Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 3 references coded [ 0.02% Coverage]

Reference 1 - 0.02% Coverage

Other intrusions threaten to damage portions of our critical infrastructure

Reference 2 - 0.01% Coverage

threats

Reference 3 - 0.01% Coverage

threats

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 3 references coded [ 0.11% Coverage]

Reference 1 - 0.06% Coverage

there is no greater threat to the American people than weapons of mass destruction, particularly the danger posed by the pursuit of nuclear weapons by violent extremists and their proliferation to additional states.

Reference 2 - 0.05% Coverage

Defense: We are strengthening our military to ensure that it can prevail in today’s wars; to prevent and deter threats against the United States, its interests, and our allies and partners;

Reference 3 - 0.01% Coverage

Threats

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 3 references coded [ 0.64% Coverage]

Reference 1 - 0.16% Coverage

Cyber Threats   
“The very technologies that empower us to lead and create also empower those who would disrupt and destroy.”

Reference 2 - 0.33% Coverage

In developing its strategy for operating in cyberspace, DoD is focused on a number of central aspects of the cyber threat; these include external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD‘s operational ability.

Reference 3 - 0.15% Coverage

the rapidly evolving threat landscape presents a complex and vital challenge for national and economic security.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 4 references coded [ 0.42% Coverage]

Reference 1 - 0.04% Coverage

defend against and defeat threats to our homeland.

Reference 2 - 0.12% Coverage

potential adversaries who underestimate our continued military strength and will to protect our national interests do so at their peril.

Reference 3 - 0.02% Coverage

threat of retaliation

Reference 4 - 0.23% Coverage

To safeguard U.S. and partner nation interests, we will be prepared to demonstrate the will and commit the resources needed to oppose any nation’s actions that jeopardize access to and use of the global commons and cyberspace, or that threaten the security of our allies.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 18 references coded [ 0.52% Coverage]

Reference 1 - 0.03% Coverage

threaten users’ confidence in online commerce

Reference 2 - 0.05% Coverage

The theft of intellectual property threatens national competitiveness

Reference 3 - 0.11% Coverage

Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace~

Reference 4 - 0.01% Coverage

threats

Reference 5 - 0.01% Coverage

threats

Reference 6 - 0.01% Coverage

threats

Reference 7 - 0.09% Coverage

The United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies

Reference 8 - 0.01% Coverage

threaten

Reference 9 - 0.03% Coverage

hreaten our national and economic security,

Reference 10 - 0.07% Coverage

the United States will respond to hostile acts in cyberspace as we would to any other threat to our country~

Reference 11 - 0.01% Coverage

confront threats

Reference 12 - 0.01% Coverage

threaten

Reference 13 - 0.01% Coverage

threaten

Reference 14 - 0.01% Coverage

threatened,

Reference 15 - 0.03% Coverage

confront potential threats in cyberspace.

Reference 16 - 0.01% Coverage

Criminal threats

Reference 17 - 0.01% Coverage

threaten,

Reference 18 - 0.02% Coverage

address real cyberspace threats,

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 2 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

direct physical threat to the United States

Reference 2 - 0.01% Coverage

adversaries challenge our interests with the threat

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review CLEAN - § 1 reference coded [ 0.08% Coverage]

Reference 1 - 0.08% Coverage

Our ability to project forces to combat terrorism in places as far away as Yemen, Afghanistan, and Mali – and to build capacity to help partners counter terrorism and counter the proliferation of weapons of mass destruction (WMD) – reduces the likelihood that these threats could find their way to U.S. shores.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 DOD Cyber Strategy CLEAN - § 2 references coded [ 0.17% Coverage]

Reference 1 - 0.09% Coverage

Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability

Reference 2 - 0.09% Coverage

The attack further spurred an already ongoing national discussion about the nature of the cyber threat and the need for improved cybersecurity.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 2 references coded [ 0.28% Coverage]

Reference 1 - 0.16% Coverage

U.S. strategic forces are kept at the   
highest state of readiness, always prepared to respond to threats to the homeland and our vital interests.

Reference 2 - 0.12% Coverage

We are modernizing our nuclear enterprise and working to protect our Nation against asymmetric threats.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 6 references coded [ 0.47% Coverage]

Reference 1 - 0.05% Coverage

That is why I have worked to ensure that America has the capabilities we need to respond to threats abroad

Reference 2 - 0.02% Coverage

threats that are truly global.

Reference 3 - 0.02% Coverage

acting decisively to defeat direct threats

Reference 4 - 0.09% Coverage

In all cases, the decision to use force must reflect a clear mandate and feasible objectives, and we must ensure our actions are effective, just, and consistent with the rule of law.

Reference 5 - 0.21% Coverage

American diplomacy and leadership, backed by a strong military, remain essential to deterring future acts of inter-state aggression and provocation by reaffirming our security commitments to allies and partners, investing in their capabilities to withstand coercion, imposing costs on those who threaten their neighbors or violate fundamental international norms, and embedding our actions within wider regional strategies.

Reference 6 - 0.08% Coverage

As countries increasingly derive benefits from space, we must join together to deal with threats posed by those who may wish to deny the peaceful use of outer space.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 9 references coded [ 1.82% Coverage]

Reference 1 - 0.25% Coverage

cyber attacks and some kinds of malicious cyber activity2 – particularly those conducted by nation-states or highly capable non-state actors and which target critical infrastructures and key industries in the United States – can constitute a significant threat to U.S. national security and economic interests.

Reference 2 - 0.16% Coverage

The United States Government is pursuing multifaceted policy efforts to leverage all instruments of national power to counter malicious cyber activity that poses significant threats to the nation

Reference 3 - 0.33% Coverage

Although cyber attacks can have a range of direct and indirect effects that vary in their severity, U.S. deterrence efforts are particularly focused on those attacks that could result in loss of life, harm to U.S. critical infrastructure, significant damage to property, or significant threats to the national security, foreign policy, or economic health or financial stability of the United States or its interests

Reference 4 - 0.25% Coverage

Although the principal focus of the United States Government’s cyber deterrence efforts focus principally on significant threats to U.S. interests, the framework outlined in this report, including the “whole of government” approach, also serves to deter lesser threats, generally through non-military means.

Reference 5 - 0.06% Coverage

we will adapt our priorities to new threats and geopolitical developments.

Reference 6 - 0.21% Coverage

Cyber attacks or other malicious cyber activity that threatens the command and control of U.S. military forces, the freedom of maneuver of U.S. military forces, or the infrastructure on which the U.S. military relies to defend U.S. interests and commitments

Reference 7 - 0.20% Coverage

However, adversaries contemplating testing U.S. resolve should understand that the United States may, in circumstances where network defense and law enforcement measures are insufficient, use cyber operations to defend our nation and our interests.

Reference 8 - 0.20% Coverage

The United States Government may also send messages through diplomatic or other channels to foreign adversaries as a warning that the United States can attribute and will respond to malicious cyber activities as necessary to protect our interests.

Reference 9 - 0.15% Coverage

In more extreme scenarios, the United States may intensify this strategic   
15   
messaging and demonstrate our resolve through stronger measures, including sanctions or military posturing.