Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 17 references coded [ 0.66% Coverage]

Reference 1 - 0.01% Coverage

determination to deter aggression

Reference 2 - 0.02% Coverage

ensuring the reliability and effectiveness of our deterrent

Reference 3 - 0.05% Coverage

Our military must maintain its conventional superiority and, as long as nuclear weapons exist, our nuclear deterrent capability, while continuing to enhance its capacity to defeat asymmetric threats

Reference 4 - 0.05% Coverage

Defense: We are strengthening our military to ensure that it can prevail in today’s wars; to prevent and deter threats against the United States, its interests, and our allies and partners;

Reference 5 - 0.02% Coverage

deterring and defeating aggression in anti-access environments

Reference 6 - 0.04% Coverage

the United States is now threatened by the potential spread of nuclear weapons to extremists who may not be deterred from using them

Reference 7 - 0.02% Coverage

We maintain superior capabilities to deter and defeat adaptive enemies and

Reference 8 - 0.04% Coverage

As we do everything within our power to prevent these dangers, we also recognize that we will not be able to deter or prevent every single threat.

Reference 9 - 0.08% Coverage

Security at home relies on our shared efforts to prevent and deter attacks by identifying and interdicting threats, denying hostile actors the ability to operate within our borders, protecting the nation’s critical infrastructure and key resources, and securing cyberspace.

Reference 10 - 0.05% Coverage

This means credibly underwriting U.S. defense commitments with tailored approaches to deterrence and ensuring the U.S. military continues to have the necessary capabilities across all domains

Reference 11 - 0.07% Coverage

As long as any nuclear weapons exist, the United States will sustain a safe, secure, and effective nuclear arsenal, both to deter potential adversaries and to assure U.S. allies and other security partners that they can count on America’s security commitments.

Reference 12 - 0.03% Coverage

We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by:

Reference 13 - 0.03% Coverage

effective border security and immigration enforcement must keep the country safe and deter unlawful entry.

Reference 14 - 0.02% Coverage

Deterring Threats to the International Financial System

Reference 15 - 0.07% Coverage

we will strengthen our regional deterrence postures—for example, through phased, adaptive missile defense architectures—in order to make certain that regional adversaries gain no advantages from their acquisition of new, offensive military capabilities.

Reference 16 - 0.01% Coverage

deter vital threats

Reference 17 - 0.06% Coverage

we will place renewed emphasis on deterrence and prevention by mobilizing diplomatic action, and use development and security sector assistance to build the capacity of at-risk nations and reduce the appeal of violent extremism

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 12 references coded [ 0.15% Coverage]

Reference 1 - 0.01% Coverage

Deter

Reference 2 - 0.01% Coverage

deter conflict

Reference 3 - 0.05% Coverage

Our deterrent remains grounded in land, air, and naval forces capable of fighting limited and large-scale conflicts in environments where anti-access weaponry and tactics are used, as well as forces prepared to respond to the full range of challenges posed by state and non-state groups.

Reference 4 - 0.02% Coverage

We will maintain a safe, secure, and effective nuclear arsenal to deter attack on the United States, and on our allies and partners.

Reference 5 - 0.01% Coverage

prevent-and-deter

Reference 6 - 0.01% Coverage

and deterring other potential major adversaries

Reference 7 - 0.01% Coverage

deterrence

Reference 8 - 0.01% Coverage

deterrence

Reference 9 - 0.01% Coverage

Deter and defeat aggression in anti-access environments

Reference 10 - 0.01% Coverage

deter,

Reference 11 - 0.06% Coverage

Deterrence of such threats and defense against them can be enhanced through measures aimed at better understanding potential threats, securing and reducing dangerous materials wherever possible, positioning forces to monitor and track lethal agents and materials and their means of delivery, and, where relevant, defeating the agents themselves.

Reference 12 - 0.01% Coverage

deter

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 6 references coded [ 1.35% Coverage]

Reference 1 - 0.24% Coverage

to deter and mitigate insider threats, DoD will strengthen its workforce communications, workforce accountability, internal monitoring, and information management capabilities.

Reference 2 - 0.33% Coverage

DoD seeks to foster a stronger culture of information assurance within its workforce to assure individual responsibility and deter malicious insiders by shaping behaviors and attitudes through the imposition of higher costs for malicious activity.

Reference 3 - 0.21% Coverage

The development of international   
shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence.

Reference 4 - 0.25% Coverage

oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national assets as necessary and appropriate

Reference 5 - 0.24% Coverage

DoD will expand its formal and informal cyber cooperation to a wider pool of allied and partner militaries to develop collective self-defense and increase collective deterrence.

Reference 6 - 0.09% Coverage

create coalitions to deter malicious activities in cyberspace.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 9 references coded [ 0.14% Coverage]

Reference 1 - 0.01% Coverage

Deterring

Reference 2 - 0.02% Coverage

and appropriate deterrence~

Reference 3 - 0.01% Coverage

Deterring

Reference 4 - 0.01% Coverage

deter

Reference 5 - 0.02% Coverage

deterring malicious actors,

Reference 6 - 0.01% Coverage

Deterrence

Reference 7 - 0.01% Coverage

domestic deterrence

Reference 8 - 0.03% Coverage

collective deterrence capabilities

Reference 9 - 0.03% Coverage

deter malicious activities in cyberspace

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 17 references coded [ 2.89% Coverage]

Reference 1 - 0.13% Coverage

we will be prepared to act as security guarantor – preferably with partners and allies, but alone if necessary – to deter and defeat acts of aggression.

Reference 2 - 0.09% Coverage

deter and defeat aggression that would undermine international stability as we fight these campaigns.

Reference 3 - 0.01% Coverage

deterrence

Reference 4 - 0.07% Coverage

We will adapt deterrence principles to our efforts in countering extremists.

Reference 5 - 0.02% Coverage

difficult to deter directly

Reference 6 - 0.02% Coverage

Deter and Defeat Aggression

Reference 7 - 0.10% Coverage

the Joint Force will be prepared to deter and defeat regional aggression that would threaten our national interests

Reference 8 - 0.70% Coverage

Deter Aggression: The United States seeks the peace and security of a world without nuclear weapons. However, as long as nuclear weapons exist, deterring nuclear attack on the United States, our allies, and partners will continue to be the fundamental role of U.S. nuclear weapons. In support of the President’s vision, we will reduce the role and numbers of nuclear weapons, while maintaining a safe, secure, and effective strategic deterrent. The Joint Force will provide capabilities to deter aggression and assure our allies and partners through our nuclear arsenal and overseas missile defense capabilities. We will continue to lead in advancing Ballistic Missile Defense capabilities against limited attacks and we seek opportunities for cooperation with allies and partners in this area.

Reference 9 - 0.14% Coverage

We must also maintain a robust conventional deterrent. Deterrence and   
assurance requires the ability to rapidly and globally project power in all domains.

Reference 10 - 0.41% Coverage

We will support whole-of-nation deterrence approaches that blend economic, diplomatic, and military tools to influence adversary behavior. Denying an aggressor the benefits of achieving its objectives can be just as effective as in altering its strategic calculus through the threat of retaliation. The most effective deterrence approaches make use of both techniques, while also providing potential adversaries acceptable alternative courses of action.

Reference 11 - 0.27% Coverage

We must also adapt deterrence principles to 21st century security challenges. We will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment and improving our ability to attribute and defeat attacks on our systems or supporting infrastructure.

Reference 12 - 0.15% Coverage

These collective domains are essential and interdependent mediums for the Joint Force’s projection and sustainment of power and ability to deter and defeat aggression.

Reference 13 - 0.19% Coverage

We will also train for power projection operations in space-degraded environments that minimize the   
9   
incentives to attack space capabilities, and will maintain a range of options to deter or punish such activities.

Reference 14 - 0.11% Coverage

Working with Canada and Mexico, we will remain prepared to deter and defeat direct threats to our North American homeland.

Reference 15 - 0.08% Coverage

employs a combination of detection, deterrence, denial, and multi-layered defense.

Reference 16 - 0.32% Coverage

Joint nuclear forces will continue to support strategic stability through maintenance of an assured second-strike capability. We will ensure our nuclear forces remain effective, safe, and secure. We will retain sufficient nuclear force structure to hedge against unexpected geopolitical change, technological problems, and operational vulnerabilities.

Reference 17 - 0.09% Coverage

measure joint readiness across the services to deter conflict and respond promptly during contingencies.

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 3 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

deterrence

Reference 2 - 0.01% Coverage

deterrence,

Reference 3 - 0.01% Coverage

deter,

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 9 references coded [ 0.38% Coverage]

Reference 1 - 0.02% Coverage

Protect the homeland, to deter and defeat attacks on the United States

Reference 2 - 0.01% Coverage

deter adversaries,

Reference 3 - 0.06% Coverage

Our nuclear deterrent is the ultimate protection against a nuclear   
attack on the United States, and through extended deterrence, it also serves to reassure our distant allies of their security against regional aggression

Reference 4 - 0.07% Coverage

Building security globally not only assures allies and   
EXEC UTIV E SUMMA R Y V   
partners and builds their capacity but also helps protect the homeland by deterring conflict and increasing stability in regions like the Middle East and North Africa.

Reference 5 - 0.02% Coverage

deterring aggression and assuring allies through forward presence and engagement.

Reference 6 - 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.

Reference 7 - 0.04% Coverage

We will continue to maintain a strong military posture in the Gulf region – one that can respond swiftly to crisis, deter aggression,

Reference 8 - 0.07% Coverage

Nuclear Deterrence. We will continue to invest in modernizing our essential nuclear delivery systems; warning, command and control; and, in collaboration with the Department of Energy, nuclear weapons and supporting infrastructure.

Reference 9 - 0.04% Coverage

pursue a multi-layered approach to deter attacks on space systems while retaining the capabilities to respond should deterrence fail.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 20 references coded [ 2.93% Coverage]

Reference 1 - 0.09% Coverage

Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability

Reference 2 - 0.14% Coverage

In a manner consistent with U.S. and international law, the Department of Defense seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests during times of peace, crisis, or conflict.

Reference 3 - 0.09% Coverage

Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability

Reference 4 - 0.03% Coverage

Deterrence in the Future Security Environment

Reference 5 - 0.15% Coverage

In the face of an escalating threat, the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests.

Reference 6 - 0.16% Coverage

Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors’ behavior.

Reference 7 - 0.26% Coverage

As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.

Reference 8 - 0.09% Coverage

The deterrence of state and non-state groups in cyberspace will thus require the focused attention of multiple U.S. government departments and agencies.

Reference 9 - 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.

Reference 10 - 0.21% Coverage

The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States’ defenses.

Reference 11 - 0.18% Coverage

DoD must increase its defensive capabilities to defend DoD networks and defend the nation from sophisticated cyberattacks, and must work with other departments, agencies,   
international allies and   
partners, and the private sector to strengthen deterrence by denial through improved cybersecurity.

Reference 12 - 0.17% Coverage

In order for resilience to succeed as a factor in effective deterrence, other agencies of the government must work with critical infrastructure owners and operators and the private sector more broadly to develop resilient and redundant systems that can withstand a potential attack.

Reference 13 - 0.09% Coverage

Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups.

Reference 14 - 0.10% Coverage

This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time.

Reference 15 - 0.14% Coverage

Because they broke the law and to deter China from conducting future cyber espionage, the Justice Department indicted five members of the People’s Liberation Army for stealing U.S. intellectual property to directly benefit Chinese companies.

Reference 16 - 0.10% Coverage

The Defense Department will support the Justice Department and other agencies in exploring new tools and capabilities to help deter such activity in cyberspace.

Reference 17 - 0.14% Coverage

The Department of Defense must work with its interagency partners, the private sector, and allied and partner nations to deter and if necessary defeat a cyberattack of significant consequence on the U.S. homeland and U.S. interests.

Reference 18 - 0.12% Coverage

To defend the nation, DoD must build partnerships with other agencies of the government to prepare to conduct combined cyber operations to deter and if necessary defeat aggression in cyberspace.

Reference 19 - 0.26% Coverage

Assess DoD’s cyber deterrence posture and strategy. Building off of the Defense Science Board’s Task Force on Cyber Deterrence, U.S. Strategic Command (USSTRATCOM), in coordination with the Joint Staff and the Office of the Secretary of Defense, will assess the Department of Defense’s ability to deter specific state and non-state actors from conducting cyberattacks of significant consequence on the U.S. homeland and against U.S. interests

Reference 20 - 0.27% Coverage

In conducting its analysis, USSTRATCOM must determine whether DoD is building the capabilities required for attributing and deterring key threats from conducting such attacks and recommend specific actions that DoD can take to improve its cyber deterrence posture. Careful attention should be devoted also to deterring non-state actors that may fall outside of traditional deterrence frameworks but which could pose a considerable threat to U.S. interests.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 19 references coded [ 2.37% Coverage]

Reference 1 - 0.13% Coverage

We are working with allies and partners to deter, deny, and – when necessary – defeat potential state adversaries.

Reference 2 - 0.17% Coverage

Emerging technologies are impacting the calculus of deterrence and conflict   
management by increasing uncertainty and compressing decision space.

Reference 3 - 0.05% Coverage

Deter, deny, and defeat state adversaries.

Reference 4 - 0.05% Coverage

to deter, deny, and defeat state adversaries

Reference 5 - 0.09% Coverage

deter aggression and assure allies through forward presence and engagement.

Reference 6 - 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 7 - 0.05% Coverage

Deter, Deny, and Defeat State Adversaries

Reference 8 - 0.13% Coverage

The U.S. military deters aggression by maintaining a credible nuclear capability that is safe, secure, and effective;

Reference 9 - 0.05% Coverage

Should deterrence fail to prevent aggression,

Reference 10 - 0.21% Coverage

Deterring a direct attack on the United States and our allies is a priority mission,   
requiring homeland and regional defenses tied to secure conventional and nuclear strike capabilities.

Reference 11 - 0.11% Coverage

provide the force depth needed to achieve victory while simultaneously deterring other threats.

Reference 12 - 0.17% Coverage

Such activities increase the capabilities and capacity of partners, thereby enhancing our collective ability to deter aggression and defeat extremists.

Reference 13 - 0.20% Coverage

NATO   
provides vital collective security guarantees and is strategically important for deterring conflict, particularly in light of recent Russian aggression on its periphery.

Reference 14 - 0.25% Coverage

With advanced partners like NATO, Australia, Japan, and Korea, our exercises emphasize sophisticated capabilities such as assuring access to contested environments and deterring and responding to hybrid conflicts.

Reference 15 - 0.06% Coverage

Maintain a Secure and Effective Nuclear Deterrent.

Reference 16 - 0.06% Coverage

Maintain a secure and effective nuclear deterrent

Reference 17 - 0.15% Coverage

flowing additional U.S. forces and capabilities to a given region to strengthen deterrence, prevent escalation, and reassure allies.

Reference 18 - 0.14% Coverage

Our goal is to strengthen deterrence while ensuring the long-term viability of our full-spectrum power projection capacity.

Reference 19 - 0.02% Coverage

deter adversaries

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 14 references coded [ 1.16% 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 - 0.05% Coverage

It signals our resolve and readiness to deter and, if necessary, defeat potential adversaries.

Reference 3 - 0.10% Coverage

Our military will remain ready to deter and defeat threats to the homeland, including against missile, cyber, and terrorist attacks, while mitigating the effects of potential attacks and natural disasters.

Reference 4 - 0.03% Coverage

deter aggression through forward presence and engagement.

Reference 5 - 0.06% Coverage

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

Reference 6 - 0.04% Coverage

protect our investment in foundational capabilities like the nuclear deterrent

Reference 7 - 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 8 - 0.10% Coverage

As long as nuclear weapons exist, the United States must invest the resources necessary to maintain—without testing—a safe, secure, and effective nuclear deterrent that preserves strategic stability.

Reference 9 - 0.08% Coverage

We will also develop technologies and tactics to deter and defeat efforts to attack our space systems; enable indications, warning, and attributions of such attacks;

Reference 10 - 0.08% Coverage

We will therefore maintain the capability to ensure the free flow of commerce, to respond quickly to those in need, and to deter those who might contemplate aggression.

Reference 11 - 0.10% Coverage

In many cases, our use of targeted sanctions and other coercive measures are meant not only to uphold international norms, but to deter severe threats to stability and order at the regional level.

Reference 12 - 0.08% Coverage

We will deter Russian aggression, remain alert to its strategic capabilities, and help our allies and partners resist Russian coercion over the long term, if necessary

Reference 13 - 0.11% Coverage

We are therefore investing in the ability of Israel, Jordan, and our Gulf partners to deter aggression while maintaining our unwavering commitment to Israel’s security, including its Qualitative Military Edge.

Reference 14 - 0.05% Coverage

We will deter and defeat any adversary that threatens our national security and that of our allies.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 52 references coded [ 7.86% Coverage]

Reference 1 - 0.03% Coverage

What the United States Will Seek to Deter

Reference 2 - 0.02% Coverage

Cyber Deterrence Strategies

Reference 3 - 0.04% Coverage

Component Elements of U.S. Cyber Deterrence Policy

Reference 4 - 0.02% Coverage

Deterrence by Denial

Reference 5 - 0.02% Coverage

Deterrence by Cost Imposition

Reference 6 - 0.03% Coverage

Activities that Support Deterrence

Reference 7 - 0.12% Coverage

It is these significant threats that the United States Government seeks to addresses through its policy for deterring adversaries in cyberspace.

Reference 8 - 0.08% Coverage

deter nation-states and non-state actors seeking to harm the United States through cyber-enabled means

Reference 9 - 0.33% Coverage

Although cyber attacks can have a range of direct and indirect effects that vary in their severity, U.S. deterrence efforts are particularly focused on those attacks that could result in loss of life, harm to U.S. critical infrastructure, significant damage to property, or significant threats to the national security, foreign policy, or economic health or financial stability of the United States or its interests

Reference 10 - 0.25% Coverage

Although the principal focus of the United States Government’s cyber deterrence efforts focus principally on significant threats to U.S. interests, the framework outlined in this report, including the “whole of government” approach, also serves to deter lesser threats, generally through non-military means.

Reference 11 - 0.03% Coverage

What the United States Will Seek to Deter

Reference 12 - 0.21% Coverage

It is the United States Government’s policy to utilize all instruments of national power to deter cyber attacks or other malicious cyber activity that pose a significant threat to the national or economic security of the United States or its vital interests.

Reference 13 - 0.07% Coverage

The following concerns represent priority areas to focus deterrence activities.

Reference 14 - 0.02% Coverage

Cyber Deterrence Strategies

Reference 15 - 0.13% Coverage

Deterrence seeks to convince adversaries – by means of influence over their decision-making – not to take actions that threaten important national interests.

Reference 16 - 0.12% Coverage

But cyber deterrence in the Information Age is substantially different from Cold War-era concepts intended to deter the use of weapons of mass destruction.

Reference 17 - 0.09% Coverage

pose challenges for deterrence that are different in kind and scope than deterrence in more traditional areas.

Reference 18 - 0.16% Coverage

To account for the distinctive characteristics of the cyber threat, the United States Government is taking a multidisciplinary approach to developing the strategies and tactics of cyber deterrence.

Reference 19 - 0.04% Coverage

Component Elements of U.S. Cyber Deterrence Policy

Reference 20 - 0.59% Coverage

Given the characteristics of cyberspace, U.S. experiences in the areas of counterterrorism and counterproliferation are highly relevant. The Administration has learned in those contexts that an important means of countering an asymmetry in capabilities and information is to adopt a broad concept of deterrence that uses a “whole-of-government” approach to bring all elements of national power to bear on a particular threat. Similarly, the United States’ cyber deterrence policy relies on all instruments of national power – diplomatic, information, military, economic, intelligence, and law enforcement – as well as public-private partnerships that enhance information security for U.S. citizens, industry, and the government.

Reference 21 - 0.14% Coverage

Deterrence by denial efforts aim to persuade adversaries that the United States can thwart malicious cyber activity, thereby reducing the incentive to conduct such activities.

Reference 22 - 0.13% Coverage

To make these deterrence efforts credible, we must deploy strong defenses and architect resilient systems that recover quickly from attacks or other disruptions.

Reference 23 - 0.06% Coverage

The United States is also pursuing deterrence through cost imposition

Reference 24 - 0.02% Coverage

Deterrence by Denial

Reference 25 - 0.24% Coverage

But the United States’ ability to successfully deter state and non-state sponsored cyber threats must also rely at least as much on defensive strategies that raise technological and other barriers as on the credible knowledge that the United States can and will appropriately respond to such threats.

Reference 26 - 0.17% Coverage

the Administration’s cyber deterrence policy seeks to demonstrate the strength of government and private sector network defenses to create doubt that such activity would succeed or have the desired effects.

Reference 27 - 0.30% Coverage

The NITTF, under joint leadership of the Attorney General and the Director of National Intelligence, brings together security, counterintelligence, and information assurance experts from across the government to develop a government-wide insider threat program for deterring, detecting, and mitigating insider threats, including compromises of classified information.

Reference 28 - 0.02% Coverage

Deterrence by Cost Imposition

Reference 29 - 0.03% Coverage

deterring certain cyber threats,

Reference 30 - 0.15% Coverage

The United States Government has used these tools for many years to address other policy challenges and will continue apply them, as appropriate, to deter and respond to cyber threats as well.

Reference 31 - 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 32 - 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 33 - 0.16% Coverage

Such successful law enforcement efforts can deter those who would consider using cyber means to cause people physical harm, or to disrupt the functioning of society, government, or key public services.

Reference 34 - 0.26% Coverage

Collectively, the Administration’s efforts are making headway in building the cooperative relationships necessary to pursue criminal cyber actors wherever they reside and bring them to justice, thus adding another deterrent to those who constitute a significant threat to our national security and economic interests.

Reference 35 - 0.16% Coverage

The United States Government’s first preference is to use network defense, law enforcement measures, economic actions, and diplomacy to defend against, to deter, and to deescalate cyber incidents.

Reference 36 - 0.13% Coverage

When defense and deterrence efforts are insufficient, however, the United States Government must have the capability and capacity to defend the nation in cyberspace.

Reference 37 - 0.16% Coverage

In taking these steps, the Department of Defense is creating credible and reliable options for the President to deter adversaries from attacking in cyberspace and to defend the nation from cyber attacks.

Reference 38 - 0.03% Coverage

Activities that Support Deterrence

Reference 39 - 0.19% Coverage

Regardless of the method of deterrence, clear and frequent signaling to adversaries that their actions would be or are unacceptable will increase the likelihood that the United States successfully deters some malicious cyber activities

Reference 40 - 0.20% Coverage

To that end, the whole-of-government consultative process, constant collaboration with the private sector, and international coordination all increase the likelihood that the signaling component of the U.S. deterrent effort is successful.

Reference 41 - 0.24% Coverage

Beyond declaratory policy, the United States will also use strategic communications as a deterrence tool. In some cases, the Administration may highlight investigations, criminal charges, successful prosecutions, or other law enforcement activities that enhance the U.S. deterrence posture.

Reference 42 - 0.11% Coverage

Intelligence collection, analysis, and operations are essential to the United States Government’s efforts to deter cyber threats.

Reference 43 - 0.12% Coverage

Global reliance on networked computer systems should encourage all nations to cooperate together in mutual self-interest to deter cyber threats.

Reference 44 - 0.27% Coverage

Effective international collaboration on cyber deterrence will require the United States to share its perspective on the threat environment with allies and international partners, lead the way in developing and promulgating norms of state behavior in cyberspace, and support international partners’ efforts to secure their own networks.

Reference 45 - 0.25% Coverage

The United States Government is also working with its counterparts around the world to enhance deterrence by expanding bilateral and multilateral defense and security relationships to include greater cooperation in the areas of network defense, information sharing, incident response, and resiliency.

Reference 46 - 0.20% Coverage

In taking these actions, the United States intends to form a group of like-minded states that together seek to deter cyber aggression and to enhance global economic security while sustaining an open and interoperable global Internet for all users.

Reference 47 - 0.21% Coverage

Such dialogues reinforce other policy efforts that support cyber deterrence by creating an environment where parties can explore new avenues of cooperation and build transparency measures to reduce the risk of miscalculation in response to a cyber incident.

Reference 48 - 0.25% Coverage

To combat this risk – and create the conditions necessary for deterrence to be successful – the United States Government is pursuing bilateral and multilateral trust and transparency measures to reduce the risk of escalation and unintended consequences that could result from a poorly understood cyber incident.

Reference 49 - 0.29% Coverage

The Administration seeks to shape the future of cybersecurity through a comprehensive plan and investment strategy to develop the tools, techniques, and national workforce necessary to continue to improve the resilience of U.S. computers, networks, and critical infrastructure and provide new technological options for deterring malicious cyber activities.

Reference 50 - 0.15% Coverage

The United States Government is committed to identifying and defending against cyber attacks and other malicious cyber activity and to deterring those who choose to conduct such activity.

Reference 51 - 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.

Reference 52 - 0.20% Coverage

This policy document offers an initial roadmap for the United States Government’s departments and agencies to identify their role in the United States’ cyber deterrence efforts, to execute on specific lines of effort, and to develop plans for the future.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 27 references coded [ 1.39% Coverage]

Reference 1 - 0.03% Coverage

Just as American weakness invites challenge, American strength and confidence deters war and promotes peace.

Reference 2 - 0.05% Coverage

Third, we will preserve peace through strength by rebuilding our military so that it remains preeminent, deters our adversaries, and if necessary, is able to fight and win.

Reference 3 - 0.03% Coverage

We must also deter, disrupt, and defeat potential threats before they reach the United States.

Reference 4 - 0.04% Coverage

The U.S. Government will work with foreign partners to deter, detect, and disrupt suspicious individuals well before they enter the United States.

Reference 5 - 0.05% Coverage

ENFORCE IMMIGRATION LAWS: We will enforce immigration laws, both at the border and in the interior, to provide an eﬀ ective deterrent to illegal immigration.

Reference 6 - 0.06% Coverage

The United States also works with allies and partners to deter and disrupt other foreign terrori st groups that threat en t he h ome la n d —i nc l ud - ing Iranian-backed groups such as Lebanese Hizballah

Reference 7 - 0.01% Coverage

DETER AND DISRUPT MALICIOUS CYBER ACTORS:

Reference 8 - 0.05% Coverage

A stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.

Reference 9 - 0.05% Coverage

Experience suggests that the willingness of rivals to abandon or forgo aggression depends on their perception of U.S. strength and the vitality of our alliances.

Reference 10 - 0.10% Coverage

A strong military ensures that our diplomats are able to operate from a position of strength. In this way we can, together with our allies and partners, deter and if necessary, defeat aggression against U.S. interests and increase the likelihood of managing competitions without violent conﬂ ict and preserving peace.

Reference 11 - 0.03% Coverage

Moreover, deterrence today i s s ign i ficant ly more complex to achieve than during the Cold War.

Reference 12 - 0.03% Coverage

Deterrence must be extended across all of these domains and must address all possible strategic attacks.

Reference 13 - 0.05% Coverage

We must ensure the ability to deter potential enemies by denial, convincing them that they cannot accomplish objectives through the use of force or other forms of aggression.

Reference 14 - 0.03% Coverage

The Joint Force must remain capable of deterring and defeating the full range of threats to the United States.

Reference 15 - 0.09% Coverage

To deter conflict and, if deterrence fails, to win in war, the Nation must be able to field forces capable of operating in sufficient scale and for ample duration to defeat enemies, consolidate military gains, and achieve sustainable outcomes that protect the American people and our vital interests.

Reference 16 - 0.08% Coverage

Nuclear weapons have served a vital purpose in America’s National Security Strategy for the past 70 years. They are the foundation of our strategy to preserve peace and stability by deterring aggression against the United States, our allies, and our partners.

Reference 17 - 0.06% Coverage

While nuclear deterrence strategies cannot prevent all conflict, they are essen-   
30   
tial to prevent nuclear att ack, non-nuclear strategic attacks, and large-scale conventional aggression

Reference 18 - 0.06% Coverage

In addition, the extension of the U.S. nuclear deterrent to more than 30 allies and partners helps to assure their security, and reduces their need to possess their own nuclear capabilities.

Reference 19 - 0.05% Coverage

The United States must maintain the credible deterrence and assurance capabilities provided by our nuclear Triad and by U.S. theater nuclear capabilities deployed abroad

Reference 20 - 0.07% Coverage

The United States does not need to match the nuclear arsenals of other powers, but we must sustain a stockpile that can deter adversaries, assure allies and partners, and achieve U.S. objectives if deterrence fails.

Reference 21 - 0.05% Coverage

MAINTAIN STABLE DETERRENCE: To avoid miscalculation, the United States will conduct discussions with other states to build predictable relationships and reduce nuclear risks.

Reference 22 - 0.05% Coverage

The United States will deter,   
N A TI O N A L S E C U R IT Y S TR A TE G Y   
defend, and when necessary defeat malicious actors who use cyberspace capabilities against the United States

Reference 23 - 0.06% Coverage

Economic tools—including sanctions, anti-money-laundering and anti-corruption measures, and enforcement actions—can be important parts of broader strategies to deter, coerce, and constrain adversaries.

Reference 24 - 0.04% Coverage

They share our interests and responsibility for resisting authoritarian trends, contesting radical ideologies, and deterring aggression.

Reference 25 - 0.04% Coverage

MILITARY AND SECURITY: We will maintain a forward military presence capable of deterring and, if necessary, defeating any adversary.

Reference 26 - 0.07% Coverage

We will maintain our strong ties with Taiwan in accordance with our “One China” policy, including our commitments under the   
47   
Taiwan Relations Act to provide for Taiwan’s legitimate defense needs and deter coercion.

Reference 27 - 0.05% Coverage

On NATO’s eastern flank we will continue to strengthen deterrence and defense, and catalyze frontline allies and partners’ efforts to better defend themselves.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 20 references coded [ 3.63% 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 - 0.18% Coverage

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive.

Reference 3 - 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 4 - 0.16% Coverage

3) preserve peace and security by strengthening the United States’ ability — in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes

Reference 5 - 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 6 - 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 7 - 0.24% Coverage

To effectively deter, disrupt, and prevent cyber threats, law enforcement will work with private industry to confront challenges presented by technological barriers, such as anonymization and encryption technologies, to obtain time-sensitive evidence pursuant to appropriate legal process.

Reference 8 - 0.12% Coverage

Law enforcement actions to combat criminal cyber activity serve as an instrument of national power by, among other things, deterring those activities.

Reference 9 - 0.10% Coverage

Deterring cybercrime requires a credible threat that perpetrators will be identified, apprehended, and brought to justice.

Reference 10 - 0.21% Coverage

The United States Government will promote implementation and   
P I L L A R I I : PROM O T E A M E R I C A N PRO S P E R I T Y   
continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem.

Reference 11 - 0.16% Coverage

Identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace.

Reference 12 - 0.05% Coverage

Attribute and Deter Unacceptable Behavior in Cyberspace

Reference 13 - 0.11% Coverage

All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States.

Reference 14 - 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 15 - 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 16 - 0.20% Coverage

The 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 17 - 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 18 - 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 19 - 0.16% Coverage

Building partner cyber capacity will empower international   
partners to implement policies and practices which allow them to be effective partners in the United States-led Cyber Deterrence Initiative

Reference 20 - 0.07% Coverage

Partners can also help detect, deter, and defeat those shared threats in cyberspace.