of the greatest threats to DoD networks and systems lies in known, high-risk vulnerabilities that potential adversaries can exploit.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 7 references coded [ 0.27% Coverage]

Reference 1 - 0.03% Coverage

Openness also imposes costs, since adversaries exploit our free and democratic system to harm the United States.

Reference 2 - 0.02% Coverage

They steal and exploit our intellectual property and personal data

Reference 3 - 0.06% Coverage

State and non-state actors place the safety of the American people and the Nation’s economic vitality at risk by exploiting vulnerabilities across the land, air, maritime, space, and cyberspace domains.

Reference 4 - 0.05% Coverage

China gathers and exploits data on an unrivaled scale and spreads features of its authoritarian system, including corruption and the use of surveillance.

Reference 5 - 0.05% Coverage

Adversaries studied the American way of war and began investing in capabilities that targeted our strengths and sought to exploit perceived weaknesses.

Reference 6 - 0.03% Coverage

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

Reference 7 - 0.03% Coverage

State and non-state actors project influence and advance their objectives by exploiting information

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 5 references coded [ 0.90% Coverage]

Reference 1 - 0.17% Coverage

Non-state actors terrorists and   
criminals — exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states.

Reference 2 - 0.09% Coverage

Most cybersecurity risks to critical infrastructure stem from the exploitation of known vulnerabilities.

Reference 3 - 0.10% Coverage

As these sectors have modernized,   
N AT I O N A L C Y BE R S T R AT E G Y   
they have also become more vulnerable to cyber exploitation or attack

Reference 4 - 0.38% Coverage

Given the criticality of maritime transportation to the United States and global economy and the minimal risk-reduction investments to protect against cyber exploitation made thus far, the United States will move quickly to clarify maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure.

Reference 5 - 0.16% Coverage

This includes promotion and use of coordinated vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack.