Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 2 references coded [ 0.10% Coverage]

Reference 1 - 0.04% Coverage

That is why we must also enhance our resilience—the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Reference 2 - 0.06% Coverage

we are working across the government and with the private sector to design more secure technology that gives us the ability to better protect and to improve the resilience of critical government and industry systems and networks

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 2 references coded [ 0.83% Coverage]

Reference 1 - 0.60% Coverage

These efforts will be supported by the development of increasingly resilient networks and systems. In the case of a contingency involving network failure or significant compromise, DoD must be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations.

Reference 2 - 0.23% Coverage

To foster resiliency and smart diversity in its networks and systems, DoD will explore new and innovative approaches and paradigms for both existing and emerging challenges.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 4 references coded [ 0.13% Coverage]

Reference 1 - 0.03% Coverage

resilient to arbitrary or malicious disruption

Reference 2 - 0.03% Coverage

national and international network resilience

Reference 3 - 0.05% Coverage

Ensuring the resilience of our networks and information systems

Reference 4 - 0.02% Coverage

enhance overall resilience

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 3 references coded [ 0.31% Coverage]

Reference 1 - 0.08% Coverage

maintain joint assured access to the global commons and cyberspace should they become contested

Reference 2 - 0.14% Coverage

Joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint Force.

Reference 3 - 0.08% Coverage

Joint Forces will secure the ‘.mil’ domain, requiring a resilient DoD cyberspace architecture

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 2 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

more resilient systems and system architectures

Reference 2 - 0.01% Coverage

resilient architectures,

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 10 references coded [ 1.98% Coverage]

Reference 1 - 0.12% Coverage

Behind these defense investments, organizations of every kind must build business continuity plans and be ready to operate in a degraded cyber environment where access to networks and data is uncertain.

Reference 2 - 0.08% Coverage

To mitigate risks in cyberspace requires a comprehensive strategy to counter and if necessary withstand disruptive and destructive attacks.

Reference 3 - 0.09% Coverage

Through years of practice and exercise, a culture of resilience took root in the military and units were ready and prepared to operate in contested environments.

Reference 4 - 0.26% Coverage

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

Reference 5 - 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 6 - 0.51% Coverage

Resilience: Because the Defense Department’s   
capabilities cannot   
necessarily guarantee that every cyberattack will be denied successfully, the Defense Department must invest in resilient and redundant systems so that it may continue its operations in the face of disruptive or destructive cyberattacks on DoD networks. The Defense Department cannot, however, foster resilience in organizations that fall outside of its authority. In order for resilience to succeed as a factor in effective deterrence, other agencies of the government must work with critical infrastructure owners and operators and the private sector more broadly to develop resilient and redundant systems that can withstand a potential attack. Effective resilience measures can help convince potential adversaries of the futility of commencing cyberattacks on U.S. networks and systems.

Reference 7 - 0.02% Coverage

Plan for network defense and resilience.

Reference 8 - 0.27% Coverage

Build and exercise continuity plans. All DoD components will identify and build resiliency plans to maintain continuity of their most critical operations in the event of network disruption and degradation. Military campaign plans must fully incorporate the ability to operate in a degraded cyber environment; military forces must exercise and be able to conduct military campaigns in a degraded cyber environment where access to networks and data is uncertain.

Reference 9 - 0.21% Coverage

Support the hardening and resiliency of Middle Eastern allies’ and partners’ networks and systems. As a part of its cyber dialogue and partnerships, DoD will work with key Middle Eastern allies and partners to improve their ability to secure their military networks as well as the critical infrastructure and key resources upon which U.S. interests depend.

Reference 10 - 0.20% Coverage

Support the hardening and resiliency of Northeast Asian allies’ networks and   
systems. As a part of its broader cyber dialogue with Asian allies, DoD will work with key allies and partners to improve their ability to secure their military networks and critical infrastructure and key resources upon which U.S. and allied interests depend.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 2 references coded [ 0.10% Coverage]

Reference 1 - 0.05% Coverage

reliable and resilient communications links

Reference 2 - 0.04% Coverage

sustaining a resilient global posture

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 7 references coded [ 0.49% Coverage]

Reference 1 - 0.04% Coverage

These actions are a part of our resilience at home and a source of our influence abroad.

Reference 2 - 0.12% Coverage

Going forward, we will strengthen our foundation by growing our economy, modernizing our defense, upholding our values, enhancing the resilience of our homeland, and promoting talent and diversity in our national security workforce.

Reference 3 - 0.03% Coverage

make sure America is resilient in the face of adversity

Reference 4 - 0.13% Coverage

We are working with the owners and operators of our Nation’s critical cyber and physical infrastructure across every sector—financial, energy, transportation, health, information technology, and more—to decrease vulnerabilities and increase resilience

Reference 5 - 0.05% Coverage

Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet.

Reference 6 - 0.09% Coverage

we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure

Reference 7 - 0.03% Coverage

enhance the resiliency of critical U.S. space capabilities.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 14 references coded [ 2.26% Coverage]

Reference 1 - 0.01% Coverage

Resiliency,

Reference 2 - 0.13% Coverage

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

Reference 3 - 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 4 - 0.19% Coverage

Building strong partnerships with the private sector to promote cybersecurity best practices; assist in building public confidence in cybersecurity measures; and lend credibility to national efforts to increase network resiliency.

Reference 5 - 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 6 - 0.03% Coverage

Defense, Resiliency, and Reconstitution

Reference 7 - 0.24% Coverage

Further, the United States Government invests heavily in improving its own information security and ensuring the resiliency of vital computer systems and networks, including developing the ability to reconstitute them rapidly, operate them in degraded states, or function without them if necessary.

Reference 8 - 0.11% Coverage

In addition to defensive measures, the United States Government must also ensure the resiliency of its networks, systems and data.

Reference 9 - 0.22% Coverage

In 2013, the Administration issued Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, which focused on advancing a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Reference 10 - 0.24% Coverage

Such efforts to improve cybersecurity information sharing and risk management within the government can strengthen both situational awareness and indications and warning, which in turn can help government network defenders prepare for attacks and improve the resilience of government systems.

Reference 11 - 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 12 - 0.11% Coverage

To keep pace, the United States Government must evolve and develop innovative solutions to make cyberspace resilient to future threats

Reference 13 - 0.08% Coverage

continue to improve the resilience of U.S. computers, networks, and critical infrastructure

Reference 14 - 0.22% Coverage

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

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 18 references coded [ 0.94% Coverage]

Reference 1 - 0.05% Coverage

We must build a culture of preparedness and resilience across our governmental functions, critical infrastructure, and economic and political systems.

Reference 2 - 0.05% Coverage

As it evolves, the government and private sector must design systems that incorporate prevention, protection, and resiliency from the start, not as an afterthought.

Reference 3 - 0.08% Coverage

IDENTIFY AND PRIORITIZE RISK: To improve the security and resilience of our critical infrastructure, we will assess risk across six key areas: national security , energy and power, banking and finance, health and safety, communications, and transportation.

Reference 4 - 0.04% Coverage

We will improve our ability to provide uninterrupted and secure communications and services under all conditions.

Reference 5 - 0.05% Coverage

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

Reference 6 - 0.01% Coverage

Promote American Resilience

Reference 7 - 0.09% Coverage

We can, however, help Americans remain resilient in the face of adversity. Resilience includes the ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks, and threats to our economy and democratic system.

Reference 8 - 0.05% Coverage

Reducing risk and building more resilient communities are the best ways to protect people, property, and taxpayer dollars from loss and disruption.

Reference 9 - 0.04% Coverage

Through risk-informed investments, we will build resilient communities and infrastructure to protect and beneﬁ t future generations.

Reference 10 - 0.04% Coverage

A democracy is only as resilient as its people. An informed and engaged citizenry is the fundamental requirement for a free and resilient nation.

Reference 11 - 0.08% Coverage

This Administration will take steps to build a culture of preparedness, informing and empowering communities and individuals to obtain the skills and take the preparatory actions necessary to become more resilient against the threats and hazards that Americans face.

Reference 12 - 0.09% Coverage

To improve the coordination among the private sector and all levels of government that is needed to improve resilience, we must make a stronger commitment to protecting sensitive information so that all partners actively identify and share vulnerabilities and work collaboratively to reduce them.

Reference 13 - 0.05% Coverage

Improvements   
in bandwidth, better broadband connectivity, and protection from persistent cyberattacks are needed to support America’s future growth

Reference 14 - 0.06% Coverage

America’s central position in the global energy system as a leading producer, consumer, and innovator—ensures that markets are free and U.S. infrastructure is resilient and secure.

Reference 15 - 0.04% Coverage

America’s role as an energy exporter will also require an assessment of our vulnerabilities and a resilient American infrastructure.

Reference 16 - 0.02% Coverage

This will require a resilient forward posture and agile global mobility forces.

Reference 17 - 0.04% Coverage

Support for a vibrant domestic manufacturing sector, a solid defense industrial base, and resilient supply chains is a national priority.

Reference 18 - 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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 14 references coded [ 2.90% Coverage]

Reference 1 - 0.08% Coverage

We have required departments and agencies to remove software vulnerable to various security risks.

Reference 2 - 0.18% Coverage

the United   
States have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and   
data as well responding to, and recovering from incidents

Reference 3 - 0.54% Coverage

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

Reference 4 - 0.11% Coverage

OBJECTIVE: Manage cybersecurity risks to increase the security and resilience of the Nation’s information and information systems.

Reference 5 - 0.23% Coverage

ICT providers are in a unique position   
to detect, prevent, and mitigate risk before it impacts their customers, and the Federal Government must work with these providers to improve ICT security and resilience in a targeted and efficient manner while protecting privacy and civil liberties.

Reference 6 - 0.17% Coverage

The Federal Government will update the National Critical Infrastructure Security and Resilience Research and Development Plan to set priorities for addressing cybersecurity risks to critical infrastructure.

Reference 7 - 0.27% Coverage

Departments and agencies will align their investments to the priorities, which will focus on building new cybersecurity approaches technologies,   
improving and building   
that use emerging information-sharing   
and risk management related to cross-sector interdependencies,   
resilience   
to large-scale or long-duration disruptions.

Reference 8 - 0.38% Coverage

Given the criticality of maritime transportation to the United States and global economy and the minimal risk-reduction investments to protect against cyber exploitation made thus far, the United States will move quickly to clarify maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure.

Reference 9 - 0.21% Coverage

The Administration will enhance efforts to protect our space assets and support infrastructure from evolving cyber threats, and we will work with industry and international partners to strengthen the cyber resilience of existing and future space systems.

Reference 10 - 0.04% Coverage

Foster a Vibrant and Resilient Digital Economy

Reference 11 - 0.18% Coverage

To enhance the resilience of cyberspace, the Administration expects the technology marketplace to support and reward the continuous development, adoption, and evolution of innovative security technologies and processes.

Reference 12 - 0.16% Coverage

The United States Government will promote foundational engineering practices to reduce systemic fragility   
and develop designs that   
degrade and recover effectively when successfully attacked.

Reference 13 - 0.17% Coverage

The United States Government will also promote regular testing and exercising of the cybersecurity and resilience of products and systems during development using best practices from forward-leaning industries.

Reference 14 - 0.16% Coverage

This includes promotion and use of coordinated vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack.