Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 2 references coded [ 0.05% Coverage]

Reference 1 - 0.01% Coverage

facing consequences when they do not.

Reference 2 - 0.04% Coverage

there must be consequences for those nations that break the rules—whether they are nonproliferation obligations, trade agreements, or human rights commitments.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

consequences

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 1 reference coded [ 0.06% Coverage]

Reference 1 - 0.06% Coverage

If deterrence fails, U.S. forces will be ready to project power globally to defeat and deny aggression in multiple theaters.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 4 references coded [ 0.78% Coverage]

Reference 1 - 0.07% Coverage

increase the costs and consequences that adversaries face as a result of their actions.

Reference 2 - 0.22% Coverage

Through the continued use of such law enforcement actions, the United States Government can reduce the risk of cyber threats by demonstrating that there are real consequences to malicious cyber activity – whether or not those responsible are associated with a foreign government.

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 - 0.20% Coverage

However, the United States Government will remain ambiguous in its statements on thresholds for response and consequences of cyber threats in order to discourage preemption or malicious cyber activities just below the threshold for response.