Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 9 references coded [ 0.49% Coverage]

Reference 1 - 0.09% Coverage

We will disrupt, dismantle, and defeat al-Qa’ida and its affiliates through a comprehensive strategy that denies them safe haven, strengthens front-line partners, secures our homeland, pursues justice through durable legal approaches, and counters a bankrupt agenda of extremism and murder with an agenda of hope and opportunity

Reference 2 - 0.11% Coverage

Our approach relies on our shared efforts to identify and interdict threats; deny hostile actors the ability to operate within our borders; maintain effective control of our physical borders; safeguard lawful trade and travel into and out of the United States; disrupt and dismantle transnational terrorist, and criminal organizations; and ensure our national resilience in the face of the threat and hazards.

Reference 3 - 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 4 - 0.01% Coverage

Deny Terrorists Weapons of Mass Destruction

Reference 5 - 0.03% Coverage

Deny Al-Qa’ida the Ability to Threaten the American People, Our Allies, Our Partners and Our Interests Overseas

Reference 6 - 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 7 - 0.03% Coverage

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

Reference 8 - 0.01% Coverage

Deny Safe Havens and Strengthen At-Risk States

Reference 9 - 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\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

U.S. capabilities to deny adversaries’ objectives

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 2 references coded [ 0.72% Coverage]

Reference 1 - 0.15% Coverage

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

Reference 2 - 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.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 2 references coded [ 0.30% Coverage]

Reference 1 - 0.21% Coverage

Today, through existing and developing collaborations in the technical and military defense arenas, nations share an unprecedented ability to recognize and respond to incidents—a crucial step in denying would-be attackers the ability to do lasting damage to our national and international networks~

Reference 2 - 0.09% Coverage

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

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 2 references coded [ 0.13% Coverage]

Reference 1 - 0.05% Coverage

Denying an aggressor the benefits of achieving its objectives

Reference 2 - 0.08% Coverage

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

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 3 references coded [ 0.16% Coverage]

Reference 1 - 0.07% Coverage

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

Reference 2 - 0.02% Coverage

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

Reference 3 - 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.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 3 references coded [ 0.51% Coverage]

Reference 1 - 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 2 - 0.22% Coverage

Denial: While DoD has made progress in building the Cyber Mission Force, 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 3 - 0.08% Coverage

Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 8 references coded [ 0.81% Coverage]

Reference 1 - 0.05% Coverage

Deter, deny, and defeat state adversaries.

Reference 2 - 0.05% Coverage

to deter, deny, and defeat state adversaries

Reference 3 - 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 4 - 0.05% Coverage

Deter, Deny, and Defeat State Adversaries

Reference 5 - 0.09% Coverage

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

Reference 6 - 0.10% Coverage

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

Reference 7 - 0.04% Coverage

Deny an adversary’s objectives

Reference 8 - 0.15% Coverage

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

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 2 references coded [ 0.08% Coverage]

Reference 1 - 0.06% Coverage

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

Reference 2 - 0.02% Coverage

deny the peaceful use of outer space.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 8 references coded [ 0.91% Coverage]

Reference 1 - 0.02% Coverage

Deterrence by Denial

Reference 2 - 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 3 - 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 4 - 0.02% Coverage

Deterrence by Denial

Reference 5 - 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.

Reference 6 - 0.07% Coverage

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

Reference 7 - 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 8 - 0.11% Coverage

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

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 9 references coded [ 0.42% Coverage]

Reference 1 - 0.03% Coverage

A layered missile defense system will defend our homeland against missile att acks.

Reference 2 - 0.04% Coverage

The United States is deploying a layered missile defense system focused on North Korea and Iran to defend our homeland against missile attacks.

Reference 3 - 0.04% Coverage

We will deny violent ideologies the space to take root by improving trust among law enforcement, the private sector, and American citizens.

Reference 4 - 0.02% Coverage

DEFEND COMMUNITIES: We will deny TCOs the ability to harm Americans.

Reference 5 - 0.06% Coverage

Today, they are ﬁ elding military capabilities designed to deny America access in times of crisis and to contest our ability to operate freely in critical commercial zones during peacetime.

Reference 6 - 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 7 - 0.09% Coverage

The United States will, in concert with allies and partners, use the information-rich open-source environment to deny the ability of state and non-state actors to attack our citizens, conduct offensive intelligence activities, and degrade America’s democratic institutions.

Reference 8 - 0.05% Coverage

We will deny revenue to terrorists, WMD proliferators, and other illicit actors in order to constrain their ability to use and move funds to support hostile acts and operations.

Reference 9 - 0.04% Coverage

We will work with partners to deny the Iranian regime all paths to a nuclear weapon and neutralize Iranian malign influence

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Defense Strategy Summary - § 1 reference coded [ 0.39% Coverage]

Reference 1 - 0.39% Coverage

It comprises four layers: contact, blunt, surge, and homeland. These are, respectively, designed to help us compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 8 references coded [ 0.46% Coverage]

Reference 1 - 0.07% Coverage

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

Reference 2 - 0.06% Coverage

Deterrence by Denial. To deter aggression, especially where potential adversaries could act to rapidly seize territory, the Department will develop asymmetric approaches and optimize our posture for denial.

Reference 3 - 0.07% Coverage

Deterring PRC Attacks. The Department will bolster deterrence by leveraging existing and emergent force capabilities, posture, and activities to enhance denial, and by enhancing the resilience of U.S. systems the PRC may seek to target.

Reference 4 - 0.07% Coverage

We will work together with our Allies and partners to modernize denial capabilities, increase interoperability, improve resilience against attack and coercion, share intelligence, and strengthen extended nuclear deterrence.

Reference 5 - 0.06% Coverage

Over time, the Department will focus on enhancing denial capabilities and key enablers in NATO’s force planning, while NATO Allies seek to bolster their conventional warfighting capabilities.

Reference 6 - 0.04% Coverage

The Department will seek to improve denial capability, including resilience, particularly for those most exposed to military coercion.

Reference 7 - 0.07% Coverage

The Joint Force will retain the ability to deny Iran a nuclear weapon; to identify and support action against Iranian and Iranian-backed threats; and to disrupt top-tier VEO threats that endanger the homeland and vital U.S. national interests.

Reference 8 - 0.03% Coverage

To enhance our ability to deny aggression, we will improve the speed and accuracy of detection and targeting.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 1 reference coded [ 0.12% Coverage]

Reference 1 - 0.12% Coverage

Our efforts will require greater collaboration by public and private sector partners to improve intelligence sharing, execute disruption campaigns at scale, deny adversaries use of U.S.-based infrastructure, and thwart global ransomware campaigns.