Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 1 reference coded [ 0.03% Coverage]

Reference 1 - 0.03% Coverage

to ensure the credibility of security partnerships that are fundamental to regional and global security.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 1 reference coded [ 0.03% Coverage]

Reference 1 - 0.03% Coverage

a range of credible response options~

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 2 references coded [ 0.22% Coverage]

Reference 1 - 0.13% Coverage

The U.S. military deters aggression by maintaining a credible nuclear capability that is safe, secure, and effective;

Reference 2 - 0.09% Coverage

Credible regional partners are vital to sustaining counter-VEO campaigns.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 6 references coded [ 1.11% 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 - 0.13% Coverage

To make these deterrence efforts credible, we must deploy strong defenses and architect resilient systems that recover quickly from attacks or other disruptions.

Reference 3 - 0.24% Coverage

But the United States’ ability to successfully deter state and non-state sponsored cyber threats must also rely at least as much on defensive strategies that raise technological and other barriers as on the credible knowledge that the United States can and will appropriately respond to such threats.

Reference 4 - 0.16% Coverage

In taking these steps, the Department of Defense is creating credible and reliable options for the President to deter adversaries from attacking in cyberspace and to defend the nation from cyber attacks.

Reference 5 - 0.19% Coverage

However, the United States must maintain consistent and credible messages and messengers, and develop the shared situational awareness necessary to determine whether an adversary received the signal and interpreted it correctly.

Reference 6 - 0.22% Coverage

A credible U.S. cyber deterrent will require sustained efforts by all elements of the government to pursuing policies and capabilities that improve network defenses, bolster the Nation’s cyber resiliency, and provide options for imposing costs on malicious cyber actors.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 2 references coded [ 0.09% Coverage]

Reference 1 - 0.03% Coverage

We must convince adversaries that we can and will defeat them—not just punish them if they att ack the United States.

Reference 2 - 0.05% Coverage

The United States must maintain the credible deterrence and assurance capabilities provided by our nuclear Triad and by U.S. theater nuclear capabilities deployed abroad

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 1 reference coded [ 0.10% Coverage]

Reference 1 - 0.10% Coverage

Deterring cybercrime requires a credible threat that perpetrators will be identified, apprehended, and brought to justice.