Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 1 reference coded [ 0.13% Coverage]

Reference 1 - 0.13% Coverage

shaping behaviors and attitudes through the imposition of higher costs for malicious activity

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 1 reference coded [ 0.03% Coverage]

Reference 1 - 0.03% Coverage

raise the cost of their support.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 1 reference coded [ 0.07% Coverage]

Reference 1 - 0.07% Coverage

If deterrence fails at any given time, U.S. forces will be capable of defeating a regional adversary in a large-scale multi-phased campaign, and denying the objectives of – or imposing unacceptable costs on – a second aggressor in another region.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 1 reference coded [ 0.16% Coverage]

Reference 1 - 0.16% Coverage

Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary’s attack will succeed.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 2 references coded [ 0.43% Coverage]

Reference 1 - 0.28% Coverage

If deterrence fails, at any given time, our military will be capable of defeating a regional adversary in a large-scale, multi-phased campaign while denying the objectives of — or imposing unacceptable costs on — another aggressor in a different region.

Reference 2 - 0.15% Coverage

Deny an Adversary’s Objectives. Denying an adversary’s goals or imposing   
unacceptable costs is central to achieving our objectives.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 9 references coded [ 0.81% Coverage]

Reference 1 - 0.06% Coverage

In lockstep with our European allies, we are enforcing tough sanctions on Russia to impose costs and deter future aggression.

Reference 2 - 0.06% Coverage

We mobilized and are leading global efforts to impose costs to counter Russian aggression, to degrade and ultimately defeat ISIL

Reference 3 - 0.08% Coverage

Targeted economic sanctions will remain an effective tool for imposing costs on irresponsible actors and helping to dismantle criminal and terrorist networks.

Reference 4 - 0.07% Coverage

It should be based on a serious appreciation for the risk to our mission, our global responsibilities, and the opportunity costs at home and abroad.

Reference 5 - 0.21% Coverage

American diplomacy and leadership, backed by a strong military, remain essential to deterring future acts of inter-state aggression and provocation by reaffirming our security commitments to allies and partners, investing in their capabilities to withstand coercion, imposing costs on those who threaten their neighbors or violate fundamental international norms, and embedding our actions within wider regional strategies.

Reference 6 - 0.07% Coverage

We will defend ourselves, consistent with U.S. and international law, against cyber attacks and impose costs on malicious cyber actors,

Reference 7 - 0.03% Coverage

At the same time, we will exact an appropriate cost on transgressors

Reference 8 - 0.13% Coverage

Targeted economic sanctions remain an effective tool for imposing costs on those irresponsible actors whose military aggression, illicit proliferation, or unprovoked violence threaten both international rules and norms and the peace they were designed to preserve.

Reference 9 - 0.08% Coverage

And we will continue to impose significant costs on Russia through sanctions and other means while countering Moscow’s deceptive propaganda with the unvarnished truth

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 14 references coded [ 1.92% Coverage]

Reference 1 - 0.02% Coverage

Deterrence by Cost Imposition

Reference 2 - 0.05% Coverage

Measures to Impose Economic Costs on Malicious Cyber Actors

Reference 3 - 0.20% Coverage

Our targeted use of these instruments is intended to create uncertainty in adversaries’ minds about the effectiveness of any malicious cyber activities and to increase the costs and consequences that adversaries face as a result of their actions.

Reference 4 - 0.06% Coverage

The United States is also pursuing deterrence through cost imposition

Reference 5 - 0.12% Coverage

inflict penalties and costs against adversaries that choose to conduct cyber attacks or other malicious cyber activity against the United States.

Reference 6 - 0.02% Coverage

Deterrence by Cost Imposition

Reference 7 - 0.06% Coverage

Developing options to impose economic costs on malicious cyber actors.

Reference 8 - 0.28% Coverage

Measures to Impose Economic Costs on Malicious Cyber Actors   
Economic tools may offer options for imposing costs on malicious cyber actors and deterring certain cyber threats, particularly from adversaries who seek to undermine U.S. economic security by illicitly obtaining trade secrets, including intellectual property, or controlled technology.

Reference 9 - 0.23% Coverage

When appropriate and warranted, the Administration will pursue actions to impose economic costs on the malicious cyber actors responsible for such activity, including when such activity constitutes a violation of international trade rules or the rules of the World Trade Organization.

Reference 10 - 0.18% Coverage

In establishing this new policy, the Administration is creating a means of imposing economic costs against not just those that conduct cyber attacks, but those responsible for supporting, enabling, or ordering such attacks.

Reference 11 - 0.18% Coverage

Law enforcement can also be an effective deterrent to cyber threats both through denial (e.g., taking down a criminal botnet that could be used in an attack) or cost imposition (e.g., arresting the perpetrators of cyber attacks).

Reference 12 - 0.18% Coverage

Successful investigations and prosecutions impose direct costs on malicious cyber actors, as well as states   
11   
that may support or harbor them, and serve to deter persons or organizations from continuing to conduct such activity.

Reference 13 - 0.11% Coverage

By publicizing such cases, the United States ensures that malicious cyber actors understand that such actions will incur significant costs.

Reference 14 - 0.22% Coverage

A credible U.S. cyber deterrent will require sustained efforts by all elements of the government to pursuing policies and capabilities that improve network defenses, bolster the Nation’s cyber resiliency, and provide options for imposing costs on malicious cyber actors.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 3 references coded [ 0.13% Coverage]

Reference 1 - 0.03% Coverage

Openness also imposes costs, since adversaries exploit our free and democratic system to harm the United States.

Reference 2 - 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.

Reference 3 - 0.04% Coverage

In other areas we should seek new capabilities that create clear advantages for our mi l itary whi le posing costly dilemmas for our adversaries.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 5 references coded [ 1.38% Coverage]

Reference 1 - 0.18% Coverage

Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and inter-   
I N T R O D U C T IO N   
national businesses and our allies and partners without paying costs likely to deter future cyber aggression.

Reference 2 - 0.24% Coverage

The Administration also   
recognizes that a purely technocratic approach to cyberspace is insufficient to address the nature of the new problems we confront.   
The   
United States must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation.

Reference 3 - 0.54% Coverage

The Strategy’s success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as   
well as detection of, resilience against, response to, and recovery from incidents; destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives.

Reference 4 - 0.18% Coverage

We will also deter malicious cyber actors by imposing costs on them and their sponsors by leveraging a range of tools, including but not limited to prosecutions and economic sanctions, as part of a broader deterrence strategy.

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.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 6 references coded [ 0.40% Coverage]

Reference 1 - 0.07% Coverage

Actions aimed at strengthening deterrence work by different logics: denial, resilience, and cost imposition. Optimal combinations need to be tailored to specific settings and deterrence objectives in an integrated deterrence approach.

Reference 2 - 0.07% Coverage

Deterrence by Direct and Collective Cost Imposition. Denial and resilience strategies are necessary but not always sufficient. Effective deterrence may also hinge on our ability to impose costs in excess to the perceived benefits of aggression.

Reference 3 - 0.09% Coverage

Direct cost imposition approaches also include a broad range of other means, including conventional long-range fires, offensive cyber, irregular warfare, support for foreign internal defense, and interagency instruments, such as economic sanctions, export controls, and diplomatic measures.

Reference 4 - 0.03% Coverage

Collective cost imposition approaches increase the expectation that aggression will be met with a collective response.

Reference 5 - 0.04% Coverage

For Ally and partner countries that border Russia, the Department will support efforts to build out response options that enable cost imposition

Reference 6 - 0.10% Coverage

Deterring North Korean Attacks. The Department will continue to deter attacks through forward posture; integrated air and missile defense; close coordination and interoperability with our ROK Ally; nuclear deterrence; resilience initiatives; and the potential for direct cost imposition approaches that come from globally deployable Joint Forces.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 4 references coded [ 0.28% Coverage]

Reference 1 - 0.07% Coverage

Our National Defense Strategy relies on integrated deterrence: the seamless combination of capabilities to convince potential adversaries that the costs of their hostile activities outweigh their benefits.1

Reference 2 - 0.08% Coverage

This augments the traditional backstop of combat-credible conventional and strategic capabilities, allowing us to better shape adversary perceptions of risks and costs of action against core U.S. interests, at any time and across any domain.

Reference 3 - 0.07% Coverage

Russia’s further invasion of Ukraine poses a grave threat to this vision, which is why we are determined to support Ukraine in defending its sovereignty and territorial integrity while imposing severe costs on Moscow for its aggression.

Reference 4 - 0.06% Coverage

In coordination with international partners and regional bodies, we will counter democratic backsliding by imposing costs for coups and pressing for progress on civilian transitions.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 2 references coded [ 0.20% Coverage]

Reference 1 - 0.12% Coverage

Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences.

Reference 2 - 0.08% Coverage

The United States seeks a world where responsible state behavior in cyberspace is expected and rewarded and where irresponsible behavior is isolating and costly.

**Annotations**

1 Definition of Integrated Deterrence