Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 36 references coded [ 0.48% Coverage]

Reference 1 - 0.02% Coverage

Other intrusions threaten to damage portions of our critical infrastructure

Reference 2 - 0.01% Coverage

response and recovery

Reference 3 - 0.01% Coverage

deterrence

Reference 4 - 0.04% Coverage

The status quo is no longer acceptable. The United States must signal to the world that it is serious about addressing this challenge with strong leadership and vision

Reference 5 - 0.01% Coverage

territorial jurisdiction,

Reference 6 - 0.01% Coverage

overeign responsibility

Reference 7 - 0.01% Coverage

use of force.

Reference 8 - 0.01% Coverage

deterrence,

Reference 9 - 0.01% Coverage

military capabilities

Reference 10 - 0.05% Coverage

Anchoring and elevating leadership for cybersecurity-related policies at the White House signals to the United States and the international community that we are serious about cybersecurity.

Reference 11 - 0.01% Coverage

threats

Reference 12 - 0.01% Coverage

develop U.S. operational capabilities in cyberspace.

Reference 13 - 0.01% Coverage

integrate capabilities,

Reference 14 - 0.01% Coverage

uneven capabilities across various groups,

Reference 15 - 0.01% Coverage

and use of force.

References 16-17 - 0.02% Coverage

prevent, and respond to significant cybersecurity incidents

Reference 18 - 0.02% Coverage

apply technical capabilities to the defense of the national infrastructure

Reference 19 - 0.02% Coverage

help the Federal government prevent as well as detect malicious behavior.

Reference 20 - 0.01% Coverage

capability

Reference 21 - 0.02% Coverage

pilot deployments of intrusion detection and prevention systems for the benefit of federal networks

Reference 22 - 0.01% Coverage

prevention

Reference 23 - 0.03% Coverage

The U.S. Government should invest in processes, technologies, and infrastructure that will help prevent cyber incidents

Reference 24 - 0.01% Coverage

preventing,

Reference 25 - 0.02% Coverage

Information is key to preventing, detecting, and responding to cyber incidents

References 26-28 - 0.07% Coverage

The strategy also must include prevention, mitigation, and response against threats to or subversion of the people who operate and benefit from the infrastructure, the processes that run or take advantage of the infrastructure, and the supply chains used to build and maintain the infrastructure

Reference 29 - 0.01% Coverage

capabilities

References 30-31 - 0.03% Coverage

Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.

Reference 32 - 0.01% Coverage

deter,

Reference 33 - 0.01% Coverage

prevent,

Reference 34 - 0.02% Coverage

nsure U.S. capabilities to operate in cyberspace in support of national goals;

Reference 35 - 0.01% Coverage

capabilities

Reference 36 - 0.04% Coverage

Capacity Building: Encompasses the overall scale of resources, activities, and capabilities required to become a more cyber-competent nation.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 55 references coded [ 1.54% Coverage]

Reference 1 - 0.01% Coverage

The Strategic Environment—The World as It Is

Reference 2 - 0.01% Coverage

Use of Force

Reference 3 - 0.01% Coverage

an unmatched military

Reference 4 - 0.01% Coverage

determination to deter aggression

Reference 5 - 0.02% Coverage

prevent the proliferation of the world’s most dangerous weapons

Reference 6 - 0.01% Coverage

facing consequences when they do not.

Reference 7 - 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.

Reference 8 - 0.06% Coverage

there is no greater threat to the American people than weapons of mass destruction, particularly the danger posed by the pursuit of nuclear weapons by violent extremists and their proliferation to additional states.

Reference 9 - 0.02% Coverage

ensuring the reliability and effectiveness of our deterrent

Reference 10 - 0.03% Coverage

We must maintain our military’s conventional superiority, while enhancing its capacity to defeat asymmetric threats

Reference 11 - 0.03% Coverage

drew a swift and forceful response from the United States and our allies and partners in Afghanistan

Reference 12 - 0.01% Coverage

most powerful military,

References 13-14 - 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

References 15-17 - 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 18 - 0.02% Coverage

deterring and defeating aggression in anti-access environments

Reference 19 - 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 20 - 0.07% Coverage

we embrace America’s unique responsibility to promote international security—a responsibility that flows from our commitments to allies, our leading role in supporting a just and sustainable international order, and our unmatched military capabilities.

References 21-22 - 0.02% Coverage

We maintain superior capabilities to deter and defeat adaptive enemies and

Reference 23 - 0.03% Coverage

to ensure the credibility of security partnerships that are fundamental to regional and global security.

Reference 24 - 0.04% Coverage

our military continues to underpin our national security and global leadership, and when we use it appropriately, our security and leadership is reinforced

References 25-26 - 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.

References 27-29 - 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 30 - 0.05% Coverage

We must deny these groups the ability to conduct operational plotting from any locale, or to recruit, train, and position operatives, including those from Europe and North America.

Reference 31 - 0.03% Coverage

In Afghanistan, we must deny al-Qa’ida a safe haven, deny the Taliban the ability to overthrow the government

Reference 32 - 0.01% Coverage

Use of Force

Reference 33 - 0.02% Coverage

mitigating where possible the need for the use of force.

References 34-35 - 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 36 - 0.05% Coverage

While the use of force is sometimes necessary, we will exhaust other options before war whenever we can, and carefully weigh the costs and risks of action against the costs and risks of inaction

Reference 37 - 0.06% Coverage

When force is necessary, we will continue to do so in a way that reflects our values and strengthens our legitimacy, and we will seek broad international support, working with such institutions as NATO and the U.N. Security Council.

Reference 38 - 0.05% Coverage

The United States must reserve the right to act unilaterally if necessary to defend our nation and our interests, yet we will also seek to adhere to standards that govern the use of force

Reference 39 - 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 40 - 0.03% Coverage

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

Reference 41 - 0.01% Coverage

response to cyber attacks

Reference 42 - 0.03% Coverage

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

References 43-44 - 0.02% Coverage

Deterring Threats to the International Financial System

Reference 45 - 0.04% Coverage

Our strategy to attack these networks must respond in kind and target their illicit resources and access to the global financial system through financial measures,

Reference 46 - 0.02% Coverage

depends in part on the capabilities of America’s Armed Forces.

References 47-48 - 0.07% Coverage

We will continue to reassure our allies and partners by retaining our ability to bring precise, sustained, and effective capabilities to bear against a wide range of military threats and decisively defeat the forces of hostile regional powers

References 49-50 - 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 51 - 0.01% Coverage

deter vital threats

Reference 52 - 0.05% Coverage

We will monitor China’s military modernization program and prepare accordingly to ensure that U.S. interests and allies, regionally and globally, are not negatively affected.

References 53-54 - 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

Reference 55 - 0.08% Coverage

We must also safeguard the sea, air, and space domains from those who would deny access or use them for hostile purposes. This includes keeping strategic straits and vital sea lanes open, improving the early detection of emerging maritime threats, denying adversaries hostile use of the air domain

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 16 references coded [ 3.37% Coverage]

Reference 1 - 0.15% Coverage

t cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its missio

Reference 2 - 0.03% Coverage

d cyberspace capabilitie

Reference 3 - 0.16% Coverage

Cyber Threats   
“The very technologies that empower us to lead and create also empower those who would disrupt and destroy.”

Reference 4 - 0.33% Coverage

In developing its strategy for operating in cyberspace, DoD is focused on a number of central aspects of the cyber threat; these include external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD‘s operational ability.

Reference 5 - 0.23% Coverage

Moreover, this threat continues to evolve as evidence grows of adversaries focusing on the development of increasingly sophisticated and potentially dangerous capabilities.

Reference 6 - 0.15% Coverage

the rapidly evolving threat landscape presents a complex and vital challenge for national and economic security.

Reference 7 - 0.15% Coverage

denial of access or service that affects the availability of networks, information, or network-enabled resources

Reference 8 - 0.24% Coverage

As directed by the National Security Strategy, DoD must ensure that it has the necessary capabilities to operate effectively in all domains- air, land, maritime, space, and cyberspace

Reference 9 - 0.24% Coverage

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

References 10-11 - 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 12 - 0.57% Coverage

Active cyber defense is DoD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems.

Reference 13 - 0.21% Coverage

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

Reference 14 - 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 15 - 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 16 - 0.09% Coverage

create coalitions to deter malicious activities in cyberspace.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 68 references coded [ 6.46% Coverage]

Reference 1 - 0.03% Coverage

The ongoing shifts in relative power

Reference 2 - 0.07% Coverage

While the strength of our military will continue to underpin national security,

Reference 3 - 0.02% Coverage

military capabilities

Reference 4 - 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 5 - 0.04% Coverage

defend against and defeat threats to our homeland.

Reference 6 - 0.08% Coverage

Our foremost priority is the security of the American people, our territory, and our way of life.

Reference 7 - 0.09% Coverage

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

References 8-9 - 0.12% Coverage

potential adversaries who underestimate our continued military strength and will to protect our national interests do so at their peril.

Reference 10 - 0.09% Coverage

The United States will remain the foremost economic and military power for the foreseeable future

Reference 11 - 0.05% Coverage

expansion of its interests within and beyond the region.

Reference 12 - 0.08% Coverage

Other states in Asia, too, are becoming more militarily capable as they grow more prosperous.

Reference 13 - 0.16% Coverage

In the Middle East, a nuclear armed Iran could set off a cascade of states in the region seeking nuclear parity or increased conventional capabilities; that could lead to regional conflict.

Reference 14 - 0.05% Coverage

platforms that challenge our ability to project power

Reference 15 - 0.04% Coverage

relative ease of developing potent capabilities.

Reference 16 - 0.01% Coverage

deterrence

Reference 17 - 0.10% Coverage

requires America’s Joint Force possesses the reach, resolve, and ability to project decisive military power.

Reference 18 - 0.10% Coverage

There are no more vital interests than the security of the American people, our territory, and our way of life.

References 19-20 - 0.09% Coverage

defeat al Qaida and its affiliates in Afghanistan and Pakistan and prevent their return to either country

Reference 21 - 0.07% Coverage

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

Reference 22 - 0.02% Coverage

difficult to deter directly

Reference 23 - 0.10% Coverage

they make cost/benefit calculations and are dependent on states and other stakeholders we are capable of influencing.

References 24-25 - 0.16% Coverage

When directed, we will provide capabilities to hold accountable any government or entity complicit in attacks against the United States or allies to raise the cost of their support.

References 26-27 - 0.17% Coverage

We will, on order, be prepared to respond to any attack across the full spectrum of military capabilities with an appropriate and measured response at a time and place of our Nation’s choosing.

References 28-29 - 0.02% Coverage

Deter and Defeat Aggression

Reference 30 - 0.06% Coverage

Preventing wars is as important as winning them, and far less costly

References 31-33 - 0.10% Coverage

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

Reference 34 - 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.

References 35-36 - 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.

References 37-41 - 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.

References 42-43 - 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 44 - 0.15% Coverage

Defeat Aggression: The core task of our   
Armed Forces remains to defend our Nation and win its wars. To do so, we must provide capabilities to defeat adversary aggression.

Reference 45 - 0.10% Coverage

Military force, at times, may be necessary to defend our Nation and allies or to preserve broader peace and security.

Reference 46 - 0.13% Coverage

Defeating adversary aggression will require the Joint Force to support National approaches to counter anti-access and area-denial strategies

Reference 47 - 0.27% Coverage

core military competencies include complementary, multi-domain power   
A prosperous and interconnected world   
requires a stable and secure environment, the absence of territorial aggression or   
conflict between states, and reliable access to resources and cyberspace for stable markets.   
8   
projection,

References 48-50 - 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.

References 51-52 - 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 53 - 0.10% Coverage

Cyberspace – Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains

Reference 54 - 0.19% Coverage

The disposition, strength, and readiness of our Joint Force form a global defense posture that provides unsurpassed capabilities allowing us, uniquely, to lead efforts that strengthen security across all regions

Reference 55 - 0.06% Coverage

shape our joint force to be able to aggregate capabilities quickly

Reference 56 - 0.05% Coverage

safeguarding our economic and security interests worldwide.

References 57-58 - 0.11% Coverage

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

Reference 59 - 0.04% Coverage

preventing Iran from acquiring nuclear arms.

Reference 60 - 0.14% Coverage

We will continue to monitor carefully China’s military developments and the implications those developments have on the military balance in the Taiwan Strait

Reference 61 - 0.23% Coverage

To safeguard U.S. and partner nation interests, we will be prepared to demonstrate the will and commit the resources needed to oppose any nation’s actions that jeopardize access to and use of the global commons and cyberspace, or that threaten the security of our allies.

Reference 62 - 0.15% Coverage

Capabilities – Our strategy, forged in war, is focused on fielding modular, adaptive, general purpose forces that can be employed in the full range of military operations.

References 63-65 - 0.30% Coverage

Joint Forces will secure the ‘.mil’ domain, requiring a resilient DoD cyberspace architecture that employs a combination of detection, deterrence, denial, and multi-layered defense. We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with less cost and lower collateral impact.

Reference 66 - 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 67 - 0.12% Coverage

Readiness is the ability to provide and integrate capabilities required by Combatant Commanders to execute their assigned missions.

Reference 68 - 0.09% Coverage

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

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 63 references coded [ 1.85% Coverage]

Reference 1 - 0.01% Coverage

Dissuading

Reference 2 - 0.01% Coverage

Deterring

Reference 3 - 0.01% Coverage

consequences

Reference 4 - 0.03% Coverage

distant and often-fraught borders~

Reference 5 - 0.03% Coverage

threaten users’ confidence in online commerce

Reference 6 - 0.05% Coverage

The theft of intellectual property threatens national competitiveness

Reference 7 - 0.11% Coverage

Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace~

Reference 8 - 0.01% Coverage

interests

Reference 9 - 0.01% Coverage

threats

Reference 10 - 0.01% Coverage

threats

Reference 11 - 0.01% Coverage

threats

Reference 12 - 0.02% Coverage

serves national interests

Reference 13 - 0.03% Coverage

because of a few nations’ political interests~

Reference 14 - 0.02% Coverage

and appropriate deterrence~

Reference 15 - 0.08% Coverage

increasing evidence that governments are seeking to exercise traditional national power through cyberspace~

Reference 16 - 0.02% Coverage

deny criminals safe havens,

Reference 17 - 0.02% Coverage

national security interests,

Reference 18 - 0.01% Coverage

Dissuading

Reference 19 - 0.01% Coverage

Deterring

Reference 20 - 0.09% Coverage

The United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies

Reference 21 - 0.01% Coverage

dissuade

Reference 22 - 0.01% Coverage

deter

Reference 23 - 0.01% Coverage

threaten

Reference 24 - 0.03% Coverage

a range of credible response options~

Reference 25 - 0.01% Coverage

dissuading

Reference 26 - 0.02% Coverage

deterring malicious actors,

Reference 27 - 0.01% Coverage

Dissuasion

Reference 28 - 0.06% Coverage

Protecting networks of such great value requires robust defensive capabilities~

Reference 29 - 0.02% Coverage

early warning capabilities~

Reference 30 - 0.02% Coverage

incident response capabilities

Reference 31 - 0.01% Coverage

Deterrence

Reference 32 - 0.01% Coverage

borders~

Reference 33 - 0.03% Coverage

hreaten our national and economic security,

Reference 34 - 0.01% Coverage

domestic deterrence

Reference 35 - 0.07% Coverage

the United States will respond to hostile acts in cyberspace as we would to any other threat to our country~

Reference 36 - 0.10% Coverage

certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners~

Reference 37 - 0.01% Coverage

our interests~

Reference 38 - 0.01% Coverage

military force

Reference 39 - 0.06% Coverage

will carefully weigh the costs and risks of action against the costs of inaction

References 40-41 - 0.04% Coverage

confront threats emanating from within their borders

Reference 42 - 0.01% Coverage

threaten

Reference 43 - 0.01% Coverage

capabilities

Reference 44 - 0.01% Coverage

threaten

Reference 45 - 0.15% Coverage

As we continue to build and enhance our own response capabilities, we will work with other countries to expand the international networks that support greater global situational awareness and incident response

Reference 46 - 0.02% Coverage

We will expand these capabilities

References 47-48 - 0.05% Coverage

focusing on preventing crime and catching and punishing offenders

Reference 49 - 0.09% Coverage

Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.

Reference 50 - 0.04% Coverage

Preventing terrorists from enhancing capabilities

Reference 51 - 0.01% Coverage

interests

Reference 52 - 0.01% Coverage

threatened,

Reference 53 - 0.06% Coverage

the United States has a compelling interest in defending its vital national assets,

Reference 54 - 0.03% Coverage

confront potential threats in cyberspace.

References 55-56 - 0.13% Coverage

Such military alliances and partnerships will bolster our collective deterrence capabilities and strengthen our ability to defend the United States against state and non-state actors~

Reference 57 - 0.01% Coverage

capabilities,

Reference 58 - 0.02% Coverage

leverage capabilities

Reference 59 - 0.03% Coverage

deter malicious activities in cyberspace

Reference 60 - 0.04% Coverage

supporting national capabilities for incident management;

Reference 61 - 0.01% Coverage

Criminal threats

Reference 62 - 0.01% Coverage

threaten,

Reference 63 - 0.02% Coverage

address real cyberspace threats,

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 61 references coded [ 0.54% Coverage]

Reference 1 - 0.01% Coverage

Roles of Military Power

Reference 2 - 0.01% Coverage

Deter

Reference 3 - 0.01% Coverage

Defeat Aggression

Reference 4 - 0.01% Coverage

Prevent Proliferation

Reference 5 - 0.01% Coverage

Counter Weapons of Mass Destruction

Reference 6 - 0.02% Coverage

The mission of the Department of Defense is to protect the American people and advance our nation’s interests.

References 7-8 - 0.01% Coverage

renewed efforts to disrupt, dismantle, and defeat Al Qaeda and the Taliban

Reference 9 - 0.03% Coverage

Above all, the United States and its allies and partners remain engaged in a broader war—a multifaceted political, military and moral struggle—against Al Qaeda and its allies around the world.

Reference 10 - 0.03% Coverage

First, to further rebalance the capabilities of America’s Armed Forces to prevail in today’s wars, while building the capabilities needed to deal with future threats.

Reference 11 - 0.01% Coverage

capabilities

Reference 12 - 0.01% Coverage

military power

Reference 13 - 0.01% Coverage

prevent harmful arms races.

Reference 14 - 0.01% Coverage

direct physical threat to the United States

Reference 15 - 0.01% Coverage

require armed forces with unmatched capabilities

Reference 16 - 0.01% Coverage

prevent

Reference 17 - 0.01% Coverage

deter conflict

Reference 18 - 0.01% Coverage

prepare to defeat adversaries

Reference 19 - 0.03% Coverage

These priorities shape not only considerations on the capabilities our Armed Forces need but also the aggregate capacity required to accomplish their missions now and in the future.

Reference 20 - 0.01% Coverage

defeat

Reference 21 - 0.01% Coverage

defeat

Reference 22 - 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.

References 23-24 - 0.01% Coverage

U.S. capabilities to deny adversaries’ objectives

Reference 25 - 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.

References 26-28 - 0.02% Coverage

the Department’s prevent-and-deter activities will be focused on ensuring a defense in depth of the United States;

Reference 29 - 0.01% Coverage

and deterring other potential major adversaries

Reference 30 - 0.01% Coverage

Prepare to defeat adversaries

Reference 31 - 0.01% Coverage

deterrence

Reference 32 - 0.01% Coverage

adversaries challenge our interests with the threat

Reference 33 - 0.01% Coverage

use of force,

Reference 34 - 0.01% Coverage

supporting a response to an attack

Reference 35 - 0.01% Coverage

defeating aggression by adversary states

Reference 36 - 0.01% Coverage

deterrence

Reference 37 - 0.01% Coverage

Enhance capabilities for domain awareness

Reference 38 - 0.01% Coverage

Accelerate the development of standoff radiological/nuclear detection capabilities

Reference 39 - 0.01% Coverage

Enhance domestic capabilities

Reference 40 - 0.02% Coverage

Strengthen and institutionalize general purpose force capabilities for security force assistance;

Reference 41 - 0.01% Coverage

critical capabilities

References 42-43 - 0.01% Coverage

Deter and defeat aggression in anti-access environments

Reference 44 - 0.01% Coverage

deter,

Reference 45 - 0.01% Coverage

defeat aggression

References 46-47 - 0.04% Coverage

In the absence of dominant U.S. power projection capabilities, the integrity of U.S. alliances and security partnerships could be called into question, reducing U.S. security and influence and increasing the possibility of conflict.

Reference 48 - 0.01% Coverage

Defeat enemy sensors and engagement systems;

Reference 49 - 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 50 - 0.01% Coverage

The security environment demands improved capabilities to counter threats in cyberspace.

Reference 51 - 0.01% Coverage

DoD must actively defend its networks.

Reference 52 - 0.01% Coverage

capabilities

Reference 53 - 0.02% Coverage

U.S. naval forces likewise will continue to be capable of robust forward presence and power projection operations,

Reference 54 - 0.01% Coverage

capabilities

Reference 55 - 0.01% Coverage

deter

Reference 56 - 0.01% Coverage

defeat adversaries

Reference 57 - 0.01% Coverage

capabilities.

Reference 58 - 0.01% Coverage

capabilities

Reference 59 - 0.01% Coverage

capabilities,

Reference 60 - 0.01% Coverage

recommendations regarding capability development

Reference 61 - 0.01% Coverage

the need for enhancements to key capabilities across a wide range of missions

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review CLEAN - § 42 references coded [ 1.49% Coverage]

Reference 1 - 0.01% Coverage

our military’s human capital and technological edge

References 2-3 - 0.02% Coverage

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

Reference 4 - 0.01% Coverage

deter adversaries,

Reference 5 - 0.01% Coverage

Project power and win decisively,

Reference 6 - 0.02% Coverage

defeat aggression, disrupt and destroy terrorist networks

Reference 7 - 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 8 - 0.05% Coverage

It also supports our ability to project power by communicating to potential nuclear-armed adversaries that they cannot escalate their way out of failed conventional aggression.

Reference 9 - 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.

References 10-11 - 0.08% Coverage

Our ability to project forces to combat terrorism in places as far away as Yemen, Afghanistan, and Mali – and to build capacity to help partners counter terrorism and counter the proliferation of weapons of mass destruction (WMD) – reduces the likelihood that these threats could find their way to U.S. shores.

Reference 12 - 0.10% Coverage

We are identifying new presence paradigms, including potentially positioning additional forward deployed naval forces in critical areas, and deploying new combinations of ships, aviation assets, regionally aligned or rotational ground forces, and crisis response forces, all with the intention of maximizing effects while minimizing costs.

Reference 13 - 0.02% Coverage

deterring aggression and assuring allies through forward presence and engagement.

References 14-17 - 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 18 - 0.05% Coverage

The President’s Budget provides the resources to build and sustain the capabilities to conduct these operations, although at increased levels of risk for some missions.

References 19-21 - 0.02% Coverage

With the President’s Budget, our military will be able to defeat or deny any aggressor.

Reference 22 - 0.03% Coverage

a smaller force strains our ability to simultaneously respond to more than one major contingency at a time.

Reference 23 - 0.03% Coverage

We will also protect the ability to regenerate capabilities that might be needed to meet future demands.

References 24-25 - 0.07% Coverage

The Joint Force must also be prepared to battle increasingly sophisticated adversaries who could employ advanced warfighting capabilities while simultaneously attempting to deny U.S. forces the advantages they currently enjoy in space and cyberspace.

Reference 26 - 0.07% Coverage

The Department is taking steps to ensure that progress continues in areas most critical to meeting future challenges such as full-spectrum cyberspace capabilities and where the potential for game-changing breakthroughs appears most promising.

Reference 27 - 0.04% Coverage

retaining robust capability for direct action, including intelligence, persistent surveillance, precision strike, and Special Operations Forces.

Reference 28 - 0.02% Coverage

We will remain focused on countering WMD, which undermine global security.

Reference 29 - 0.06% Coverage

We will continue our contributions to the U.S. rebalance to the Asia-Pacific region, seeking to preserve peace and stability in a region that is increasingly central to U.S. political, economic, and security interests.

Reference 30 - 0.06% Coverage

As part of our broader efforts for stability in the Asia-Pacific region, the United States will maintain a robust footprint in Northeast Asia while enhancing our presence in Oceania and Southeast Asia.

References 31-32 - 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 33 - 0.02% Coverage

while making sure that our military capabilities evolve to meet new threats.

Reference 34 - 0.02% Coverage

Rebalancing capability, capacity, and readiness within the Joint Force.

Reference 35 - 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 36 - 0.04% Coverage

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

Reference 37 - 0.02% Coverage

rebalance investments toward systems that are operationally responsive

Reference 38 - 0.05% Coverage

Reductions in capacity and capability would significantly challenge our ability to respond to strategic surprise, particularly those requiring large numbers of modern forces.

Reference 39 - 0.07% Coverage

The centerpiece of the Department of Defense commitment to the U.S. Government’s rebalance to the Asia-Pacific region continues to be our efforts to modernize and enhance our security alliances with Australia, Japan, the ROK, the Philippines, and Thailand.

Reference 40 - 0.04% Coverage

We will continue efforts to help stabilize Central and Southwest Asia and deepen our engagement in the Indian Ocean region to bolster our rebalance to Asia

Reference 41 - 0.10% Coverage

Asia-Pacific. Supporting the broader U.S. rebalance to the region, the United States will maintain a robust footprint in Northeast Asia while enhancing our presence in Oceania, Southeast Asia, and the Indian Ocean. By 2020, 60 percent of U.S. Navy assets will be stationed in the Pacific, including enhancements to our critical naval presence in Japan.

Reference 42 - 0.06% Coverage

Under sequestration-level cuts, the United States would continue prioritizing efforts to sustain and complete our rebalance to the Asia-Pacific region, including our focus on ensuring strong relations with our allies and partners.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 DOD Cyber Strategy CLEAN - § 5 references coded [ 0.29% Coverage]

References 1-2 - 0.09% Coverage

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

Reference 3 - 0.06% Coverage

North Korea accompanied their cyberattacks with coercion, intimidation, and the threat of terrorism.

Reference 4 - 0.06% Coverage

The North Korean attack on Sony was one of the most destructive cyberattacks on a U.S. entity to date.

Reference 5 - 0.09% Coverage

The attack further spurred an already ongoing national discussion about the nature of the cyber threat and the need for improved cybersecurity.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 114 references coded [ 10.56% Coverage]

Reference 1 - 0.20% Coverage

Since the last National Military Strategy was published in 2011, global disorder has significantly increased while some of our comparative military advantage has begun to erode.

Reference 2 - 0.14% Coverage

This National Military Strategy describes how we will employ our military forces to   
protect and advance our national interests.

Reference 3 - 0.18% Coverage

Success will increasingly depend on how well our military instrument can support the other instruments of power and enable our network of allies and partners.

Reference 4 - 0.20% Coverage

But it also asserts that the application of the military instrument of power against state   
threats is very different than the application of military power against non-state threats.

References 5-6 - 0.13% Coverage

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

Reference 7 - 0.11% Coverage

Concurrently, we are leading multiple coalition efforts to disrupt, degrade, and defeat VEOs.

Reference 8 - 0.16% Coverage

sustain the capabilities, capacity, and readiness required to prevail in conflicts that may differ significantly in scope, scale, and duration.

Reference 9 - 0.11% Coverage

States, meanwhile, are using information sharing to develop advanced capabilities of their own.

Reference 10 - 0.15% Coverage

It is a state-sponsor of terrorism that has undermined stability in many nations, including Israel, Lebanon, Iraq, Syria, and Yemen.

Reference 11 - 0.11% Coverage

North Korea also has conducted cyber attacks, including causing major damage to a U.S. corporation.

Reference 12 - 0.17% Coverage

China has responded with aggressive land reclamation efforts that will allow it to position military forces astride vital international sea lanes.

Reference 13 - 0.11% Coverage

It must provide a full range of military options for addressing both revisionist states and VEOs

Reference 14 - 0.21% Coverage

Of particular concern are the proliferation of ballistic missiles, precision strike technologies, unmanned systems, space and cyber capabilities, and weapons of mass destruction (WMD)

Reference 15 - 0.17% Coverage

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

References 16-17 - 0.18% Coverage

attacks on our communications and sensing systems could occur with little to no warning, impacting our ability to assess, coordinate, communicate, and respond.

Reference 18 - 0.08% Coverage

The U.S. military’s purpose is to protect our Nation and win our wars.

Reference 19 - 0.14% Coverage

We do this   
through military operations to defend the homeland, build security globally, and project power and win decisively.

Reference 20 - 0.03% Coverage

The survival of the Nation.

Reference 21 - 0.07% Coverage

The prevention of catastrophic attack against U.S. territory.

References 22-24 - 0.05% Coverage

Deter, deny, and defeat state adversaries.

Reference 25 - 0.07% Coverage

Disrupt, degrade, and defeat violent extremist organizations.

Reference 26 - 0.03% Coverage

the survival of the Nation

Reference 27 - 0.07% Coverage

the   
prevention of catastrophic attack against U.S. territory

Reference 28 - 0.19% Coverage

NSIs guide military leaders in providing recommendations on when and where our Nation should use military force, the type and degree of force to employ, and at what cost.

References 29-31 - 0.05% Coverage

to deter, deny, and defeat state adversaries

Reference 32 - 0.04% Coverage

to disrupt, degrade, and defeat VEOs;

Reference 33 - 0.17% Coverage

sustaining the capabilities, capacity, and readiness required to prevail in conflicts that may differ significantly in scope, scale, and duration.

Reference 34 - 0.09% Coverage

deter aggression and assure allies through forward presence and engagement.

References 35-38 - 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.

References 39-41 - 0.05% Coverage

Deter, Deny, and Defeat State Adversaries

Reference 42 - 0.22% Coverage

The U.S. military is the world’s preeminent Joint Force. It supports the Nation by   
providing a full range of options to protect the homeland and our interests while assuring the security of our allies.

References 43-45 - 0.13% Coverage

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

Reference 46 - 0.13% Coverage

Forward deployed, rotational, and globally responsive forces regularly demonstrate the capability and will to act.

References 47-48 - 0.05% Coverage

Should deterrence fail to prevent aggression,

References 49-50 - 0.09% Coverage

the U.S. military stands ready to project power to deny an adversary’s objectives

Reference 51 - 0.13% Coverage

decisively defeat any actor that threatens the U.S. homeland, our national interests, or our allies and partners.

References 52-54 - 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 55 - 0.10% Coverage

In case of aggression, denying adversaries their goals will be an immediate objective.

Reference 56 - 0.17% Coverage

Timely interagency planning and coordination also will be leveraged to develop holistic options that serve to integrate all elements of national power.

References 57-58 - 0.14% Coverage

Should any actor directly attack the United States or our interests, the U.S. military will   
take action to defend our Nation.

References 59-60 - 0.15% Coverage

We are prepared to project power across all domains to stop aggression and win our Nation’s wars by decisively defeating adversaries.

Reference 61 - 0.11% Coverage

While we prefer to act in concert with others, we will act unilaterally if the situation demands.

References 62-64 - 0.21% Coverage

In the event of an attack, the U.S. military will respond by inflicting damage of such magnitude as to compel the adversary to cease hostilities or render it incapable of further aggression.

Reference 65 - 0.11% Coverage

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

Reference 66 - 0.04% Coverage

Disrupt, Degrade, and Defeat VEOs

Reference 67 - 0.18% Coverage

Today, the United States is leading a broad coalition of nations to defeat VEOs in   
multiple regions by applying pressure across the full extent of their networks.

Reference 68 - 0.03% Coverage

ultimately defeat them

Reference 69 - 0.20% Coverage

In support of these efforts, we are widely distributing U.S. military forces and leveraging globally integrated command and control processes to enable transregional operations.

Reference 70 - 0.09% Coverage

Credible regional partners are vital to sustaining counter-VEO campaigns.

References 71-72 - 0.17% Coverage

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

Reference 73 - 0.24% Coverage

The presence of U.S. military forces in key locations around the world underpins the   
international order and provides opportunities to engage with other countries while positioning forces to respond to crises.

Reference 74 - 0.18% Coverage

Therefore we will press forward with the rebalance to the AsiaPacific region, placing our most advanced capabilities and greater capacity in that vital theater.

Reference 75 - 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 76 - 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 77 - 0.12% Coverage

They also develop partner military capabilities for self-defense and support to multinational operations.

Reference 78 - 0.06% Coverage

Maintain a Secure and Effective Nuclear Deterrent.

References 79-81 - 0.16% Coverage

U.S. strategic forces are kept at the   
highest state of readiness, always prepared to respond to threats to the homeland and our vital interests.

Reference 82 - 0.12% Coverage

These capabilities will better defend us against both high technology threats and terrorist dangers.

Reference 83 - 0.02% Coverage

Defeat an Adversary.

References 84-87 - 0.33% Coverage

In the event of an attack against the United States or one of its   
allies, the U.S. military along with allies and partners will project power across multiple domains to decisively defeat the adversary by compelling it to cease hostilities or render its military incapable of further aggression.

Reference 88 - 0.09% Coverage

positions the Joint Force to execute emergency actions in response to a crisis.

Reference 89 - 0.06% Coverage

Maintain a secure and effective nuclear deterrent

Reference 90 - 0.02% Coverage

Defeat an adversary

Reference 91 - 0.04% Coverage

Counter weapons of mass destruction

Reference 92 - 0.04% Coverage

Deny an adversary’s objectives

Reference 93 - 0.07% Coverage

Respond to crisis and conduct limited contingency operations

References 94-95 - 0.15% Coverage

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

Reference 96 - 0.14% Coverage

This puts emphasis on maintaining highly-ready, forward-deployed forces, well trained and equipped surge forces at home

Reference 97 - 0.09% Coverage

These capabilities provide the means to curtail crises before they can escalate.

Reference 98 - 0.07% Coverage

Respond to Crisis and Conduct Limited Contingency Operations.

Reference 99 - 0.12% Coverage

Another form of   
power projection is teaming with partners to conduct limited contingency operations.

References 100-101 - 0.15% Coverage

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

Reference 102 - 0.23% Coverage

To execute this strategy, the U.S. military requires a sufficient level of investment in capacity, capabilities, and readiness so that when our Nation calls, our military remains ready to deliver success.

Reference 103 - 0.04% Coverage

advanced military capabilities

Reference 104 - 0.06% Coverage

the effect of applying all instruments of national power

Reference 105 - 0.06% Coverage

Anticipate and adapt to surprise, uncertainty, and chaos

Reference 106 - 0.14% Coverage

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

Reference 107 - 0.13% Coverage

The ability to quickly aggregate and disaggregate   
forces anywhere in the world is the essence of global agility.

Reference 108 - 0.02% Coverage

deter adversaries

Reference 109 - 0.22% Coverage

We are positioning forces where they are most needed, exemplified by our rebalance to the Asia-Pacific region as well as our evolving presence in Europe, the Middle East, Latin America, and Africa.

Reference 110 - 0.11% Coverage

We are in the process of defining the next set   
of interoperability standards for future capabilities.

References 111-112 - 0.12% Coverage

Future capabilities must sustain our   
ability to defend the homeland and project military power globally.

Reference 113 - 0.12% Coverage

We are modernizing our nuclear enterprise and working to protect our Nation against asymmetric threats.

Reference 114 - 0.20% Coverage

As we develop new capabilities to counter threats along the continuum of conflict, we   
also must procure sufficient capacity and readiness to sustain our global responsibilities.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 74 references coded [ 3.17% Coverage]

Reference 1 - 0.05% Coverage

We possess a military whose might, technology, and geostrategic reach is unrivaled in human history.

References 2-3 - 0.06% Coverage

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

References 4-5 - 0.05% Coverage

That is why I have worked to ensure that America has the capabilities we need to respond to threats abroad

References 6-7 - 0.05% Coverage

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

References 8-9 - 0.06% Coverage

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

Reference 10 - 0.02% Coverage

Our military might is unrivaled.

Reference 11 - 0.06% Coverage

Our military will remain ready to defend our enduring national interests while providing essential leverage for our diplomacy

Reference 12 - 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 13 - 0.05% Coverage

We embrace our responsibilities for underwriting international security because it serves our interests

Reference 14 - 0.02% Coverage

threats that are truly global.

Reference 15 - 0.04% Coverage

requires a global security posture in which our unique capabilities are employed

References 16-17 - 0.02% Coverage

acting decisively to defeat direct threats

Reference 18 - 0.05% Coverage

we will focus on building the capacity of others to prevent the causes and consequences of conflict

Reference 19 - 0.03% Coverage

A strong military is the bedrock of our national security

References 20-21 - 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 22 - 0.03% Coverage

deter aggression through forward presence and engagement.

References 23-27 - 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 28 - 0.04% Coverage

Although our military will be smaller, it must remain dominant in every domain.

Reference 29 - 0.04% Coverage

protect our investment in foundational capabilities like the nuclear deterrent

Reference 30 - 0.03% Coverage

We will be principled and selective in the use of force.

Reference 31 - 0.05% Coverage

The use of force should not be our first choice, but it will sometimes be the necessary choice.

References 32-34 - 0.11% Coverage

The United States will use military force, unilaterally if necessary, when our enduring interests demand it: when our people are threatened; when our livelihoods are at stake; and when the security of our allies is in danger.

References 35-37 - 0.05% Coverage

The threshold for military action is higher when our interests are not directly threatened

Reference 38 - 0.09% Coverage

In all cases, the decision to use force must reflect a clear mandate and feasible objectives, and we must ensure our actions are effective, just, and consistent with the rule of law.

References 39-40 - 0.13% 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. Whenever and wherever we use force, we will do so in a way that reflects our values and strengthens our legitimacy.

Reference 41 - 0.03% Coverage

We are more responsive and resilient when prevention fails

Reference 42 - 0.09% Coverage

we shifted away from a model of fighting costly, large-scale ground wars in Iraq and Afghanistan in which the United States—particularly our military—bore an enormous burden.

Reference 43 - 0.06% Coverage

increased efforts to prevent the growth of violent extremism and radicalization that drives increased threats

Reference 44 - 0.06% Coverage

when capture or other actions to disrupt the threat are not feasible, we will not hesitate to take decisive action.

Reference 45 - 0.04% Coverage

We have undertaken a comprehensive effort to degrade and ultimately defeat ISIL.

References 46-50 - 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 51 - 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 52 - 0.07% Coverage

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

References 53-54 - 0.08% Coverage

As countries increasingly derive benefits from space, we must join together to deal with threats posed by those who may wish to deny the peaceful use of outer space.

References 55-57 - 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 58 - 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 59 - 0.06% Coverage

On territorial disputes, particularly in Asia, we denounce coercion and assertive behaviors that threaten escalation

Reference 60 - 0.07% Coverage

In addition to being a key measure of power and influence in its own right, it underwrites our military strength and diplomatic influence.

Reference 61 - 0.06% Coverage

America’s energy revival is not only good for growth, it offers new buffers against the coercive use of energy by some

Reference 62 - 0.03% Coverage

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

Reference 63 - 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.

References 64-65 - 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 66 - 0.03% Coverage

we will manage competition from a position of strength

Reference 67 - 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

References 68-69 - 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 70 - 0.04% Coverage

prevent the development, proliferation, or use of weapons of mass destruction.

Reference 71 - 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 72 - 0.07% Coverage

It clarifies the purpose and promise of American power. It aims to advance our interests and values with initiative and from a position of strength.

References 73-74 - 0.05% Coverage

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

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 225 references coded [ 20.30% 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

References 4-5 - 0.02% Coverage

Deterrence by Denial

References 6-7 - 0.02% Coverage

Deterrence by Cost Imposition

Reference 8 - 0.05% Coverage

Measures to Impose Economic Costs on Malicious Cyber Actors

Reference 9 - 0.05% Coverage

Building Capabilities to Defend the Nation in Cyberspace

Reference 10 - 0.03% Coverage

Activities that Support Deterrence

References 11-12 - 0.07% Coverage

Bolstering “Whole-of-Government” and “Whole of Nation” Response Capabilities

Reference 13 - 0.04% Coverage

Declaratory Policy and Strategic Communications

Reference 14 - 0.02% Coverage

Intelligence Capabilities

References 15-16 - 0.26% Coverage

At the same time, cyber attacks and some kinds of malicious cyber activity2 – particularly those conducted by nation-states or highly capable non-state actors and which target critical infrastructures and key industries in the United States – can constitute a significant threat to U.S. national security and economic interests.

Reference 17 - 0.12% Coverage

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

References 18-19 - 0.16% Coverage

The United States Government is pursuing multifaceted policy efforts to leverage all instruments of national power to counter malicious cyber activity that poses significant threats to the nation

Reference 20 - 0.08% Coverage

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

References 21-22 - 0.20% Coverage

In taking this approach, the Administration will continually refine current capabilities and develop new ones that will raise the costs and reduce the benefits of conducting malicious cyber activity against the United States and its interests.

Reference 23 - 0.22% Coverage

For the purpose of this document, a cyber attack refers to an attempt to deny access to, disrupt, disable, degrade, destroy, or otherwise render inoperable computers, information or communications systems, networks, or physical or virtual systems controlled by computers.

References 24-26 - 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.

References 27-28 - 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 29 - 0.03% Coverage

What the United States Will Seek to Deter

References 30-33 - 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 34 - 0.02% Coverage

military command and control

Reference 35 - 0.07% Coverage

The following concerns represent priority areas to focus deterrence activities.

Reference 36 - 0.06% Coverage

we will adapt our priorities to new threats and geopolitical developments.

Reference 37 - 0.09% Coverage

the Administration is most concerned about threats that could cause wide-scale disruption, destruction

Reference 38 - 0.06% Coverage

Cyber attacks or other malicious cyber activity intended to cause casualties

Reference 39 - 0.23% Coverage

Cyber attacks or other malicious cyber activity intended to cause significant disruption to the normal functioning of U.S. society or government, including attacks against critical infrastructure that could damage systems used to provide key services4 to the public or the government.

References 40-42 - 0.21% Coverage

Cyber attacks or other malicious cyber activity that threatens the command and control of U.S. military forces, the freedom of maneuver of U.S. military forces, or the infrastructure on which the U.S. military relies to defend U.S. interests and commitments

Reference 43 - 0.09% Coverage

Malicious actors employ various tactics for attacking, exploiting, or disrupting networks, systems, and data.

Reference 44 - 0.16% Coverage

Although the full spectrum of operational capabilities requires resources, persistence, and access to technological expertise, none of these methods are solely within the purview of nation-states.

Reference 45 - 0.02% Coverage

Cyber Deterrence Strategies

Reference 46 - 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.

References 47-49 - 0.17% Coverage

Influence is achieved by credibly demonstrating the ability and willingness to deny benefits or impose costs to convince the adversary that restraint will result in better outcomes than will confrontation.

Reference 50 - 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.

References 51-52 - 0.22% Coverage

Today, the United States possesses dominant military capabilities, but is asymmetrically dependent on cyberspace and faces highly capable state and non-state adversaries that have the capability, expertise, and intent to conduct significant cyber attacks against us.

Reference 53 - 0.09% Coverage

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

Reference 54 - 0.14% Coverage

Complicating matters further, potential adversaries in cyberspace may not have equal capabilities and each side is unlikely to know the extent of the other’s capabilities.

Reference 55 - 0.01% Coverage

cyber attack

Reference 56 - 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 57 - 0.04% Coverage

Component Elements of U.S. Cyber Deterrence Policy

References 58-61 - 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.

References 62-63 - 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.

References 64-66 - 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.

References 67-69 - 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.

References 70-71 - 0.06% Coverage

The United States is also pursuing deterrence through cost imposition

References 72-74 - 0.13% Coverage

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

References 75-76 - 0.09% Coverage

United States Government’s ability and willingness to respond to cyber attacks through all necessary means

Reference 77 - 0.04% Coverage

conducting offensive and defensive cyber operations

Reference 78 - 0.10% Coverage

projecting power through air, land, sea, and space, and, after exhausting all available options, to use military force.

References 79-80 - 0.02% Coverage

Deterrence by Denial

References 81-83 - 0.20% Coverage

Pursuing defense, resiliency, and reconstitution initiatives to provide critical networks with a greater capability to prevent or minimize the impact of cyber attacks or other malicious cyber activity, and reconstitute rapidly if attacks succeed.

References 84-86 - 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.

References 87-88 - 0.23% Coverage

In particular, there should be certainty about the fact that, even in the face of sophisticated cyber threats, the United States can maintain robust defenses, ensure resilient networks and systems, and implement a robust response capability that can project power and secure U.S. interests.

Reference 89 - 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 90 - 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 91 - 0.28% Coverage

DHS and other elements of the United States Government have developed infrastructure and processes for disseminating specific and targeted cybersecurity threat information to the identified critical infrastructure owners and operators. This information is used to detect and prevent intrusion attempts from a range of cyber adversaries.

Reference 92 - 0.07% Coverage

potential cascading effects from a cyber attack against their networks and systems.

Reference 93 - 0.12% Coverage

These efforts are improving the private sector’s ability to detect and prevent intrusion attempts, as well as recover from a range of cyber incidents.

Reference 94 - 0.23% Coverage

The Administration will continue to promote the adoption of the Framework as a key means of improving U.S. cyber defenses and, by extension, decreasing adversaries’ perceptions of the benefits to be gained from engaging in malicious cyber activities against U.S. computers and networks.

Reference 95 - 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.

References 96-97 - 0.24% Coverage

The Federal government continues to improve the security of its information and systems through broad implementation of cybersecurity capabilities and services designed to detect and prevent malicious cyber activities as well as manage internal networks and systems more effectively and securely.

References 98-100 - 0.26% Coverage

In addition to defensive measures, the United States Government must also ensure the resiliency of its networks, systems and data. To do so, the Administration has implemented policies intended to improve the Federal government’s ability to identify and respond to incidents, and reconstitute rapidly if attacks succeed.

Reference 101 - 0.02% Coverage

prepare for attacks

References 102-103 - 0.02% Coverage

Deterrence by Cost Imposition

Reference 104 - 0.06% Coverage

Developing options to impose economic costs on malicious cyber actors.

Reference 105 - 0.07% Coverage

(2) deny adversaries access to infrastructure used to conduct malicious cyber activity.

References 106-107 - 0.08% Coverage

As necessary, developing appropriate military options to defend the nation from cyber attacks.

Reference 108 - 0.11% Coverage

Just because an attack takes place in cyberspace does not mean that a lawful and appropriate response must be conducted through cyber means.

Reference 109 - 0.06% Coverage

Nor is a direct response always the most appropriate and proportional response.

References 110-111 - 0.23% Coverage

Instead, the United States must maintain a spectrum of response capabilities that provide the President and senior U.S. leaders with options that can be tailored to   
10   
particular adversaries, the impact of the malicious activities, and the level of certainty regarding attribution.

References 112-113 - 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 114 - 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.

References 115-116 - 0.08% Coverage

In particular, financial sanctions can offer an effective tool for responding to cyber attacks.

References 117-119 - 0.44% Coverage

In response to North Korea’s destructive and coercive cyber attack in November 2014 – which was intended to harm a U.S. business and suppress free speech – the Administration announced new sanctions on certain North Korean actors. Further, in April 2015 the President issued a new Executive Order authorizing the imposition of sanctions on individuals and entities whose cyberenabled activities have contributed to a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

References 120-122 - 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.

References 123-124 - 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.

References 125-129 - 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 130 - 0.03% Coverage

attacks on computers and networks

Reference 131 - 0.16% Coverage

Since there is an individual or organization behind every intrusion, U.S. law enforcement agencies are a critical element of the United States Government’s cyber incident response mechanism.

References 132-133 - 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 134 - 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 135 - 0.11% Coverage

Law enforcement can also deny adversaries access to the infrastructure used to conduct malicious cyber activities against the United States.

Reference 136 - 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 137 - 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 138 - 0.05% Coverage

Building Capabilities to Defend the Nation in Cyberspace

Reference 139 - 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 140 - 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.

References 141-144 - 0.13% Coverage

The United States Government will be prepared, if directed by the President, to use all necessary means, including military, to respond to a cyber attack on the nation.

References 145-149 - 0.49% Coverage

To support this operational requirement, the Department of Defense established U.S. Cyber Command in October 2010 to consolidate U.S. military cyber capabilities to meet cyber threats. U.S. Cyber Command, in conjunction with the combatant commands, is now building a highly capable force. The Cyber Mission Force is capable of full spectrum cyber operations, and it plans and prepares on an ongoing basis to defend the nation. In September 2013, U.S. Cyber Command activated the headquarters for its Cyber National Mission Force, one of three distinct forces8 that could rapidly react to a cyber attack on the nation.

References 150-152 - 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 153 - 0.11% Coverage

Further, the Department of Defense is able, if directed, to conduct operations in cyberspace, including offensive cyber operations.

References 154-155 - 0.35% Coverage

Even though the United States Government is not limited to responding to a cyber attack through cyberspace, there are unique advantages to such a symmetrical response. Cyber operations can be narrowly tailored to target the precise system or systems that are perpetrating an attack against the United States. Further, the methods for neutralizing a malicious system can be sufficiently precise so as to minimize collateral effects.

Reference 156 - 0.11% Coverage

Developing these capabilities does not mean the United States is militarizing cyberspace, any more than having a navy militarizes the oceans.

References 157-158 - 0.20% Coverage

However, adversaries contemplating testing U.S. resolve should understand that the United States may, in circumstances where network defense and law enforcement measures are insufficient, use cyber operations to defend our nation and our interests.

Reference 159 - 0.03% Coverage

Activities that Support Deterrence

Reference 160 - 0.10% Coverage

Bringing a “whole-of-government” and “whole-of-nation” approach to cyber incident response and national-level events.

References 161-165 - 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 166 - 0.10% Coverage

Further developing intelligence capabilities that improve our ability to attribute and act against malicious cyber activities

Reference 167 - 0.06% Coverage

appropriate responses for cyber attacks against critical infrastructure.

References 168-169 - 0.07% Coverage

Bolstering “Whole-of-Government” and “Whole of Nation” Response Capabilities

Reference 170 - 0.09% Coverage

The Department of State uses its relationships with foreign governments to coordinate policy responses.

References 171-172 - 0.20% Coverage

DHS has an intimate knowledge of U.S. critical infrastructure, significant expertise in incident response and mitigation, and the deep relationships with the private sector necessary to protect critical infrastructure and respond to cyber attacks.

References 173-174 - 0.19% Coverage

These capabilities, matched with the expertise of the Intelligence Community and the Department of Defense, reflect a “whole-of-government” approach to identify, mitigate, and defend against cyber incidents and national-level events

References 175-176 - 0.17% Coverage

In addition, the Administration has put in place mechanisms that ensure departments and agencies are combining their capabilities and resources into effective, coordinated responses to malicious cyber activity.

Reference 177 - 0.18% Coverage

As one example, in 2014, the White House began using the Cyber Response Group, or CRG—modeled on the highly effective and long-standing Counterterrorism Security Group—to handle certain incident response coordination tasks.

Reference 178 - 0.13% Coverage

The CRG focuses on sharing threat information, malware signatures, plans of state and non-state actors, and coordinating responses across the government.

References 179-181 - 0.39% Coverage

Malicious actors are increasingly willing to intrude into public and private networks for the purpose of destructive cyber attacks, and the   
14   
Administration views forums for agile interagency coordination, like the CRG as a linchpin in the government’s response capabilities. In standing up the CRG and similar mechanisms, the Administration seeks to share knowledge about ongoing threats and attacks and coordinate all elements of the government’s response at the highest levels.

Reference 182 - 0.18% Coverage

All of these efforts are aimed at improving the government’s ability to understand the nature of a given cyber incident and to make rapid decisions about whether and how to respond to cyber incidents of significant national concern.

Reference 183 - 0.04% Coverage

Declaratory Policy and Strategic Communications

References 184-187 - 0.62% 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. Such signaling can be direct or indirect, private or public. However, the United States must maintain consistent and credible messages and messengers, and develop the shared situational awareness necessary to determine whether an adversary received the signal and interpreted it correctly. 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.

References 188-189 - 0.12% Coverage

The United States has issued clear statements in the past regarding the U.S. intention to respond as necessary and appropriate to cyber threats.

References 190-191 - 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.

References 192-193 - 0.22% Coverage

The Administration will consider whether to speak more openly about whether and how the United States might respond to malicious cyber activities, although such public discussion will require carefully balancing such transparency against intelligence and military equities.

Reference 194 - 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 195 - 0.11% Coverage

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

References 196-198 - 0.20% Coverage

The United States Government may also send messages through diplomatic or other channels to foreign adversaries as a warning that the United States can attribute and will respond to malicious cyber activities as necessary to protect our interests.

Reference 199 - 0.15% Coverage

In more extreme scenarios, the United States may intensify this strategic   
15   
messaging and demonstrate our resolve through stronger measures, including sanctions or military posturing.

Reference 200 - 0.02% Coverage

Intelligence Capabilities

Reference 201 - 0.11% Coverage

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

Reference 202 - 0.01% Coverage

cyber attacks

Reference 203 - 0.22% Coverage

The United States Government will continue to use its intelligence capabilities in a way that optimally protects U.S. national and economic security while supporting foreign policy, protecting privacy and civil liberties, and building and maintaining the public trust.

Reference 204 - 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 205 - 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.

References 206-207 - 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 208 - 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 209 - 0.02% Coverage

crippling cyber attacks

References 210-211 - 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 212 - 0.02% Coverage

intentions to attack

Reference 213 - 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 214 - 0.02% Coverage

respond to cyber incidents

Reference 215 - 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 216 - 0.01% Coverage

cyber attacks

References 217-218 - 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.

References 219-220 - 0.08% Coverage

we will use all necessary and appropriate instruments of national power to protect our interests

References 221-224 - 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 225 - 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.