Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 2 references coded [ 0.09% Coverage]

Reference 1 - 0.04% Coverage

The status quo is no longer acceptable. The United States must signal to the world that it is serious about addressing this challenge with strong leadership and vision

Reference 2 - 0.05% Coverage

Anchoring and elevating leadership for cybersecurity-related policies at the White House signals to the United States and the international community that we are serious about cybersecurity.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 3 references coded [ 0.70% Coverage]

Reference 1 - 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 2 - 0.21% Coverage

The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States’ defenses.

Reference 3 - 0.23% Coverage

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.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 1 reference coded [ 0.08% Coverage]

Reference 1 - 0.08% Coverage

We will also develop technologies and tactics to deter and defeat efforts to attack our space systems; enable indications, warning, and attributions of such attacks;

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 7 references coded [ 1.54% Coverage]

Reference 1 - 0.04% Coverage

Declaratory Policy and Strategic Communications

Reference 2 - 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 3 - 0.29% Coverage

Promoting a nuanced and graduated declaratory policy and strategic communications that highlight the United States Government commitment to using its capabilities to defend against cyber attacks, but remains ambiguous on thresholds for response and consequences to discourage preemption or malicious cyber activities just below the threshold for response.

Reference 4 - 0.04% Coverage

Declaratory Policy and Strategic Communications

Reference 5 - 0.62% Coverage

Regardless of the method of deterrence, clear and frequent signaling to adversaries that their actions would be or are unacceptable will increase the likelihood that the United States successfully deters some malicious cyber activities. Such signaling can be direct or indirect, private or public. 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. To that end, the whole-of-government consultative process, constant collaboration with the private sector, and international coordination all increase the likelihood that the signaling component of the U.S. deterrent effort is successful.

Reference 6 - 0.12% Coverage

The United States has issued clear statements in the past regarding the U.S. intention to respond as necessary and appropriate to cyber threats.

Reference 7 - 0.22% Coverage

The Administration will consider whether to speak more openly about whether and how the United States might respond to malicious cyber activities, although such public discussion will require carefully balancing such transparency against intelligence and military equities.

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.