Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 17 references coded [ 0.39% Coverage]

Reference 1 - 0.01% Coverage

globally-interconnected

Reference 2 - 0.01% Coverage

interconnectivity.

Reference 3 - 0.01% Coverage

globally-interconnected

Reference 4 - 0.01% Coverage

connectivity

Reference 5 - 0.01% Coverage

Internet as a primary means of interconnectivity

Reference 6 - 0.01% Coverage

interconnectivity

Reference 7 - 0.01% Coverage

interconnected networks

Reference 8 - 0.09% Coverage

“[M]ultiple vendors’products are used to configure U.S. telecommunications infrastructure and deliver services … that cross provider boundaries. As a result of the industry’s shift to a horizontal structure and its fragmentation into a large number of firms, neither vendors nor service providers are prepared to take responsibility for end-to-end systems design.”

Reference 9 - 0.06% Coverage

movement of data across jurisdictional boundaries presents challenges for law enforcement, the protection of privacy and civil liberties as defined by different countries, and liability decisions in the event of data or network breaches

Reference 10 - 0.01% Coverage

interconnected

References 11-12 - 0.03% Coverage

The United States cannot succeed by acting in isolation, because cyberspace crosses geographic and jurisdictional boundaries.

References 13-15 - 0.04% Coverage

The first popular computers for the mass consumer market first emerged in the early 1980s, coincident in time with the emergence of the Internet as a global network-of-networks

Reference 16 - 0.01% Coverage

interconnect

Reference 17 - 0.12% Coverage

wireless broadband network infrastructures have been (and continue to be) deployed that provide an increasingly diverse array of applications and services to both commercial and individual users, accessible over a growing variety of fixed and mobile devices. They support the clearing of billions of dollars in transactions among financial institutions, trading on exchanges, online banking, e-commerce, as well as billing and account management for many retailers and service providers;

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 10 references coded [ 0.33% Coverage]

Reference 1 - 0.02% Coverage

power, in an interconnected world, is no longer a zero sum game

Reference 2 - 0.01% Coverage

interconnected,

Reference 3 - 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 4 - 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

Reference 5 - 0.02% Coverage

Their support networks have global reach and are not contained by national borders

Reference 6 - 0.02% Coverage

The threat of contagious disease transcends political boundaries

Reference 7 - 0.05% Coverage

These threats cross borders and continents and undermine the stability of nations, subverting government institutions through corruption and harming citizens worldwide.

References 8-9 - 0.06% Coverage

These shared areas, which exist outside exclusive national jurisdictions, are the connective tissue around our globe upon which all nations’ security   
★ 49 ★   
NaTIONal SeCurITy STraTegy   
and prosperity depend

Reference 10 - 0.06% Coverage

Many of these goals are equally applicable to cyberspace. While cyberspace relies on the digital infrastructure of individual countries, such infrastructure is globally connected, and securing it requires global cooperation

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 12 references coded [ 2.41% Coverage]

Reference 1 - 0.15% Coverage

. Individuals and communities worldwide   
connect, socialize, and organize themselves in and through cyberspac

Reference 2 - 0.17% Coverage

. As Internet usage continues to expand, cyberspace will become increasingly woven into the fabric of everyday life across the globe

Reference 3 - 0.02% Coverage

r exploitation

Reference 4 - 0.11% Coverage

y foreign nations are working to exploit DoD unclassified and classified network

Reference 5 - 0.16% Coverage

The global scope of DoD networks and systems presents adversaries with broad opportunities for exploitation and attack.

Reference 6 - 0.04% Coverage

theft or exploitation of data

Reference 7 - 0.26% Coverage

Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption.

Reference 8 - 0.25% Coverage

“Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space.” - 2010 Quadrennial Defense Review1

Reference 9 - 0.30% Coverage

Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD’s national security missions.

Reference 10 - 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 11 - 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.

Reference 12 - 0.12% Coverage

extend across national boundaries and through multiple components of the global economy.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 13 references coded [ 1.27% Coverage]

Reference 1 - 0.03% Coverage

increasing interconnectedness

References 2-3 - 0.07% Coverage

The space environment is becoming more congested, contested, and competitive.

Reference 4 - 0.11% Coverage

Some states are conducting or condoning cyber intrusions that foreshadow the growing threat in this globally connected domain.

Reference 5 - 0.11% Coverage

U.S. foreign policy and the international security architecture must continue to adapt to this dynamic security environment

Reference 6 - 0.19% Coverage

A prosperous and interconnected world requires a stable and secure environment, the absence of territorial aggression or conflict between states, and reliable access to resources and cyberspace for stable markets

Reference 7 - 0.03% Coverage

global economy’s interconnectedness

Reference 8 - 0.08% Coverage

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

Reference 9 - 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 10 - 0.12% Coverage

The global commons and globally connected domains constitute the connective tissue upon which all nations’ security and prosperity depend.

Reference 11 - 0.18% Coverage

The interlinked domains of air, space, and cyberspace allow for the high-speed, high-volume exchange of people, ideas, goods, information and capital that are equally critical to the global economy.

Reference 12 - 0.11% Coverage

The United States faces persistent, widespread, and growing threats from state and non-state actors in space and cyberspace

Reference 13 - 0.08% Coverage

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

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 29 references coded [ 1.30% Coverage]

Reference 1 - 0.10% Coverage

“This world—cyberspace—is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history.”

Reference 2 - 0.03% Coverage

integrity of the interconnected networks

Reference 3 - 0.03% Coverage

resilient to arbitrary or malicious disruption

Reference 4 - 0.07% Coverage

We have also witnessed offline challenges, like exploitation and aggression, move into cyberspace~

Reference 5 - 0.03% Coverage

These challenges transcend national borders

Reference 6 - 0.04% Coverage

The best cybersecurity solutions are dynamic and adaptable,

Reference 7 - 0.14% Coverage

Computers can communicate with one another across a seamless landscape of global networks permitting trusted, instantaneous communication with friends and colleagues down the block or around the world~

Reference 8 - 0.03% Coverage

flows freely beyond national borders

Reference 9 - 0.01% Coverage

interconnection~

Reference 10 - 0.04% Coverage

nternationally interconnected infrastructure~

Reference 11 - 0.03% Coverage

cyberspace is a dynamic environment

Reference 12 - 0.03% Coverage

national and international network resilience

Reference 13 - 0.05% Coverage

Ensuring the resilience of our networks and information systems

Reference 14 - 0.01% Coverage

interconnection

Reference 15 - 0.02% Coverage

exploiting our networks

Reference 16 - 0.04% Coverage

interconnected networks link nations more closely,

Reference 17 - 0.05% Coverage

an attack on one nation’s networks may have impact far beyond its borders

Reference 18 - 0.02% Coverage

globally interconnected networks

Reference 19 - 0.02% Coverage

cooperate across borders

Reference 20 - 0.08% Coverage

In an interconnected global environment, weak security in one nation’s systems compounds the risk to others~

Reference 21 - 0.02% Coverage

enhance overall resilience

Reference 22 - 0.07% Coverage

Exploitation of these vulnerabilities impairs economic performance and national security

Reference 23 - 0.02% Coverage

exploit online systems,

Reference 24 - 0.05% Coverage

exploit the Internet for operational planning, financing, or attacks

Reference 25 - 0.01% Coverage

exploit our networks

Reference 26 - 0.11% Coverage

the interconnected nature of networked systems of our closest allies, such as those of NATO and its member states, creates opportunities and new risks~

References 27-28 - 0.06% Coverage

The benefits of an interconnected world should not be limited by national borders~

Reference 29 - 0.09% Coverage

expectation that under normal circumstances, data will flow across borders without regard for its national origin or destination~

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review CLEAN - § 3 references coded [ 0.08% Coverage]

Reference 1 - 0.06% Coverage

modern warfare is evolving rapidly, leading to increasingly contested battlespace in the air, sea, and space domains – as well as cyberspace – in which our forces enjoyed dominance in our most recent conflicts.

Reference 2 - 0.01% Coverage

more resilient systems and system architectures

Reference 3 - 0.01% Coverage

resilient architectures,

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 DOD Cyber Strategy CLEAN - § 3 references coded [ 0.30% Coverage]

Reference 1 - 0.08% Coverage

Computer code blurs the line between the cyber and physical world and connects millions of objects to the Internet or private networks.

Reference 2 - 0.10% Coverage

Without strong investments in cybersecurity and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack.

Reference 3 - 0.12% Coverage

And an actor in one region of the globe can use cyber capabilities to strike directly at a network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 5 references coded [ 0.40% Coverage]

Reference 1 - 0.04% Coverage

global   
information environment

Reference 2 - 0.05% Coverage

reliable and resilient communications links

Reference 3 - 0.04% Coverage

sustaining a resilient global posture

Reference 4 - 0.07% Coverage

our future force will have to operate in contested environments.

Reference 5 - 0.19% Coverage

The results of these initiatives — particularly the enhanced connectivity and cybersecurity provided by the JIE — will provide the foundation for future interoperability.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 8 references coded [ 0.58% 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 - 0.09% Coverage

It establishes instead a diversified and balanced set of priorities appropriate for the world’s leading global power with interests in every part of an increasingly interconnected world.

Reference 4 - 0.03% Coverage

make sure America is resilient in the face of adversity

Reference 5 - 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 6 - 0.05% Coverage

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

Reference 7 - 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 8 - 0.03% Coverage

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

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 21 references coded [ 3.07% Coverage]

Reference 1 - 0.01% Coverage

Resiliency,

Reference 2 - 0.09% Coverage

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

Reference 3 - 0.10% Coverage

the full spectrum of operational capabilities requires resources, persistence, and access to technological expertise

Reference 4 - 0.09% Coverage

Supply-chain operations seek to exploit access to products and services provided to the intended victim.

Reference 5 - 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 6 - 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 7 - 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 8 - 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 9 - 0.03% Coverage

Defense, Resiliency, and Reconstitution

Reference 10 - 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 11 - 0.20% Coverage

Shared situational awareness of cyber threats and indicators of malicious cyber activity – including information on those responsible – provides network defenders the opportunity to close known vulnerabilities before they can be fully exploited.

Reference 12 - 0.11% Coverage

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

Reference 13 - 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 14 - 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 15 - 0.13% Coverage

Combating cybercrime is not only a domestic issue. Many adversaries use foreign-based infrastructure to stage their intrusions or disruptive activities.

Reference 16 - 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 17 - 0.10% Coverage

The asymmetric advantages granted to malicious cyber actors reward competition, not cooperation, among nation-states.

Reference 18 - 0.11% Coverage

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

Reference 19 - 0.08% Coverage

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

Reference 20 - 0.11% Coverage

increased connectivity between critical infrastructure and the Internet are factors that create additional enablers for cyber attacks.

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.

**Annotations**

1 QDR Quote: Cyberspace as a man-made domain as critical as the other four physical domains.