Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 1 reference coded [ 0.09% Coverage]

Reference 1 - 0.09% Coverage

The cyber threat is expanded and   
3   
exacerbated by lack of international norms, difficulties of attribution

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 3 references coded [ 0.37% Coverage]

Reference 1 - 0.17% Coverage

State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation.

Reference 2 - 0.11% Coverage

In addition, the United States requires strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution.

Reference 3 - 0.09% Coverage

The Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 1 reference coded [ 0.09% Coverage]

Reference 1 - 0.09% Coverage

Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 3 references coded [ 0.46% Coverage]

Reference 1 - 0.23% Coverage

While the United States’ ability to attribute a cyber attack to a specific actor   
4   
through long-term analysis has improved dramatically in recent years, allowing for malicious actors to be held responsible for their actions, high-confidence attribution5 in real-time remains difficult.

Reference 2 - 0.12% Coverage

Such efforts to change an adversary’s risk-benefit calculus have the potential to limit perceived options and can be pursued independent of attribution.

Reference 3 - 0.10% Coverage

Further developing intelligence capabilities that improve our ability to attribute and act against malicious cyber activities

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 2 references coded [ 0.10% Coverage]

Reference 1 - 0.05% Coverage

Such att acks have the capability to harm large numbers of people and institutions with comparatively minimal investment and a troubling degree of deniability.

Reference 2 - 0.05% Coverage

IMPROVE ATTRIBUTION , ACCOUNTABIL ITY, AND RESPONSE: We will invest in capabilities to support and improve our ability to attribute cyberattacks, to al low for rapid response.