Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 2 references coded [ 0.17% Coverage]

Reference 1 - 0.14% Coverage

Enhance Security at Home: Security at home relies on our shared efforts to prevent and deter attacks by identifying and interdicting threats, denying hostile actors the ability to operate within our borders, protecting the nation’s critical infrastructure and key resources, and securing cyberspace. That is why we are pursuing initiatives to protect and reduce vulnerabilities in critical infrastructure, at our borders, ports, and airports, and to enhance overall air, maritime, transportation, and space and cyber security.

Reference 2 - 0.03% Coverage

We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by:

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 1 reference coded [ 0.05% Coverage]

Reference 1 - 0.05% Coverage

In the future, as our forces transition into a period of lessintensive sustained operations, the Department’s force planning assumes an ability to undertake a broader and deeper range of prevent-and-deter missions, acting wherever possible as part of a whole-of-government approach and in concert with allies and partners.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 2 references coded [ 1.39% Coverage]

Reference 1 - 0.33% Coverage

DoD seeks to foster a stronger culture of information assurance within its workforce to assure individual responsibility and deter malicious insiders by shaping behaviors and attitudes through the imposition of higher costs for malicious activity.

Reference 2 - 1.06% Coverage

As malicious cyber activity continues to grow, DoD has employed active cyber defense to prevent intrusions and defeat adversary activities on DoD networks and systems. Active cyber defense is DoD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems.   
As intrusions may not always be stopped at the network   
boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 7 references coded [ 0.61% Coverage]

Reference 1 - 0.02% Coverage

Defense: Dissuading and Deterring

Reference 2 - 0.11% Coverage

We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options~

Reference 3 - 0.06% Coverage

eserving the right to defend these vital national assets as necessary and appropriate~

Reference 4 - 0.10% Coverage

The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks~

Reference 5 - 0.16% Coverage

For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them~

Reference 6 - 0.10% Coverage

We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense

Reference 7 - 0.05% Coverage

we will exhaust all options before military force whenever we can

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 1 reference coded [ 0.41% Coverage]

Reference 1 - 0.41% Coverage

We will support whole-of-nation deterrence approaches that blend economic, diplomatic, and military tools to influence adversary behavior. Denying an aggressor the benefits of achieving its objectives can be just as effective as in altering its strategic calculus through the threat of retaliation. The most effective deterrence approaches make use of both techniques, while also providing potential adversaries acceptable alternative courses of action.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 6 references coded [ 1.59% Coverage]

Reference 1 - 0.14% Coverage

As a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the U.S. homeland or U.S. interests before conducting a cyberspace operation.

Reference 2 - 0.44% Coverage

The United States government has a limited and specific role to play in defending the nation against cyberattacks of significant consequence. The private sector owns and operates over ninety percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense. One of the most important steps for improving the United States’ overall cybersecurity posture is for companies to prioritize the networks and data that they must protect and to invest in improving their own cybersecurity. While the U.S. government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves.

Reference 3 - 0.24% Coverage

the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary’s military systems to prevent the use of force against U.S. interests. United States Cyber Command (USCYBERCOM) may also be directed to conduct cyber operations, in coordination with other U.S. government agencies as appropriate, to deter or defeat strategic threats in other domains.

Reference 4 - 0.14% Coverage

To ensure that the Internet remains open, secure, and prosperous, the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property.

Reference 5 - 0.26% Coverage

As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.

Reference 6 - 0.37% Coverage

Response: The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. The United States has articulated this declaratory policy in the 2011 United States International Strategy for Cyberspace, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense. The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 1 reference coded [ 0.37% Coverage]

Reference 1 - 0.37% Coverage

Respond to Crisis and Conduct Limited Contingency Operations. Another form of   
power projection is teaming with partners to conduct limited contingency operations. Such operations may involve flowing additional U.S. forces and capabilities to a given region to strengthen deterrence, prevent escalation, and reassure allies.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 1 reference coded [ 0.10% Coverage]

Reference 1 - 0.10% Coverage

On cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 3 references coded [ 0.51% Coverage]

Reference 1 - 0.17% Coverage

Influence is achieved by credibly demonstrating the ability and willingness to deny benefits or impose costs to convince the adversary that restraint will result in better outcomes than will confrontation.

Reference 2 - 0.16% Coverage

The United States Government’s first preference is to use network defense, law enforcement measures, economic actions, and diplomacy to defend against, to deter, and to deescalate cyber incidents.

Reference 3 - 0.18% Coverage

All of these efforts are aimed at improving the government’s ability to understand the nature of a given cyber incident and to make rapid decisions about whether and how to respond to cyber incidents of significant national concern.