Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 11 references coded [ 0.50% Coverage]

Reference 1 - 0.04% Coverage

This strategy recognizes the fundamental connection between our national security, our national competitiveness, resilience, and moral example.

Reference 2 - 0.02% Coverage

These efforts are also tied to our commitment to secure a more resilient nation.

Reference 3 - 0.04% Coverage

We will support the development of prepared, vigilant, and engaged communities and underscore that our citizens are the heart of a resilient country.

Reference 4 - 0.05% Coverage

In addition to facing enemies on traditional battlefields, the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace.

Reference 5 - 0.05% Coverage

At home, we are integrating our homeland security efforts seamlessly with other aspects of our national security approach, and strengthening our preparedness and resilience.

Reference 6 - 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 7 - 0.06% Coverage

When incidents occur, we must show resilience by maintaining critical operations and functions, returning to our normal life, and learning from disasters so that their lessons can be translated into pragmatic changes when necessary.

Reference 8 - 0.05% Coverage

We will emphasize individual and community preparedness and resilience through frequent engagement that provides clear and reliable risk and emergency information to the public.

Reference 9 - 0.04% Coverage

Our efforts to inform and empower Americans and their communities recognize that resilience has always been at the heart of the American spirit.

Reference 10 - 0.04% Coverage

Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient.

Reference 11 - 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 - § 7 references coded [ 0.81% Coverage]

Reference 1 - 0.13% Coverage

At the same time, our networks must be secure and reliable; they must retain the trust of individuals, businesses and governments, and should be resilient to arbitrary or malicious disruption~

Reference 2 - 0.11% Coverage

We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options~

Reference 3 - 0.15% Coverage

Ensuring the resilience of our networks and information systems requires collective and concerted national action that spans the whole of government, in collaboration with the private sector and individual citizens~

Reference 4 - 0.17% Coverage

Developing international, voluntary, consensus-based cybersecurity standards and deploying products, processes, and services based upon such standards are the basis of an interoperable, secure and resilient global infrastructure~

Reference 5 - 0.11% Coverage

They foster innovation; facilitate interoperability, security, and resiliency; improve trust in online transactions; and spur competition in global markets~

Reference 6 - 0.05% Coverage

Protecting Our Networks: Enhancing Security, Reliability, and Resiliency

Reference 7 - 0.07% Coverage

We will expand these capabilities through international collaboration to 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 DoD Cyber Strategy Summary - § 6 references coded [ 3.64% Coverage]

Reference 1 - 0.35% Coverage

We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages.

Reference 2 - 0.78% Coverage

The Department must respond to these activities by exposing, disrupting, and degrading cyber activity threatening U.S. interests, strengthening the cybersecurity and resilience of key potential targets, and working closely with other departments and agencies, as well as with our allies and partners.

Reference 3 - 0.52% Coverage

We will defend forward to halt or degrade cyberspace operations targeting the Department, and we will collaborate to strengthen the cybersecurity and resilience of DoD, DCI, and DIB networks and systems.

Reference 4 - 0.85% Coverage

As the Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI, the Department will: set and enforce standards for cybersecurity, resilience, and reporting; and be prepared, when requested and authorized, to provide direct assistance, including on non-DoD networks, prior to, during, and after an incident.

Reference 5 - 0.70% Coverage

Increase the resilience of U.S. critical infrastructure: The Department will work with its interagency and private sector partners to reduce the risk that malicious cyber activity targeting U.S. critical infrastructure could have catastrophic or cascading consequences.

Reference 6 - 0.44% Coverage

We will streamline our publicprivate information-sharing mechanisms and strengthen the resilience and cybersecurity of critical infrastructure networks and systems.

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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Defense Strategy Summary - § 2 references coded [ 0.73% Coverage]

Reference 1 - 0.32% Coverage

A more lethal, resilient, and rapidly innovating Joint Force, combined with a robust constellation of allies and partners, will sustain American influence and ensure favorable balances of power that safeguard the free and open international order.

Reference 2 - 0.41% Coverage

Space and cyberspace as warfighting domains. The Department will prioritize investments in resilience, reconstitution, and operations to assure our space capabilities. We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 17 references coded [ 1.02% Coverage]

Reference 1 - 0.03% Coverage

Fourth, to ensure our future military advantage, we will build a resilient Joint Force and defense ecosystem.

Reference 2 - 0.04% Coverage

We will make our supporting systems more resilient and agile in the face of threats that range from competitors to the effects of climate change.

Reference 3 - 0.02% Coverage

► Building a resilient Joint Force and defense ecosystem.

Reference 4 - 0.05% Coverage

Deterrence by Resilience. Denying the benefits of aggression also requires resilience – the ability to withstand, fight through, and recover quickly from disruption.

Reference 5 - 0.07% Coverage

The Department will improve its ability to operate in the face of multi-domain attacks on a growing surface of vital networks and critical infrastructure, both in the homeland and in collaboration with Allies and partners at risk.

Reference 6 - 0.03% Coverage

Because the cyber and space domains empower the entire Joint Force, we will prioritize building resilience in these areas.

Reference 7 - 0.03% Coverage

Cyber resilience will be enhanced by, for example, modern encryption and a zero-trust architecture.

Reference 8 - 0.06% Coverage

The Department will take steps to raise potential attackers’ direct and indirect costs while reducing their expected benefits for aggressive action against the homeland, particularly by increasing resilience.

Reference 9 - 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 10 - 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 11 - 0.10% Coverage

Deterring North Korean Attacks. The Department will continue to deter attacks through forward posture; integrated air and missile defense; close coordination and interoperability with our ROK Ally; nuclear deterrence; resilience initiatives; and the potential for direct cost imposition approaches that come from globally deployable Joint Forces.

Reference 12 - 0.09% Coverage

Deterring Iranian Attacks. To deter large-scale Iranian attacks on vital national security interests and partners in the region, the Department will work to increase partner capability and resilience, particularly in air and missile defense, while collaborating with partners to expose Iranian gray zone operations.

Reference 13 - 0.09% Coverage

We will strengthen strategic stability through dialogue with competitors, unilateral measures that make command, control, and communications more robust, and by developing defenses and architectural   
10 2022 NATIONAL DEFENSE STRATEGY   
resilience to maintain operational capabilities in cyberspace and space during conflict.

Reference 14 - 0.04% Coverage

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

Reference 15 - 0.07% Coverage

The Department will maintain its bedrock commitment to NATO collective security, working alongside Allies and partners to deter, defend, and build resilience against further Russian military aggression and acute forms of gray zone coercion.

Reference 16 - 0.09% Coverage

The Department will collaborate with Allies and partners to build capacity along Europe’s eastern flank, strengthening defensive antiarea/access-denial capabilities and indications and warning; expanding readiness, training, and exercises; and promoting resilience, including against hybrid and cyber actions.

Reference 17 - 0.07% Coverage

To preserve command, control, and communications in a fast-paced battlefield, we will make our network architectures more resilient against system-level exploitation and disruption so as to ensure effective coordination of distributed forces.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 2 references coded [ 1.10% Coverage]

Reference 1 - 0.60% Coverage

9. BUILD A RESILIENT JOINT FORCE   
Harness robust and effective combat capabilities that can resist degradation and quickly reconstitute in future combat.

Reference 2 - 0.49% Coverage

 Focus technical and non-technical modernization into a resilient Joint Force and maintain the ability to respond to crises.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 13 references coded [ 0.78% Coverage]

Reference 1 - 0.04% Coverage

That is why we must make far-reaching investments in the sources of our natural strength while building our resilience.

Reference 2 - 0.07% Coverage

We are identifying and investing in key areas where private industry, on its own, has not mobilized to protect our core economic and national security interests, including bolstering our national resilience.

Reference 3 - 0.06% Coverage

As we do this work, we are also protecting our investments and bolstering their resilience through tracking, attributing, and defending against the activities of malicious actors in cyberspace.

Reference 4 - 0.03% Coverage

This stronger workforce will also build enduring advantages that bolster our strength and resilience.

Reference 5 - 0.10% Coverage

This framework’s four pillars— trade and the digital economy, supply chains and resilience, clean energy and decarbonization,   
18 NATIONAL SECURITY STRATEGY   
        
and tax and anticorruption—will allow this partnership to determine the rules of the road for an economically vital region, and therefore the global economy.

Reference 6 - 0.04% Coverage

And, we will build a resilient force and defense ecosystem to ensure we can perform these functions for decades to come.

Reference 7 - 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 8 - 0.05% Coverage

Our strategy toward the PRC is threefold: 1) to invest in the foundations of our strength at home – our competitiveness, our innovation, our resilience, our democracy

Reference 9 - 0.04% Coverage

And we are renewing our focus on bolstering our collective resilience against shared threats from Russia, including asymmetric threats.

Reference 10 - 0.08% Coverage

That requires working with a broad range of partners to   
NATIONAL SECURITY STRATEGY 33   
        
advance network infrastructure resilience in 5G and other advanced communication technologies, including by promoting vendor diversity and securing supply chains.

Reference 11 - 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 12 - 0.04% Coverage

We will enhance the resilience of U.S. space systems that we rely on for critical national and homeland security functions.

Reference 13 - 0.09% Coverage

By enhancing our industrial capacity, investing in our people, and strengthening our democracy, we will have strengthened the foundation of our economy, bolstered our national resilience, enhanced our credibility on the world stage, and ensured our competitive advantages.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 9 references coded [ 2.53% Coverage]

Reference 1 - 0.19% Coverage

The Department will enhance the cyber resilience of the Joint Force and ensure its ability to fight in and through contested and congested cyberspace.

Reference 2 - 0.23% Coverage

While these efforts have yielded   
4 2 0 2 3 C Y B E R S T R A T E G Y   
limited results, this is due largely to the resilience of Ukrainian networks and support from the international community.

Reference 3 - 0.34% Coverage

We will track the organization, capabilities, and intent of malicious cyber actors. We will leverage these insights to bolster the cyber resilience of the Nation and will coordinate with interagency partners to publicize this information as circumstances permit.

Reference 4 - 0.27% Coverage

The Department will support whole-of-Government efforts to raise U.S. cybersecurity standards in order to increase resilience and make it more difficult for adversaries to disrupt these essential services.

Reference 5 - 0.41% Coverage

The Department will use cyberspace operations to enable and empower the Joint Force. These efforts will unfold in multiple ways: through persistent campaigning below the level of armed conflict1, through cyber defense and the fostering of cyber resilience, and through support of campaign and contingency planning.

Reference 6 - 0.24% Coverage

The Department will be resilient against malicious cyber activity and ready to operate in congested and contested cyberspace. This effort will be grounded in our defense of the DODIN.

Reference 7 - 0.51% Coverage

Build Cyber Resilience in the Joint Force   
The Department will enhance the cyber resilience of the Joint Force and ensure its ability to fight in and through contested and congested cyberspace. We will prioritize those cyber capabilities that support the Joint Force’s military mission assurance and commit to training the force to operate amid network and warfighting platform degradation.

Reference 8 - 0.14% Coverage

They have also bolstered the cyber resilience of Allies and partners by exposing hostile TTPs and malware.

Reference 9 - 0.20% Coverage

We will defend forward, disrupting and degrading malicious cyber actors, and help ensure the resilience of the homeland with all tools at our disposal.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 53 references coded [ 4.54% Coverage]

Reference 1 - 0.03% Coverage

PILLAR THREE | SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE

Reference 2 - 0.02% Coverage

PILLAR FOUR | INVEST IN A RESILIENT FUTURE

Reference 3 - 0.08% Coverage

We are building a smart grid, powered by distributed renewable electricity and balanced with intelligent systems, that promises a bright and resilient future of energy abundance.

Reference 4 - 0.07% Coverage

Achieving this vision of a prosperous, connected future will depend upon the cybersecurity and resilience of its underlying technologies and systems.

Reference 5 - 0.12% Coverage

Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences.

Reference 6 - 0.10% Coverage

This strategy will position the United States and its allies and partners to build that digital ecosystem together, making it more easily and inherently defensible, resilient, and aligned with our values.

Reference 7 - 0.07% Coverage

Too often, we are layering new functionality and technology onto already intricate and brittle systems at the expense of security and resilience.

Reference 8 - 0.12% Coverage

OUR APPROACH: A PATH TO RESILIENCE IN CYBERSPACE   
Deep and enduring collaboration between stakeholders across our digital ecosystem will be the foundation upon which we make it more inherently defensible, resilient, and aligned with U.S. values.

Reference 9 - 0.03% Coverage

(3) Shape Market Forces to Drive Security and Resilience

Reference 10 - 0.01% Coverage

(4) Invest in a Resilient Future

Reference 11 - 0.06% Coverage

Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens.

Reference 12 - 0.08% Coverage

Instead, across both the public and private sectors, we must ask more of the most capable and bestpositioned actors to make our digital ecosystem secure and resilient.

Reference 13 - 0.07% Coverage

We must defend the systems we have now, while investing in and building toward a future digital ecosystem that is more inherently defensible and resilient.

Reference 14 - 0.16% Coverage

We must ensure that market forces and public programs alike reward security and resilience, build a robust and diverse cyber workforce, embrace security and resilience by design, strategically coordinate research and development investments in cybersecurity, and promote the collaborative stewardship of our digital ecosystem.

Reference 15 - 0.09% Coverage

To achieve these goals, the Federal Government will focus on points of leverage, where minimally invasive actions will produce the greatest gains in defensibility and systemic resilience.

Reference 16 - 0.08% Coverage

The United States has an opportunity to rebalance the incentives necessary to lay a stronger, more resilient foundation on which to build the future of our digital ecosystem.

Reference 17 - 0.05% Coverage

The Administration remains committed to enhancing the security and resilience of U.S. space systems

Reference 18 - 0.07% Coverage

The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides.

Reference 19 - 0.11% Coverage

We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem.

Reference 20 - 0.07% Coverage

Finally, the Federal Government can better support the defense of critical infrastructure by making its own systems more defensible and resilient.

Reference 21 - 0.08% Coverage

In doing so, Federal cybersecurity can be a model for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems.

Reference 22 - 0.06% Coverage

Regulation can level the playing field, enabling healthy competition without sacrificing cybersecurity or operational resilience.

Reference 23 - 0.10% Coverage

A collaborative process between industry and regulators will produce regulatory requirements that are operationally and commercially viable and will ensure the safe and resilient operation of critical infrastructure.

Reference 24 - 0.06% Coverage

Further, these and other critical sectors rely upon the cybersecurity and resilience of their third-party service providers.

Reference 25 - 0.09% Coverage

Cloud-based services enable better and more economical cybersecurity practices at scale, but they are also essential to operational resilience across many critical infrastructure sectors.

Reference 26 - 0.08% Coverage

Effective regulations minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets.

Reference 27 - 0.04% Coverage

CISA is the national coordinator for critical infrastructure security and resilience.

Reference 28 - 0.06% Coverage

SRMAs have day-to-day responsibility and sector-specific expertise to improve security and resilience within their sectors.

Reference 29 - 0.08% Coverage

Investment by the Federal Government in building out the capabilities of SRMAs will enable security and resilience improvements across critical infrastructure.

Reference 30 - 0.11% Coverage

The Federal Government will also deepen operational and strategic collaboration with software, hardware, and managed service providers with the capability to reshape the cyber landscape in favor of greater security and resilience.

Reference 31 - 0.08% Coverage

By making its   
NAT I ONAL CY B E RS E CU RI T Y S T RATEGY 12   
        
own networks more defensible and resilient, the Federal Government will be a model for private sector emulation.

Reference 32 - 0.14% Coverage

Replacing legacy systems with more secure technology, including through accelerating migration to cloud-based services, will elevate the cybersecurity posture across the Federal Government and, in turn, improve the security and resilience of the digital services it provides to the American people.

Reference 33 - 0.04% Coverage

(3) bolstering critical infrastructure resilience to withstand ransomware attacks

Reference 34 - 0.03% Coverage

The CRI has conducted global exercises to build resilience

Reference 35 - 0.03% Coverage

PILLAR THREE | SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE

Reference 36 - 0.08% Coverage

To build the secure and resilient future we want, we must shape market forces to place responsibility on those within our digital ecosystem that are best positioned to reduce risk.

Reference 37 - 0.08% Coverage

Our goal is a modern digital economy that promotes practices that enhance the security and resilience of our digital ecosystem while preserving innovation and competition.

Reference 38 - 0.10% Coverage

Continued disruptions of critical infrastructure and thefts of personal data make clear that market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience.

Reference 39 - 0.09% Coverage

To address these challenges, the Administration will shape the long-term security and resilience of the digital ecosystem, against both today’s threats and tomorrow’s challenges.

Reference 40 - 0.10% Coverage

Federal grant programs offer strategic opportunities to make investments in critical infrastructure that are designed, developed, fielded, and maintained with cybersecurity and all-hazards resilience in mind.

Reference 41 - 0.06% Coverage

This Administration is committed to making investments in a manner that increases our collective systemic resilience.

Reference 42 - 0.12% Coverage

Together, we can drive investment in critical products and services that are secure- and resilient-by-design, and sustain and incentivize security and resilience throughout the lifecycle of   
21 NAT I ONAL CY B E RS E CU RI T Y S T RATEGY   
        
critical infrastructure.

Reference 43 - 0.10% Coverage

The Federal Government will also prioritize funding for cybersecurity research, development, and demonstration (RD&D) programs aimed at strengthening critical infrastructure cybersecurity and resilience.

Reference 44 - 0.06% Coverage

PILLAR FOUR | INVEST IN A RESILIENT FUTURE   
A resilient and flourishing digital future tomorrow begins with investments made today.

Reference 45 - 0.08% Coverage

We can build a more secure, resilient, privacy-preserving, and equitable digital ecosystem through strategic investments and coordinated, collaborative action.

Reference 46 - 0.08% Coverage

We will ensure that resilience is not a discretionary element of new technical capabilities but a commercially viable element of the innovation and deployment process.

Reference 47 - 0.12% Coverage

Through Federal efforts to prioritize research and development in defensible and resilient architectures and reduce vulnerabilities in underlying technologies, we can ensure that the technologies of tomorrow are more secure than those of today.

Reference 48 - 0.15% Coverage

Departments and agencies will direct RD&D projects to advance cybersecurity and resilience in areas such as artificial intelligence, operational technologies and industrial control systems, cloud infrastructure, telecommunications, encryption, system transparency, and data analytics used in critical infrastructure.

Reference 49 - 0.12% Coverage

Our accelerating national transition to a clean energy future is bringing online a new generation of interconnected hardware and software systems that have the potential to strengthen the resiliency, safety, and efficiency of the U.S. electric grid.

Reference 50 - 0.12% Coverage

It will address the need for cybersecurity expertise across all sectors of the economy, with a special focus on critical infrastructure, and will enable the American workforce to continue to innovate in secure and resilient next-generation technologies.

Reference 51 - 0.18% Coverage

To counter common threats, preserve and reinforce global Internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community.

Reference 52 - 0.24% Coverage

The Indo-Pacific Economic Framework for Prosperity (IPEF) and the Americas Partnership for Economic Prosperity (APEP) create opportunities for the United States and regional governments to collaborate in setting rules of the road for the digital economy, including facilitating the development of technical standards, mechanisms to enable cross-border data flows that protect privacy while avoiding strict data localization requirements, and actions to foster supply chain security and resilience.

Reference 53 - 0.12% Coverage

Extending this model to other critical technologies will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more secure, resilient, and trustworthy.

**Annotations**

1 First direct linkage between persistence and campaigning.