Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 1 reference coded [ 0.03% Coverage]

Reference 1 - 0.03% Coverage

make certain that regional adversaries gain no advantages from their acquisition of new, offensive military capabilities

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 DOD Cyber Strategy CLEAN - § 1 reference coded [ 0.06% Coverage]

Reference 1 - 0.06% Coverage

The North Korean attack on Sony was one of the most destructive cyberattacks on a U.S. entity to date.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 6 references coded [ 1.18% Coverage]

Reference 1 - 0.11% Coverage

North Korea also has conducted cyber attacks, including causing major damage to a U.S. corporation.

Reference 2 - 0.18% Coverage

attacks on our communications and sensing systems could occur with little to no warning, impacting our ability to assess, coordinate, communicate, and respond.

Reference 3 - 0.21% Coverage

Deterring a direct attack on the United States and our allies is a priority mission,   
requiring homeland and regional defenses tied to secure conventional and nuclear strike capabilities.

Reference 4 - 0.14% Coverage

Should any actor directly attack the United States or our interests, the U.S. military will   
take action to defend our Nation.

Reference 5 - 0.21% Coverage

In the event of an attack, the U.S. military will respond by inflicting damage of such magnitude as to compel the adversary to cease hostilities or render it incapable of further aggression.

Reference 6 - 0.33% Coverage

In the event of an attack against the United States or one of its   
allies, the U.S. military along with allies and partners will project power across multiple domains to decisively defeat the adversary by compelling it to cease hostilities or render its military incapable of further aggression.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 1 reference coded [ 0.06% Coverage]

Reference 1 - 0.06% Coverage

when capture or other actions to disrupt the threat are not feasible, we will not hesitate to take decisive action.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 41 references coded [ 2.65% Coverage]

Reference 1 - 0.26% Coverage

At the same time, 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 - 0.22% Coverage

For the purpose of this document, a cyber attack refers to an attempt to deny access to, disrupt, disable, degrade, destroy, or otherwise render inoperable computers, information or communications systems, networks, or physical or virtual systems controlled by computers.

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 - 0.01% Coverage

cyber attacks

Reference 5 - 0.09% Coverage

the Administration is most concerned about threats that could cause wide-scale disruption, destruction

Reference 6 - 0.06% Coverage

Cyber attacks or other malicious cyber activity intended to cause casualties

Reference 7 - 0.23% Coverage

Cyber attacks or other malicious cyber activity intended to cause significant disruption to the normal functioning of U.S. society or government, including attacks against critical infrastructure that could damage systems used to provide key services4 to the public or the government.

Reference 8 - 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 9 - 0.09% Coverage

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

Reference 10 - 0.12% Coverage

highly capable state and non-state adversaries that have the capability, expertise, and intent to conduct significant cyber attacks against us.

Reference 11 - 0.01% Coverage

cyber attack

Reference 12 - 0.01% Coverage

attacks

Reference 13 - 0.01% Coverage

cyber attacks

Reference 14 - 0.01% Coverage

cyber attacks

Reference 15 - 0.04% Coverage

conducting offensive and defensive cyber operations

Reference 16 - 0.01% Coverage

cyber attacks

Reference 17 - 0.07% Coverage

potential cascading effects from a cyber attack against their networks and systems.

Reference 18 - 0.03% Coverage

reconstitute rapidly if attacks succeed

Reference 19 - 0.02% Coverage

prepare for attacks

Reference 20 - 0.03% Coverage

defend the nation from cyber attacks.

Reference 21 - 0.01% Coverage

cyber attacks

Reference 22 - 0.01% Coverage

cyber attack

Reference 23 - 0.01% Coverage

cyber attacks

Reference 24 - 0.01% Coverage

attacks.

Reference 25 - 0.01% Coverage

attack)

Reference 26 - 0.02% Coverage

perpetrators of cyber attacks

Reference 27 - 0.03% Coverage

attacks on computers and networks

Reference 28 - 0.03% Coverage

respond to a cyber attack on the nation.

Reference 29 - 0.04% Coverage

could rapidly react to a cyber attack on the nation.

Reference 30 - 0.03% Coverage

defend the nation from cyber attacks

Reference 31 - 0.11% Coverage

Further, the Department of Defense is able, if directed, to conduct operations in cyberspace, including offensive cyber operations.

Reference 32 - 0.35% Coverage

Even though the United States Government is not limited to responding to a cyber attack through cyberspace, there are unique advantages to such a symmetrical response. Cyber operations can be narrowly tailored to target the precise system or systems that are perpetrating an attack against the United States. Further, the methods for neutralizing a malicious system can be sufficiently precise so as to minimize collateral effects.

Reference 33 - 0.02% Coverage

defend against cyber attacks

Reference 34 - 0.01% Coverage

cyber attacks

Reference 35 - 0.02% Coverage

destructive cyber attacks

Reference 36 - 0.01% Coverage

attacks

Reference 37 - 0.01% Coverage

cyber attacks

Reference 38 - 0.02% Coverage

crippling cyber attacks

Reference 39 - 0.02% Coverage

intentions to attack

Reference 40 - 0.01% Coverage

cyber attacks

Reference 41 - 0.01% Coverage

cyber attacks