Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 8 references coded [ 0.51% Coverage]

Reference 1 - 0.08% Coverage

This interconnection has empowered individuals for good and ill, and 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 2 - 0.04% Coverage

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

Reference 3 - 0.05% Coverage

In the 21st century, the ability of individuals and nongovernment actors to play a positive role in shaping the international environment represents a distinct opportunity for the United States.

Reference 4 - 0.06% Coverage

Competition among states endures, but instead of a single nuclear adversary, the United States is now threatened by the potential spread of nuclear weapons to extremists who may not be deterred from using them.

Reference 5 - 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 6 - 0.04% Coverage

The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states.

Reference 7 - 0.05% Coverage

We depend on U.S. overseas laboratories, relationships with host nation governments, and the willingness of states to share health data with nongovernmental and international organizations.

Reference 8 - 0.09% Coverage

Transnational criminal organizations have accumulated unprecedented wealth and power through trafficking and other illicit activities, penetrating legitimate financial systems and destabilizing commercial markets. They extend their reach by forming alliances with government officials and some state security services.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 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.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 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\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 7 references coded [ 1.39% Coverage]

Reference 1 - 0.10% Coverage

Multi-stakeholder Governance: Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders~

Reference 2 - 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 3 - 0.30% Coverage

In Internet governance policy, important steps have been made to ensure responsiveness and international representation in key organizations~ The United States salutes those efforts, and will continue to recognize the unique contribution of such fora that represent the entire Internet community by integrating the private sector, civil society, academia, as well as governments in a multi-stakeholder environment~

Reference 4 - 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 5 - 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 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 - 0.33% Coverage

The United States stands firm in our conviction that when the international community meets to discuss the range of Internet governance issues, these conversations must take place in a multi-stakeholder manner; 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\\CS1\_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\\CS1\_Secondary Sources\_Authoritative\\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\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 12 references coded [ 1.57% Coverage]

Reference 1 - 0.11% Coverage

Yet these same qualities of openness and dynamism that led to the Internet’s rapid expansion now provide dangerous state and non-state actors with a means to undermine U.S. interests.

Reference 2 - 0.07% Coverage

State and non-state actors conduct cyber operations to achieve a variety of political, economic, or military objectives.

Reference 3 - 0.08% Coverage

Vulnerable data systems present state and non-state actors with an enticing opportunity to strike the United States and its interests.

Reference 4 - 0.13% Coverage

Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate.

Reference 5 - 0.15% Coverage

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

Reference 6 - 0.11% Coverage

State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators.

Reference 7 - 0.14% Coverage

A nation-state, non-state group, or individual actor can purchase destructive malware and other capabilities on the black market. State and non-state actors also pay experts to search for vulnerabilities and develop exploits.

Reference 8 - 0.13% Coverage

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

Reference 9 - 0.15% Coverage

In the face of an escalating threat, the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests.

Reference 10 - 0.16% Coverage

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

Reference 11 - 0.20% Coverage

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

Reference 12 - 0.14% Coverage

State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States’ technological and military advantage.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 8 references coded [ 1.82% Coverage]

Reference 1 - 0.21% Coverage

We now face multiple, simultaneous security challenges from traditional state actors and transregional networks of sub-state groups – all taking advantage of rapid technological change.

Reference 2 - 0.20% Coverage

But it also asserts that the application of the military instrument of power against state   
threats is very different than the application of military power against non-state threats.

Reference 3 - 0.10% Coverage

violent extremist organizations (VEOs) that are undermining transregional security

Reference 4 - 0.22% Coverage

Individuals and groups today have access to more information than entire governments once possessed. They can swiftly organize and act on what they learn, sometimes leading to violent change.

Reference 5 - 0.21% Coverage

Despite these changes, states remain the international system’s dominant actors. They   
are preeminent in their capability to harness power, focus human endeavors, and provide security.

Reference 6 - 0.27% Coverage

In this complex strategic security environment, the U.S. military does not have the   
luxury of focusing on one challenge to the exclusion of others. It must provide a full range of military options for addressing both revisionist states and VEOs.

Reference 7 - 0.44% Coverage

Overlapping state and non-state violence, there exists an area of conflict where actors blend techniques, capabilities, and resources to achieve their objectives. Such “hybrid” conflicts may consist of military forces assuming a non-state identity, as Russia did in the Crimea, or involve a VEO fielding rudimentary combined arms capabilities, as ISIL has demonstrated in Iraq and Syria.

Reference 8 - 0.17% Coverage

To win against the diverse range of state and non-state threats confronting us, we must think innovatively, challenge assumptions, and embrace change.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 6 references coded [ 0.77% Coverage]

Reference 1 - 0.13% Coverage

Now, at this pivotal moment, we continue to face serious challenges to our national security, even as we are working to shape the opportunities of tomorrow. Violent extremism and an evolving terrorist threat raise a persistent risk of attacks on America and our allies.

Reference 2 - 0.14% Coverage

Yet, we will continuously expand the scope of cooperation to encompass other state partners, non-state and private actors, and international institutions—particularly the United Nations (U.N.), international financial institutions, and key regional organizations.

Reference 3 - 0.15% Coverage

Second, power is shifting below and beyond the nation-state. Governments once able to operate with few checks and balances are increasingly expected to be more accountable to sub-state and non-state actors—from mayors of mega-cities and leaders in private industry to a more empowered civil society.

Reference 4 - 0.06% Coverage

expanding partnerships with the private sector in support of missions and capabilities previously claimed by governments alone.

Reference 5 - 0.12% Coverage

We will also keep our edge by opening our national labs to more commercial partnerships while tapping research and development in the private sector, including a wide range of start-ups and firms at the leading edge of America’s innovation economy.

Reference 6 - 0.16% Coverage

we will continue to work closely with governments, the private sector, and civil society to foster inclusive economic growth, reduce corruption, and build capacity at the local level. Investment in critical infrastructure and security will facilitate trade among countries, especially for developing and emerging economies.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 6 references coded [ 1.13% Coverage]

Reference 1 - 0.28% Coverage

Criminals, terrorists, and nation-state adversaries are able to exploit the United States’ pervasive dependence on vulnerable technologies to alter, steal, or destroy information; divert or steal money; gain competitive advantages through intellectual property theft; disrupt services; and potentially cripple critical infrastructures.

Reference 2 - 0.25% Coverage

cyber attacks and some kinds of malicious cyber activity2 – particularly those conducted by nation-states or highly capable non-state actors and which target critical infrastructures and key industries in the United States – can constitute a significant threat to U.S. national security and economic interests.

Reference 3 - 0.08% Coverage

deter nation-states and non-state actors seeking to harm the United States through cyber-enabled means

Reference 4 - 0.06% Coverage

none of these methods are solely within the purview of nation-states.

Reference 5 - 0.22% Coverage

Today, the United States possesses dominant military capabilities, but is asymmetrically dependent on cyberspace and faces highly capable state and non-state adversaries that have the capability, expertise, and intent to conduct significant cyber attacks against us.

Reference 6 - 0.24% Coverage

But the United States’ ability to successfully deter state and non-state sponsored cyber threats must also rely at least as much on defensive strategies that raise technological and other barriers as on the credible knowledge that the United States can and will appropriately respond to such threats.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 7 references coded [ 0.60% Coverage]

Reference 1 - 0.05% Coverage

Non-state actors undermine social order through drug and human trafficking networks, which they use to commit violent crimes and kill thousands of American each year.

Reference 2 - 0.23% Coverage

e primary transnational threats Americans face are from jihadist terrorists and transnational criminal organizations. Although their objectives diﬀ er, these actors pose some common challenges. First, they exploit our open society. Second, they often operate in loose confederations and adapt rapidly. Th ird, they rely on encrypted communication and the dark web to evade detection as they plot, recruit, ﬁ nance, and execute their operations. Fourth, they thrive under conditions of state weakness and prey on the vulnerable as they accelerate the breakdown of rules to create havens from which to plan and launch att acks on the United States, our allies, and our partners. Fifth, some are sheltered and supported by states and do their bidding.

Reference 3 - 0.04% Coverage

The United States must devote greater resources to dismantle transnational criminal organizations (TCOs) and their subsidiary networks.

Reference 4 - 0.05% Coverage

ese organizations weaken our allies and partners too, by corrupting and undermining democratic institutions. TCOs are motivated by proﬁ t, power, and political inﬂ uence.

Reference 5 - 0.07% Coverage

some state adversaries use TCOs as instruments of national power, offering them territorial sanctuary where they are free to conduct unattributable cyber intrusions, sabotage, theft, and political subversion.

Reference 6 - 0.12% Coverage

Governments and private sector ﬁ rms have the ability to launch satellites into space at increasingly lower costs. Th e fusion of data from imagery, communications, and geolocation services allows motivated actors to access previously unavailable information. Th is “democratization of space” has an impact on military operations and on America’s ability to prevail in conﬂ ict.

Reference 7 - 0.05% Coverage

State and non-state actors project influence and advance their objectives by exploiting information, democratic media freedoms, and international institutions.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 3 references coded [ 0.79% Coverage]

Reference 1 - 0.18% Coverage

— including   
Non-state actors terrorists and   
criminals — exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states.

Reference 2 - 0.19% Coverage

The United States is regularly the victim of malicious cyber activity perpetrated by criminal actors, including state and non-state actors and their proxies and terrorists using network infrastructure in the United States and abroad.

Reference 3 - 0.41% Coverage

Computer hacking conducted by transnational criminal groups poses a significant threat to our national security. Equipped with sizeable funds, organized criminal groups operating abroad employ sophisticated malicious software, spearphishing campaigns, and other hacking tools — some of which rival those of nation states in sophistication — to hack into sensitive financial systems, conduct massive data breaches, spread ransomware, attack critical infrastructure, and steal intellectual property.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Defense Strategy Summary - § 3 references coded [ 0.90% Coverage]

Reference 1 - 0.33% Coverage

The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed.

Reference 2 - 0.21% Coverage

States are the principal actors on the global stage, but non-state actors also threaten the security environment with increasingly sophisticated capabilities.

Reference 3 - 0.36% Coverage

There is a positive side to this as well, as our partners in sustaining security are also more than just nation-states: multilateral organizations, non-governmental organizations, corporations, and strategic influencers provide opportunities for collaboration and partnership.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 5 references coded [ 0.46% Coverage]

Reference 1 - 0.09% Coverage

We are doing so by working with governments, civil society, independent media, and the private sector to prevent credible information from being crowded out, exposing disinformation campaigns, and strengthening the integrity of the media environment - a bedrock of thriving democracies.

Reference 2 - 0.11% Coverage

The United States will work pragmatically with any partner willing to join us in constructive problem-solving, reinforcing and building new ties based on shared interests. This includes not just nation states, but also civil society groups, private companies, philanthropies, and subnational governments at home and around the world.

Reference 3 - 0.07% Coverage

We are working with like-minded governments, civil society, and the technology sector to address terrorist and violent extremist content online, including through innovative research collaborations.

Reference 4 - 0.11% Coverage

To ensure these investments support positive technological outcomes, we will partner with industry and governments in shaping technological standards that ensure quality, consumer safety, and global interoperability, and to advance the open and transparent standards process that has enabled innovation, growth, and interconnectivity for decades.

Reference 5 - 0.08% Coverage

Advancing America’s national interests will hinge in part on working more closely, not only with African nations, but also with regional bodies, such as the African Union, subnational governments, civil society, and private sector and diaspora communities.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 1 reference coded [ 0.49% Coverage]

Reference 1 - 0.49% Coverage

U.S. interests in cyberspace are also threatened by profit-motivated transnational criminal organizations: ransomware gangs, hacktivists, and state-sponsored cyber mercenaries. Small groups of experienced hackers, harnessing sophisticated TTPs, are capable of achieving cyber effects similar to those caused by professional intelligence and military services.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 5 references coded [ 0.57% Coverage]

Reference 1 - 0.08% Coverage

These tools and services empower countries that previously lacked the ability to harm U.S. interests in cyberspace and enable a growing threat from organized criminal syndicates.

Reference 2 - 0.08% Coverage

The cyber operations of criminal syndicates now represent a threat to the national security, public safety, and economic prosperity of the United States and its allies and partners.

Reference 3 - 0.10% Coverage

Each effort requires unprecedented levels of collaboration across its respective stakeholder communities, including the public sector, private industry, civil society, and international allies and partners.

Reference 4 - 0.11% Coverage

Together, industry and government must drive effective and equitable collaboration to correct market failures, minimize the harms from cyber incidents to society’s most vulnerable, and defend our shared digital ecosystem.

Reference 5 - 0.20% Coverage

DoD’s new strategy will clarify how U.S. Cyber Command and other DoD components will integrate cyberspace operations into their efforts to defend against state and non-state actors capable of posing strategic-level threats to U.S. interests, while continuing to strengthen their integration and coordination of operations with civilian, law enforcement, and intelligence partners to disrupt malicious activity at scale.

**Annotations**

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