Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 12 references coded [ 0.72% Coverage]

Reference 1 - 0.04% Coverage

The space and cyberspace capabilities that power our daily lives and military operations are vulnerable to disruption and attack.

Reference 2 - 0.05% Coverage

Credible and effective alternatives to military action—from sanctions to isolation—must be strong enough to change behavior, just as we must reinforce our alliances and our military capabilities.

Reference 3 - 0.07% 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, preserve access to the global commons, and strengthen partners.

Reference 4 - 0.07% Coverage

We will continue to rebalance our military capabilities to excel at counterterrorism, counterinsurgency, stability operations, and meeting increasingly sophisticated security threats, while ensuring our force is ready to address the full range of military operations.

Reference 5 - 0.07% Coverage

Furthermore, 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.

Reference 6 - 0.06% Coverage

We maintain superior capabilities to deter and defeat adaptive enemies and   
★ 17 ★   
NaTIONal SeCurITy STraTegy   
to ensure the credibility of security partnerships that are fundamental to regional and global security.

Reference 7 - 0.04% Coverage

To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities.

Reference 8 - 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 9 - 0.06% Coverage

This requires investing now in the capable partners of the future; building today the capacity to strengthen the foundations of our common security, and modernizing our capabilities in order to ensure that we are agile in the face of change.

Reference 10 - 0.09% Coverage

Leverage and Grow our Space Capabilities: For over 50 years, our space community has been a catalyst for innovation and a hallmark of U.S. technological leadership. Our space capabilities underpin global commerce and scientific advancements and bolster our national security strengths and those of our allies and partners.

Reference 11 - 0.04% Coverage

Our ability to sustain these alliances, and to build coalitions of support toward common objectives, depends in part on the capabilities of America’s Armed Forces.

Reference 12 - 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

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 18 references coded [ 0.17% Coverage]

Reference 1 - 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 2 - 0.01% Coverage

capabilities

Reference 3 - 0.01% Coverage

require armed forces with unmatched capabilities

Reference 4 - 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 5 - 0.01% Coverage

U.S. capabilities to deny adversaries’ objectives

Reference 6 - 0.01% Coverage

Enhance capabilities for domain awareness

Reference 7 - 0.01% Coverage

Accelerate the development of standoff radiological/nuclear detection capabilities

Reference 8 - 0.01% Coverage

Enhance domestic capabilities

Reference 9 - 0.02% Coverage

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

Reference 10 - 0.01% Coverage

critical capabilities

Reference 11 - 0.01% Coverage

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

Reference 12 - 0.01% Coverage

capabilities

Reference 13 - 0.01% Coverage

capabilities

Reference 14 - 0.01% Coverage

capabilities.

Reference 15 - 0.01% Coverage

capabilities

Reference 16 - 0.01% Coverage

capabilities,

Reference 17 - 0.01% Coverage

recommendations regarding capability development

Reference 18 - 0.01% Coverage

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

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 4 references coded [ 0.66% 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 - 0.23% Coverage

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

Reference 4 - 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

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 7 references coded [ 0.73% Coverage]

Reference 1 - 0.06% Coverage

Protecting networks of such great value requires robust defensive capabilities~

Reference 2 - 0.07% Coverage

However, a globally distributed network requires globally distributed early warning capabilities~1

Reference 3 - 0.02% Coverage

incident response capabilities

Reference 4 - 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 5 - 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 6 - 0.14% Coverage

Dialogues and best practice exchanges to enhance partner capabilities, such as digital forensics, work force development, and network penetration and resiliency testing will be important to this effort~

Reference 7 - 0.15% Coverage

The United States will work in close partnership with like-minded states to leverage capabilities, reduce collective risk, and foster multi-stakeholder initiatives to deter malicious activities in cyberspace~

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 10 references coded [ 1.08% Coverage]

Reference 1 - 0.02% Coverage

military capabilities

Reference 2 - 0.08% Coverage

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

Reference 3 - 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 4 - 0.04% Coverage

relative ease of developing potent capabilities.

Reference 5 - 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.

Reference 6 - 0.10% Coverage

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

Reference 7 - 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 8 - 0.06% Coverage

shape our joint force to be able to aggregate capabilities quickly

Reference 9 - 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.

Reference 10 - 0.12% Coverage

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

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 10 references coded [ 0.12% Coverage]

Reference 1 - 0.01% Coverage

military capabilities

Reference 2 - 0.01% Coverage

develop U.S. operational capabilities in cyberspace.

Reference 3 - 0.01% Coverage

integrate capabilities,

Reference 4 - 0.01% Coverage

uneven capabilities across various groups,

Reference 5 - 0.02% Coverage

apply technical capabilities to the defense of the national infrastructure

Reference 6 - 0.01% Coverage

capability

Reference 7 - 0.01% Coverage

capabilities

Reference 8 - 0.02% Coverage

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

Reference 9 - 0.01% Coverage

capabilities

Reference 10 - 0.04% Coverage

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

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 8 references coded [ 0.35% Coverage]

Reference 1 - 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.

Reference 2 - 0.03% Coverage

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

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.

Reference 4 - 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 5 - 0.04% Coverage

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

Reference 6 - 0.02% Coverage

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

Reference 7 - 0.02% Coverage

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

Reference 8 - 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.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 16 references coded [ 2.25% Coverage]

Reference 1 - 0.16% Coverage

Governments, companies, and organizations must carefully prioritize the systems and data that they need to protect, assess risks and hazards, and make prudent investments in cybersecurity and cyber defense capabilities to achieve their security goals and objectives.

Reference 2 - 0.19% Coverage

To this end the Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.

Reference 3 - 0.09% Coverage

DoD helps U.S. allies and partners to understand the cyber threats they face and to build the cyber capabilities necessary to defend their networks and data.

Reference 4 - 0.14% Coverage

Allies and partners also often have complementary capabilities that can augment those of the United States, and the United States seeks to build strong alliances and coalitions to counter potential adversaries’ cyber activities.

Reference 5 - 0.12% Coverage

The Defense Department must further develop adequate warning intelligence of adversary intentions and capabilities for conducting destructive and disruptive cyberattacks against DoD and the United States.

Reference 6 - 0.05% Coverage

Russia and China have developed advanced cyber capabilities and strategies.

Reference 7 - 0.11% Coverage

While Iran and North Korea have less developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests in cyberspace.

Reference 8 - 0.15% Coverage

In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber capabilities.

Reference 9 - 0.16% Coverage

To conduct a disruptive or destructive cyber operation against a military system or industrial control system requires expertise, but a potential adversary need not spend   
9   
Th e De pa r tme n t o f De f e n s e Cy be r S t r a t e g y   
billions of dollars to develop an offensive capability.

Reference 10 - 0.13% Coverage

As cyber capabilities become more readily available over time, the Department of Defense assesses that state and non-state actors will continue to seek and develop cyber capabilities to use against U.S. interests.

Reference 11 - 0.14% Coverage

Although DoD has prioritized the allocation of resources in its budget to develop cyber capabilities, continued fiscal uncertainty requires that DoD plan to build its cyber capabilities under a declining overall defense budget.

Reference 12 - 0.16% Coverage

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

Reference 13 - 0.20% Coverage

Finally, cyber capabilities present state and non-state actors with the ability to strike at U.S. interests in a manner that may or may not necessarily warrant a purely military response by the United States, but which may nonetheless present a significant threat to U.S. national security and may warrant a non-military response of some kind.

Reference 14 - 0.10% Coverage

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

Reference 15 - 0.09% Coverage

DoD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property.

Reference 16 - 0.27% Coverage

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

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 15 references coded [ 2.18% Coverage]

Reference 1 - 0.16% Coverage

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

Reference 2 - 0.11% Coverage

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

Reference 3 - 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 4 - 0.17% Coverage

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

Reference 5 - 0.13% Coverage

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

Reference 6 - 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 7 - 0.12% Coverage

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

Reference 8 - 0.12% Coverage

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

Reference 9 - 0.09% Coverage

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

Reference 10 - 0.15% Coverage

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

Reference 11 - 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 12 - 0.04% Coverage

advanced military capabilities

Reference 13 - 0.11% Coverage

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

Reference 14 - 0.12% Coverage

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

Reference 15 - 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\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 2 references coded [ 0.09% Coverage]

Reference 1 - 0.05% Coverage

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

Reference 2 - 0.04% Coverage

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

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 21 references coded [ 3.03% Coverage]

Reference 1 - 0.05% Coverage

Building Capabilities to Defend the Nation in Cyberspace

Reference 2 - 0.07% Coverage

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

Reference 3 - 0.02% Coverage

Intelligence Capabilities

Reference 4 - 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 5 - 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 6 - 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 7 - 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 8 - 0.23% Coverage

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.

Reference 9 - 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.

Reference 10 - 0.11% Coverage

the United States must maintain a spectrum of response capabilities that provide the President and senior U.S. leaders with options

Reference 11 - 0.05% Coverage

Building Capabilities to Defend the Nation in Cyberspace

Reference 12 - 0.15% 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.

Reference 13 - 0.11% Coverage

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

Reference 14 - 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 15 - 0.10% Coverage

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

Reference 16 - 0.07% Coverage

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

Reference 17 - 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

Reference 18 - 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 19 - 0.02% Coverage

Intelligence Capabilities

Reference 20 - 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 21 - 0.22% Coverage

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

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 48 references coded [ 2.44% Coverage]

Reference 1 - 0.04% Coverage

We will strengthen America’s capabilities—including in space and cyberspace—and revitalize others that have been neglected.

Reference 2 - 0.07% Coverage

We will also better integrate intelligence, law enforcement, and emergency management operations to ensure that frontline defenders have the right information and capabilities to respond to WMD threats from state and non-state actors.

Reference 3 - 0.05% Coverage

China and Russia are developing advanced weapons and capabilities that could threaten our critical infrastructure and our command and control architecture.

Reference 4 - 0.05% Coverage

Dedicated state actors are likely to develop more advanced bioweapons, and these capabilities may become available to malicious non-state actors as well.

Reference 5 - 0.05% Coverage

We will assess where cyberattacks could have catastrophic or cascading consequences and prioritize our protective efforts, capabilities, and defenses accordingly.

Reference 6 - 0.07% Coverage

The Federal Government will ensure that those charged with securing critical infrastructure have the necessary authorities, information, and capabilities to prevent attacks before they affect or hold at risk U.S. critical infrastructure

Reference 7 - 0.03% Coverage

We will also invest in capabilities that improve the ability of the United States to attribute cyberatt acks.

Reference 8 - 0.05% Coverage

Agencies from all levels of government must coordinate bett er and apply lessons learned from exercises to pinpoint the areas and capabilities that require improvement.

Reference 9 - 0.05% Coverage

The NSIB is the American network of knowledge, capabilities, and people—including academia, National Laboratories, and the private sector—that turns ideas into innovations

Reference 10 - 0.06% Coverage

e U.S. Government will develop a capability to integrate, monitor, and better understand the national security implications of unfair industry trends and the actions of our rivals.

Reference 11 - 0.07% Coverage

Russia is investing in new military capabilities, including nuclear systems that remain the most significant existential threat to the United States, and in   
N A TI O N A L S E C U R IT Y S TR A TE G Y   
destabilizing cyber capabilities

Reference 12 - 0.06% Coverage

The combination of Russian ambition and growing military capabilities creates an unstable frontier in Eurasia, where the risk of conflict due to Russian miscalculation is growing.

Reference 13 - 0.04% Coverage

Our allies and partners must also contribute the capabilities, and demonstrate the will, to confront shared threats

Reference 14 - 0.04% Coverage

The United States must develop new concepts and capabilities to protect our homeland, advance our prosperity , and preserve peace.

Reference 15 - 0.01% Coverage

Instead of developing important capabilities

Reference 16 - 0.04% Coverage

entered a nearly decade long “procurement holiday” during which the acquisition of new weapon systems was severely limited.

Reference 17 - 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 18 - 0.05% Coverage

Adversaries studied the American way of war and began investing in capabilities that targeted our strengths and sought to exploit perceived weaknesses.

Reference 19 - 0.09% Coverage

Despite decades of efforts to reform the way that the United States develops and procures new weapons, our acquisition system remained sclerotic. The Joint Force did not keep pace with emerging threats or technologies. We got less for our defense dollars, shortchanging American taxpayers and warﬁ ghters.

Reference 20 - 0.03% Coverage

New advances in computing, autonomy, and manufacturing are already transforming the way we ﬁ ght.

Reference 21 - 0.01% Coverage

Renew Capabilities

Reference 22 - 0.04% Coverage

Given the new features of the geopolitical environment, the United States must renew key capabilities to address the challenges we face.

Reference 23 - 0.06% Coverage

The United States must retain overmatch— the combination of capabilities in sufficient scale to prevent enemy success and to ensure that America’s sons and daughters will never be in a fair fight.

Reference 24 - 0.09% Coverage

To retain military overmatch the United States must restore our ability to produce innovative capabilities, restore the readiness of our forces for major war, and grow the size of the force so that it is capable of operating at sufficient scale and for ample duration to win across a range of scenarios.

Reference 25 - 0.05% Coverage

We need our allies to do the same—to modernize, acquire necessary capabilities, improve readiness, expand the size of their forces, and affirm the political will to win.

Reference 26 - 0.04% Coverage

Ensuring that the U.S. military can defeat our adversaries requires weapon systems that clearly overmatch theirs in lethality.

Reference 27 - 0.04% Coverage

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

Reference 28 - 0.05% Coverage

Departments and agencies must work with industry to experiment, prototype, and rapidly field new capabilities that can be easily upgraded as new technologies come online.

Reference 29 - 0.07% Coverage

The erosion of American manufacturing over the last two decades, however, has had a negative impact on these capabilities and threatens to undermine the ability of U.S. manufacturers to meet national security requirements.

Reference 30 - 0.05% Coverage

Where possible, the U.S. Government will work with industry partners to strengthen U.S. competitiveness in key technologies and manufacturing capabilities

Reference 31 - 0.06% Coverage

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

Reference 32 - 0.05% Coverage

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

Reference 33 - 0.07% Coverage

As the U.S. Government partners with U.S. commercial space capabilities to improve the resiliency of our space architecture, we will also consider extending national security protections to our private sector partners as needed.

Reference 34 - 0.05% Coverage

Many countries now view cyber capabilities as tools for projecting influence, and some use cyber tools to protect and extend their autocratic regimes.

Reference 35 - 0.05% Coverage

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

Reference 36 - 0.05% Coverage

IMPROVE ATTRIBUTION , ACCOUNTABIL ITY, AND RESPONSE: We will invest in capabilities to support and improve our ability to attribute cyberattacks, to al low for rapid response.

Reference 37 - 0.07% Coverage

ENHANCE CYBER TOOLS AND EXPERTISE: We will improve our cyber tools across the spectrum of conflict to protect U.S. Government assets and U.S. critical infrastructure, and to protect the integrity of data and information.

Reference 38 - 0.04% Coverage

The ability of the United States to modernize our military forces to overmatch our adversaries requires intelligence support.

Reference 39 - 0.07% Coverage

Intelligence is needed to understand and anticipate foreign doctrine and the intent of foreign leaders, prevent tactical and operational surprise, and ensure that U.S. capabilities are not compromised before they are fielded.

Reference 40 - 0.05% Coverage

Allies and partners are a great strength of the United States. They add directly to U.S. political, economic, military, intelligence, and other capabilities.

Reference 41 - 0.05% Coverage

The United States must marshal the will and capabilities to compete and prevent unfavorable shifts in the Indo-Pacific, Europe, and the Middle East.

Reference 42 - 0.04% Coverage

For example, we will cooperate on missile defense with Japan and South Korea to move toward an area defense capability .

Reference 43 - 0.05% Coverage

Russia continues to intimidate its neighbors with threatening behavior, such as nuclear posturing and the forward deployment of offensive capabilities.

Reference 44 - 0.06% Coverage

We expect our European allies to increase defense spending to 2 percent of gross domestic product by 2024, with 20 percent of this spending devoted to increasing military capabilities.

Reference 45 - 0.06% Coverage

We will work with NATO to improve its integrated air and missile defense capabilities to counter existing and projected ballistic and cruise missile threats, particularly from Iran.

Reference 46 - 0.04% Coverage

It continues to develop more capable ballistic missiles and intelligence capabilities, and it undertakes malicious cyber activities.

Reference 47 - 0.06% Coverage

We will assist regional partners in strengthening their institutions and capabilities, including in law enforcement, to conduct counterterrorism and counterinsurgency efforts.

Reference 48 - 0.04% Coverage

We will help partners procure interoperable missile defense and other capabilities to better defend against active missile threats.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 DoD Cyber Strategy Summary - § 1 reference coded [ 0.38% Coverage]

Reference 1 - 0.38% Coverage

We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 9 references coded [ 1.46% Coverage]

Reference 1 - 0.07% Coverage

These adversaries are continually developing new and more effective cyber weapons.

Reference 2 - 0.08% Coverage

and the United States is positioned to use cyber capabilities to achieve national security objectives.

Reference 3 - 0.23% Coverage

Federal law enforcement works to apprehend and prosecute offenders, disable criminal infrastructure, limit the spread and use of nefarious cyber capabilities, prevent cyber criminals and their state sponsors from profiting from their illicit activity, and seize their assets.

Reference 4 - 0.26% Coverage

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

Reference 5 - 0.15% Coverage

The Administration will eliminate policy   
barriers that inhibit a robust cybersecurity industry from developing, sharing, and building innovative capabilities to reduce cyber threats.

Reference 6 - 0.16% Coverage

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

Reference 7 - 0.24% Coverage

All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities.

Reference 8 - 0.08% Coverage

Many United States allies and partners possess unique cyber capabilities that can complement our own.

Reference 9 - 0.19% Coverage

The United States will work to strengthen the capacity and interoperability of those allies and partners to improve our ability to optimize our combined skills, resources, capabilities, and perspectives against shared threats.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Defense Strategy Summary - § 12 references coded [ 2.98% Coverage]

Reference 1 - 0.23% Coverage

In this environment, there can be no complacency—we must make difficult choices and prioritize what is most important to field a lethal, resilient, and rapidly adapting Joint Force.

Reference 2 - 0.28% Coverage

Collectively, our force posture, alliance and partnership architecture, and Department modernization will provide the capabilities and agility required to prevail in conflict and preserve peace through strength.

Reference 3 - 0.29% Coverage

The use of emerging technologies to discredit and subvert democratic processes in Georgia, Crimea, and eastern Ukraine is concern enough, but when coupled with its expanding and modernizing nuclear arsenal the challenge is clear.

Reference 4 - 0.37% Coverage

North Korea seeks to guarantee regime survival and increased leverage by seeking a mixture of nuclear, biological, chemical, conventional, and unconventional weapons and a growing ballistic missile capability to gain coercive influence over South Korea, Japan, and the United States.

Reference 5 - 0.24% Coverage

Terrorists, trans-national criminal organizations, cyber hackers and other malicious non-state actors have transformed global affairs with increased capabilities of mass disruption.

Reference 6 - 0.16% Coverage

Modernize key capabilities. We cannot expect success fighting tomorrow’s conflicts with yesterday’s weapons or equipment.

Reference 7 - 0.24% Coverage

To address the scope and pace of our competitors’ and adversaries’ ambitions and capabilities, we must invest in modernization of key capabilities through sustained, predictable budgets.

Reference 8 - 0.24% Coverage

Dynamic Force Employment will prioritize maintaining the capacity and capabilities for major combat, while providing options for proactive and scalable employment of the Joint Force.

Reference 9 - 0.15% Coverage

Foundational capabilities include: nuclear; cyber; space; C4ISR; strategic mobility, and counter WMD proliferation.

Reference 10 - 0.28% Coverage

Our allies and partners provide complementary capabilities and forces along with unique perspectives, regional relationships, and information that improve our understanding of the environment and expand our options.

Reference 11 - 0.29% Coverage

We will uphold our commitments and we expect allies and partners to contribute an equitable share to our mutually beneficial collective security, including effective investment in modernizing their defense capabilities.

Reference 12 - 0.20% Coverage

the Department will deepen its relations with regional countries that contribute military capabilities to shared regional and global security challenges.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Military Strategy Description - § 4 references coded [ 5.04% Coverage]

Reference 1 - 1.40% Coverage

From its global perspective, the NMS premises an adaptive and innovative Joint Force capable of employing its capabilities seamlessly across multiple regions and all domains -- continuing the transition from a regional to a global mindset and approach.

Reference 2 - 1.23% Coverage

To achieve military advantage over competitors and adversaries, the NMS introduces the notion of joint combined arms, defined as the conduct of operational art through the integration of joint capabilities in all domains.

Reference 3 - 1.11% Coverage

It will mark a shift to a concept-driven, threat-informed, capability development process and provide a campaign approach to unify service capabilities across materiel and non-materiel solutions.

Reference 4 - 1.30% Coverage

Consistent with the guidance laid out in the NDS, capability investments must emphasize military advantages in lethality and operational reach, while enabling the Joint Force to compete effectively below the level of armed conflict.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 24 references coded [ 1.79% Coverage]

Reference 1 - 0.10% Coverage

The United States will operate forces, synchronize broader Departmental efforts, and align Departmental activities with other instruments of national power to counter forms of competitor coercion, complicate competitors’ military preparations, and develop our own warfighting capabilities together with those of our Allies and partners.

Reference 2 - 0.05% Coverage

We will work closely with the North Atlantic Treaty Organization (NATO) and our partners to provide U.S. leadership, develop key enabling capabilities, and deepen interoperability.

Reference 3 - 0.13% Coverage

Now and over the next two decades, we face strategic challenges stemming from complex interactions between a rapidly changing global balance of military   
capabilities; emerging   
technologies; competitor doctrines that pose new threats to the U.S. homeland and to strategic stability; an escalation of competitors’ coercive and malign activities in the “gray zone”; and transboundary challenges that impose new demands on the Joint Force and the defense enterprise.

Reference 4 - 0.14% Coverage

Competitor strategies seek to exploit perceived vulnerabilities in the American way of war, including by creating anti-access/area-denial environments; developing conventional capabilities to undertake rapid interventions; posing all-domain threats to the U.S. homeland in an effort to jeopardize the U.S. military’s ability to project power and counter regional aggression; and using the cyber and space domains to gain operational, logistical, and information advantages.

Reference 5 - 0.09% Coverage

The PRC seeks to undermine U.S. alliances and security partnerships in the Indo-Pacific region, and leverage its growing capabilities, including its economic influence and the People’s Liberation Army’s (PLA) growing strength and military footprint, to coerce its neighbors and threaten their interests.

Reference 6 - 0.07% Coverage

In addition to expanding its conventional forces, the PLA is rapidly advancing and integrating its space, counterspace, cyber, electronic, and informational warfare capabilities to support its holistic approach to joint warfare.

Reference 7 - 0.03% Coverage

In parallel, the PRC is accelerating the modernization and expansion of its nuclear capabilities.

Reference 8 - 0.06% Coverage

Russia has incorporated these capabilities and methods into an overall strategy that, like the PRC’s, seeks to exploit advantages in geography and time backed by a mix of threats to the U.S. homeland and to our Allies and partners.

Reference 9 - 0.07% Coverage

North Korea continues to expand its nuclear and missile capability to threaten the U.S. homeland, deployed U.S. forces, and the Republic of Korea (ROK) and Japan, while seeking to drive wedges between the United StatesROK and United States-Japan Alliances.

Reference 10 - 0.10% Coverage

A wide range of new or fast-evolving technologies and applications are complicating escalation dynamics and creating new challenges for strategic stability. These include counterspace weapons, hypersonic weapons, advanced CBW, and new and emerging payload and delivery systems for both conventional and non-strategic nuclear weapons.

Reference 11 - 0.06% Coverage

In the cyber and space domains, the risk of inadvertent escalation is particularly high due to unclear norms of behavior and escalation thresholds, complex domain interactions, and new capabilities.

Reference 12 - 0.06% Coverage

Over the mid- to long-term, we will develop new capabilities, including in long-range strike, undersea, hypersonic, and autonomous systems, and improve information sharing and the integration of non-kinetic tools.

Reference 13 - 0.06% Coverage

The Department will employ an integrated deterrence approach that draws on tailored combinations of conventional, cyber, space, and information capabilities, together with the unique deterrent effects of nuclear weapons.

Reference 14 - 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 15 - 0.04% Coverage

We will develop new operational concepts and enhanced future warfighting capabilities against potential PRC aggression.

Reference 16 - 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 17 - 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 18 - 0.08% Coverage

The Department strengthens deterrence and gains military advantages not only by building Joint Force capabilities, but also by campaigning – the conduct and sequencing of logically-linked military activities to achieve strategy-aligned objectives over time.

Reference 19 - 0.05% Coverage

In Europe, our posture will focus on command and control, fires, and key enablers that complement our NATO Allies’ capabilities and strengthen deterrence by increasing combat credibility

Reference 20 - 0.06% Coverage

To strengthen and sustain deterrence, the Department will prioritize interoperability and enable coalitions with enhanced capabilities, new operating concepts, and combined, collaborative force planning.

Reference 21 - 0.11% Coverage

As we continue contributing to NATO capabilities and readiness – including through improvements to our posture in Europe and our extended nuclear deterrence commitments – the Department will work with Allies bilaterally and through NATO’s established processes to better focus NATO capability development and military modernization to address Russia’s military threat.

Reference 22 - 0.09% Coverage

The Department will prioritize cooperation with our regional and global partners that results in their increased ability to deter and defend against potential aggression from Iran, for example by working to advance integrated air and missile defense, maritime security, and irregular warfare capabilities.

Reference 23 - 0.09% Coverage

The Department will deter threats to the U.S. homeland from and through the Arctic region by improving early warning and ISR capabilities, partnering with Canada to enhance North American Aerospace Defense Command capabilities, and working with Allies and partners to increase shared maritime domain awareness.

Reference 24 - 0.07% Coverage

These include coordination with and contributions of Allies and partners, deterrent effects of U.S. nuclear posture, and leveraging posture and capabilities not solely engaged in the primary warfight – for example, cyber and space.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 3 references coded [ 1.75% Coverage]

Reference 1 - 0.64% Coverage

2. ENHANCE DETERRENCE   
Develop capabilities that deter adversaries from advancing their goals, employing their military strengths, or attacking U.S. interests.

Reference 2 - 0.48% Coverage

10. INTEGRATE CAPABILITIES RAPIDLY   
Timely integrate advanced capabilities to amplify existing warfighting advantages.

Reference 3 - 0.63% Coverage

 Ensure the Joint Force possesses the combat-credible capabilities necessary to prevail in conflict against the PRC in the Indo-Pacific, then Russia in Europe.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 17 references coded [ 1.23% Coverage]

Reference 1 - 0.08% Coverage

3) modernize and strengthen our military so it is equipped for the era of strategic competition with major powers, while maintaining the capability to disrupt the terrorist threat to the homeland. This is covered in Part II of this strategy.

Reference 2 - 0.07% Coverage

We will use these capabilities to outcompete our strategic competitors, galvanize collective action on global challenges, and shape the rules of the road for technology, cybersecurity, and trade and economics.

Reference 3 - 0.06% Coverage

Russia poses an immediate and ongoing threat to the regional security order in Europe and it is a source of disruption and instability globally but it lacks the across the spectrum capabilities of the PRC.

Reference 4 - 0.09% Coverage

As we modernize our military and work to strengthen our democracy at home, we will call on our allies to do the same, including by investing in the type of capabilities and undertaking the planning necessary to bolster deterrence in an increasingly confrontational world.

Reference 5 - 0.06% Coverage

We will modernize the joint force to be lethal, resilient, sustainable, survivable, agile, and responsive, prioritizing operational concepts and updated warfighting capabilities.

Reference 6 - 0.07% Coverage

It must not only be capable of rapidly manufacturing proven capabilities needed to defend against adversary aggression, but also empowered to innovate and creatively design solutions as battlefield conditions evolve.

Reference 7 - 0.12% Coverage

As emerging technologies transform warfare and pose novel threats to the United States and our allies and partners, we are investing in a range of advanced technologies including applications in the cyber and space domains, missile defeat capabilities, trusted artificial intelligence, and quantum systems, while deploying new capabilities to the battlefield in a timely manner.

Reference 8 - 0.07% Coverage

We also seek to remove barriers to deeper collaboration with allies and partners, to include issues related to joint capability development and production to safeguard our shared military-technological edge.

Reference 9 - 0.07% Coverage

Our National Defense Strategy relies on integrated deterrence: the seamless combination of capabilities to convince potential adversaries that the costs of their hostile activities outweigh their benefits.2

Reference 10 - 0.06% Coverage

Integration with allies and partners through investments in interoperability and joint capability development, cooperative posture planning, and coordinated diplomatic and economic approaches.

Reference 11 - 0.08% Coverage

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

Reference 12 - 0.03% Coverage

Welcoming Finland and Sweden to NATO will further improve our security and capabilities.

Reference 13 - 0.04% Coverage

Working with partners and allies, we will strengthen the Biological Weapons Convention to deter state biological warfare capabilities

Reference 14 - 0.10% Coverage

Many of these groups still intend to carry out or inspire others to attack the United States and our interests abroad, even as years of sustained counterterrorism and law enforcement pressure have constrained their capabilities, and enhanced security measures and information sharing have improved our defenses.

Reference 15 - 0.07% Coverage

We are working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks.

Reference 16 - 0.12% Coverage

As we step up our own sizable   
38 NATIONAL SECURITY STRATEGY   
        
contributions to NATO capabilities and readiness—including by strengthening defensive forces and capabilities, and upholding our long-standing commitment to extended deterrence—we will count on our Allies to continue assuming greater responsibility by increasing their spending, capabilities, and contributions.

Reference 17 - 0.04% Coverage

We will continue to work with allies and partners to enhance their capabilities to deter and counter Iran’s destabilizing activities.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 8 references coded [ 1.81% Coverage]

Reference 1 - 0.20% Coverage

The Department’s experiences have shown that cyber capabilities held in reserve or employed in isolation render little deterrent effect on their own.

Reference 2 - 0.23% Coverage

Instead, these military capabilities are most effective when used in concert with other instruments of national power, creating a deterrent greater than the sum of its parts.

Reference 3 - 0.26% Coverage

Both the People’s Republic of China (PRC) and Russia have embraced malicious cyber activity as a means to counter U.S. conventional military power and degrade the combat capability of the Joint Force.

Reference 4 - 0.19% Coverage

It exports dangerous cyber capabilities to like-minded nations and works to accelerate the rise of digital authoritarianism around the globe.

Reference 5 - 0.27% Coverage

In Russia’s war on Ukraine, Russian military and intelligence units have employed a range of cyber capabilities to support kinetic operations and defend Russian actions through a global propaganda campaign.

Reference 6 - 0.23% Coverage

In cyberspace, the Department will harness outwardfacing capabilities to enable internal defense, identifying and mitigating threats before they can harm the American people.

Reference 7 - 0.26% Coverage

In cyberspace, the capabilities of Allies and partners combine with those of the United States to enable timely information sharing and interoperability as well as contribute to our collective security.

Reference 8 - 0.18% Coverage

We will bolster the cyber capability and capacity of our Allies and partners and reinforce norms of responsible behavior in cyberspace.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 7 references coded [ 0.78% Coverage]

Reference 1 - 0.13% Coverage

Having successfully harnessed the Internet as the backbone of its surveillance state and influence capabilities, the PRC is exporting its vision of digital authoritarianism, striving to shape the global Internet in its image and imperiling human rights beyond its borders.

Reference 2 - 0.09% Coverage

For more than two decades, the Russian government has used its cyber capabilities to destabilize its neighbors and interfere in the domestic politics of democracies around the world.

Reference 3 - 0.22% Coverage

Iran has used cyber capabilities to threaten U.S. allies in the Middle East and elsewhere, while the DPRK conducts cyber activities to generate revenue through criminal enterprises, such as through the theft of cryptocurrency, ransomware, and the deployment of surreptitious information technology (IT) workers for the purposes of fueling its nuclear ambitions. Further maturation of these capabilities could have significant impacts on U.S., allied, and partner interests.

Reference 4 - 0.12% Coverage

We must build new and innovative capabilities that allow owners and operators of critical infrastructure, Federal agencies, product vendors and service providers, and other stakeholders to effectively collaborate with each other at speed and scale.

Reference 5 - 0.08% Coverage

Federal agencies that support critical infrastructure providers must enhance their own capabilities and their ability to collaborate with other Federal entities.

Reference 6 - 0.07% Coverage

strengthening the capabilities of the National Cyber Investigative Joint Task Force (NCIJTF) to coordinate law enforcement and other disruption actions

Reference 7 - 0.07% Coverage

These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities.

**Annotations**

1 Foreshadowing justification for future strategy of "defend foward".

2 Definition of Integrated Deterrence