Files\\2011 Case Study\\CS1\_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\\CS1\_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\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 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\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 1 reference coded [ 0.05% Coverage]

Reference 1 - 0.05% Coverage

e United States will impose swift and costly consequences on foreign governments, criminals, and other actors who undertake signiﬁ cant malicious cyber activities.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 11 references coded [ 2.26% Coverage]

Reference 1 - 0.18% Coverage

We will simultaneously use a consequence-driven approach to prioritize actions that reduce the potential that the most advanced adversaries could cause large-scale or long-duration disruptions to critical infrastructure.

Reference 2 - 0.26% Coverage

The Admin-   
istration will clarify the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response. Clarity will enable proactive risk management that comprehensively   
addresses bilities, and consequences. threats, vulnera

Reference 3 - 0.27% Coverage

The Administration will work with the Congress to update electronic surveillance and computer crime statutes to enhance law enforcement’s capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious

Reference 4 - 0.20% Coverage

As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners.

Reference 5 - 0.23% Coverage

The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners.

Reference 6 - 0.15% Coverage

IMPOSE CONSEQUENCES: The United States will develop swift and transparent consequences,   
which we will impose consistent with our obligations and commitments to deter future bad behavior.

Reference 7 - 0.20% Coverage

he Administration will conduct interagency policy planning for the time periods leading up to, during, and after the imposition of consequences to ensure a timely and consistent process for responding to and deterring malicious cyber activities.

Reference 8 - 0.15% Coverage

The United States will work with partners when appropriate to impose consequences against malicious cyber actors in response to their activities against our nation and interests.

Reference 9 - 0.16% Coverage

BUILD A CYBER DETERRENCE INITIATIVE: The imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states.

Reference 10 - 0.18% Coverage

The United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior.

Reference 11 - 0.28% Coverage

The United States will work with like-minded states to coordinate and support each other’s responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.