Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 14 references coded [ 1.18% Coverage]

Reference 1 - 0.11% Coverage

Information and communications networks are largely owned and operated by the private sector, both nationally and internationally. Thus, addressing network security issues requires a publicprivate partnership as well as international cooperation and norms. The United States needs a comprehensive framework to ensure coordinated response and recovery by the government, the private sector, and our allies to a significant incident or threat.

Reference 2 - 0.17% Coverage

The review team reached out to a wide array of stakeholders inside and outside the Federal government. The review team sought to be transparent by engaging a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches to identify and assess other relevant programs and issues. Recognizing that there are opportunities for everyone—academia, industry, and government—to work together to build a trusted and resilient communications and information infrastructure, the review team engaged these stakeholders about the scope of the reviews and asked for input on pertinent areas of interest.

Reference 3 - 0.05% Coverage

The public and private sectors’ interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend.

Reference 4 - 0.14% Coverage

The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of their citizens. The private sector, however, designs, builds, owns, and operates most of the network infrastructures that support government and private users alike. Industry and governments share the responsibility for the security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies.

Reference 5 - 0.15% Coverage

the diffusion of effort has left some participants frustrated with unclear delineation of roles and responsibilities, uneven capabilities across various groups, and a proliferation of plans and recommendations. As a result, government and private-sector personnel, time, and resources are spread across a host of bodies engaged in sometimes duplicative or inconsistent efforts. Partnerships must evolve to clearly define the nature of the relationship, the roles and responsibilities of various groups and their participants, the expectations of each party’s contribution, and accountability mechanisms

Reference 6 - 0.07% Coverage

As part of the partnership, government should work creatively and collaboratively with the private sector to identify tailored solutions that take into account both the need to exchange information and protect public and private interests and take an integrated approach to national and economic security.

Reference 7 - 0.11% Coverage

More than a dozen international organizations—including the United   
Nations, the Group of Eight, NATO, the Council of Europe, the Asia-Pacific Economic Cooperation forum, the Organization of American States, the Organization for Economic Cooperation and Development, the InternationalTelecommunicationUnion (ITU), and the InternationalOrganization for Standardization (ISO)—address issues concerning the information and communications infrastructure.56

Reference 8 - 0.04% Coverage

The sheer number, variety, and differing focuses of these venues strain the capacity of many governments, including the United States, to engage adequately.

Reference 9 - 0.06% Coverage

The Federal government—in collaboration with State, local, and tribal governments and industry— should develop a set of threat scenarios and metrics that all can use for risk management decisions, recovery planning, and prioritization of R&D.

Reference 10 - 0.06% Coverage

The Federal government, in collaboration with the private sector and other stakeholders, also should use the infrastructure objectives and the R&D framework to help define goals for national and international standardsbodies.

Reference 11 - 0.03% Coverage

The Federal government—in collaboration with industry and the civil liberties and privacy communities—

Reference 12 - 0.06% Coverage

Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.

Reference 13 - 0.11% Coverage

The U.S. depends upon a privately owned, globally operated digital infrastructure. The review team engaged with industry to continue building the foundation of a trusted partnership. This engagement underscored the importance of developing value propositions that are understood by both government and industry partners. It also made clear that increasing information sharing is not enough; the government must foster an environment for collaboration.

Reference 14 - 0.03% Coverage

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

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 7 references coded [ 0.31% Coverage]

Reference 1 - 0.02% Coverage

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

Reference 2 - 0.06% Coverage

challenged state based international institutions that were largely designed in the wake of World War II by policymakers who had different challenges in mind. Nonstate actors can have a dramatic influence on the world around them

Reference 3 - 0.01% Coverage

More actors exert power and influence

Reference 4 - 0.04% Coverage

Meanwhile, individuals, corporations, and civil society play an increasingly important role in shaping events around the world.

Reference 5 - 0.02% Coverage

Competition among states endures, but instead of a single nuclear adversary

Reference 6 - 0.10% Coverage

Instead of a hostile expansionist empire, we now face a diverse array of challenges, from a loose network of violent extremists to states that flout international norms or face internal collapse. 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 7 - 0.06% Coverage

Transnational criminal organizations have accumulated unprecedented wealth and power through trafficking and other illicit activities, penetrating legitimate financial systems and destabilizing commercial markets.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 4 references coded [ 0.80% Coverage]

Reference 1 - 0.20% Coverage

DoD must address vulnerabilities and the concerted efforts of both state and non-state actors to gain unauthorized access to its networks and systems.

Reference 2 - 0.23% Coverage

“Neither government nor the private sector nor individual citizens can meet this challenge alone– we will expand the ways we work together.”   
- 2010 National Security Strategy1

Reference 3 - 0.26% Coverage

The challenges of cyberspace cross sectors, industries, and U.S. government departments and agencies; they extend across national boundaries and through multiple components of the global economy.

Reference 4 - 0.11% Coverage

no single state or organization can maintain effective cyber defenses on its own.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 6 references coded [ 1.13% Coverage]

Reference 1 - 0.13% Coverage

The United States remains the world’s preeminent power, even as a growing number of state and non-state actors exhibit consequential influence.

Reference 2 - 0.23% Coverage

This changing distribution of power indicates evolution to a "multi-nodal" world characterized more by shifting, interest-driven coalitions based on   
diplomatic, military, and economic power, than by rigid security competition between opposing blocs.

Reference 3 - 0.22% Coverage

Energy-state relationships will intersect geopolitical concerns as state-run companies will control an increasing share of the world’s hydrocarbon resources and the persistent challenge of resource scarcity may overlap with territorial disputes.

Reference 4 - 0.24% Coverage

Non-state actors such as criminal organizations, traffickers, and terrorist groups find a nexus of interests in exploiting the commons. States are developing anti-access and area-denial capabilities and strategies to constrain U.S. and international freedom of action.

Reference 5 - 0.18% Coverage

Non-state Actors – State-sponsored and non-state actors complicate deterrence and accountability by extending their reach through advanced technologies that were once solely the domain of states.

Reference 6 - 0.14% Coverage

We must identify and encourage states and regional organizations that have demonstrated a leadership role to continue to contribute to Africa’s security.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 7 references coded [ 1.12% Coverage]

Reference 1 - 0.18% Coverage

In the international arena in particular, states have an enduring role to play in preserving peace and stability, empowering innovation, safeguarding economic and national security interests, and protecting and promoting the individual rights of citizens~

Reference 2 - 0.15% Coverage

Although the private sector already plays an important role in international and multi-stakeholder organizations, we will continue to leverage existing partnership mechanisms to engage with industry partners~

Reference 3 - 0.15% Coverage

We also seek the private sector’s participation in Internet governance as essential to upholding its multi-stakeholder character, and will continue to advocate for inclusiveness in fora that take up such issues~

Reference 4 - 0.10% Coverage

we continually seek new ways to strengthen our partnership with the private sector to enhance the security of the systems on which we both rely~

Reference 5 - 0.18% Coverage

Much of this capacity will result from private-sector investment, and the United States will work with governments and industry to build a climate friendly to those efforts, and in which they can be leveraged to address countries’ core development needs~

Reference 6 - 0.18% 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—including between government and industry~

Reference 7 - 0.18% Coverage

we will continue to support successful venues like the Internet Governance Forum, which embodies the open and inclusive nature of the Internet itself by allowing nongovernment stakeholders to contribute to the discussion on equal footing with governments~

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 2 references coded [ 0.07% Coverage]

Reference 1 - 0.04% Coverage

shape an international system that is no longer easily defined—one in which the United States will remain the most powerful actor but must increasingly work with key allies and partners if it is to sustain stability and peace.

Reference 2 - 0.03% Coverage

As technological innovation and global information flows accelerate, non-state actors will continue to gain influence and capabilities that, during the past century, remained largely the purview of states.

**Annotations**

1 Refers back to 2010 NSS, quoting a NLI core concept of states sharing power with non-state entitiesl