Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 1 reference coded [ 0.20% Coverage]

Reference 1 - 0.20% Coverage

We will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment and improving our ability to attribute and defeat attacks on our systems or supporting infrastructure.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 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\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 4 references coded [ 0.79% Coverage]

Reference 1 - 0.17% Coverage

For the purpose of this document, attribution is defined as the capability to determine the identity or location of those responsible for conducting or directing cyber attacks or other malicious cyber activity.

Reference 2 - 0.20% Coverage

Although achieving a high degree of certainty in a timely manner can prove difficult, the United States is continually improving our ability to attribute malicious cyber activities and will hold malicious actors accountable for their actions.

Reference 3 - 0.23% Coverage

Instead, the United States must maintain a spectrum of response capabilities that provide the President and senior U.S. leaders with options that can be tailored to   
10   
particular adversaries, the impact of the malicious activities, and the level of certainty regarding attribution.

Reference 4 - 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.