Files\\2011 Case Study\\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\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 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\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 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