Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 3 references coded [ 0.10% Coverage]

Reference 1 - 0.03% Coverage

America must demonstrate through words and deeds the resilience of our values and Constitution

Reference 2 - 0.01% Coverage

Nations must have incentives to behave responsibly,

Reference 3 - 0.06% Coverage

But when our overtures are rebuffed, we must lead the international community in using public and private diplomacy, and drawing on incentives and disincentives, in an effort to change repressive behavior.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 1 reference coded [ 0.03% Coverage]

Reference 1 - 0.03% Coverage

The United States will work with like-minded nations to foster norms regarding behavior in domains where an attack on one nation has consequences for all—especially in space and cyberspace.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 1 reference coded [ 0.04% Coverage]

Reference 1 - 0.04% Coverage

encourage responsible behavior

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 20 references coded [ 0.45% Coverage]

Reference 1 - 0.03% Coverage

widely-recognized illegal behavior

Reference 2 - 0.01% Coverage

norms of behavior,

Reference 3 - 0.02% Coverage

responsible behavior

Reference 4 - 0.01% Coverage

state behavior;

Reference 5 - 0.11% Coverage

Politically, we must help to maintain an environment of respect for technical infrastructure, so disputes do not become excuses to disrupt and degrade networks~

Reference 6 - 0.01% Coverage

behavior,

Reference 7 - 0.03% Coverage

acceptable state behavior in cyberspace~

Reference 8 - 0.03% Coverage

what constitutes acceptable behavior,

Reference 9 - 0.04% Coverage

shared understandings about acceptable behavior

Reference 10 - 0.02% Coverage

guiding state behavior

Reference 11 - 0.01% Coverage

behavior

Reference 12 - 0.02% Coverage

international behavior

Reference 13 - 0.03% Coverage

responsible behavior in cyberspace

Reference 14 - 0.01% Coverage

behavior

Reference 15 - 0.01% Coverage

behavior~

Reference 16 - 0.02% Coverage

encourage responsible behavior

Reference 17 - 0.03% Coverage

behave as responsible stakeholders

Reference 18 - 0.01% Coverage

behavior

Reference 19 - 0.01% Coverage

Criminal behavior

Reference 20 - 0.02% Coverage

escalatory behavior~

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 2 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

desired behaviors

Reference 2 - 0.01% Coverage

Behavior

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 1 reference coded [ 0.04% Coverage]

Reference 1 - 0.04% Coverage

Unprecedented levels of global connectedness provide common incentives for international cooperation and shared norms of behavior

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 3 references coded [ 0.47% Coverage]

Reference 1 - 0.28% Coverage

To support its missions in cyberspace, the Defense Department conducts a range of activities outside of cyberspace to improve collective cybersecurity and protect U.S. interests. For example, the Defense Department cooperates with agencies of the U.S government, with the private sector, and with our international partners to share information, build alliances and partnerships, and foster norms of responsible behavior to improve global strategic stability.

Reference 2 - 0.13% Coverage

As it makes its investments and builds cyber capabilities to defend U.S. national interests, the Defense Department will always be attentive to the potential impact of defense policies on state and non-state actors’ behavior.

Reference 3 - 0.06% Coverage

This behavior can make attribution more difficult and increases the chance of miscalculation.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 8 references coded [ 0.64% Coverage]

Reference 1 - 0.09% Coverage

The international community’s ability to respond effectively to these and other risks is helped or hindered by   
★ 1 ★   
NATIONAL SECURITY STRATEGY   
the behaviors of major powers

Reference 2 - 0.10% Coverage

These partnerships can deliver essential capacity to share the burdens of maintaining global security and prosperity and to uphold the norms that govern responsible international behavior.

Reference 3 - 0.07% Coverage

Collective action is needed to assure access to the shared spaces—cyber, space, air, and oceans—where the dangerous behaviors of some threaten us all.

Reference 4 - 0.14% Coverage

arteries of the global economy and civil society, and access is at risk due to increased competition and provocative behaviors. Therefore, we will continue to promote rules for responsible behavior while making sure we have the capabilities to assure access to these shared spaces.

Reference 5 - 0.04% Coverage

Globally, cybersecurity requires that long-standing norms of international behavior

Reference 6 - 0.03% Coverage

We insist on safe and responsible behaviors in the sky and at sea.

Reference 7 - 0.06% Coverage

On territorial disputes, particularly in Asia, we denounce coercion and assertive behaviors that threaten escalation.

Reference 8 - 0.11% Coverage

We will protect the free movement of information and work to prevent the risky behavior that led to the recent crisis, while addressing resurgent economic forces, from state capitalism to market-distorting free-riding.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 6 references coded [ 0.79% Coverage]

Reference 1 - 0.25% Coverage

Bolstering international engagement to establish norms of state behavior in cyberspace, improve collective network defenses, foster cooperation in countering cybercrime, enhance alliances, and create consensus regarding appropriate responses for cyber attacks against critical infrastructure.

Reference 2 - 0.07% Coverage

lead the way in developing and promulgating norms of state behavior in cyberspace

Reference 3 - 0.03% Coverage

Norms of State Behavior in Cyberspace

Reference 4 - 0.16% Coverage

Endorsement of, and adherence to, specific norms of state behavior in cyberspace could further build mutual confidence that nations are not threatening each other with crippling cyber attacks.

Reference 5 - 0.17% Coverage

Such norms would also socialize standards of behavior in cyberspace consistent with each nation’s security interests and develop the international support necessary for collective action to counter bad actors

Reference 6 - 0.12% Coverage

The United States Government has identified several peacetime norms of state behavior in cyberspace and will seek international support for these norms:

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 4 references coded [ 0.14% Coverage]

Reference 1 - 0.05% Coverage

We will not allow adversaries to use threats of nuclear escalation or other irresponsible nuclear behaviors to coerce the United States, our allies, and our partners.

Reference 2 - 0.03% Coverage

Through our words and deeds, America demonstrates a positive alternative to political and religious despotism.

Reference 3 - 0.02% Coverage

Russia continues to intimidate its neighbors with threatening behavior

Reference 4 - 0.03% Coverage

We seek a Pakistan that is not engaged in destabilizing behavior and a stable and self-reliant Afghanistan.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 7 references coded [ 1.51% Coverage]

Reference 1 - 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 2 - 0.06% Coverage

Enhance Cyber Stability through Norms of Responsible State Behavior

Reference 3 - 0.29% Coverage

The United States will promote a framework of 20   
responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity.

Reference 4 - 0.21% Coverage

International law and voluntary   
non-binding norms of responsible state behavior in cyberspace provide stabilizing, security-enhancing standards that define acceptable behavior to all states and promote greater predictability and stability in cyberspace.

Reference 5 - 0.16% Coverage

Increased public affirmation by the United States and other governments will   
state behavior and thus contribute to greater predictability and stability in cyberspace.   
lead to accepted expectations of

Reference 6 - 0.05% Coverage

Attribute and Deter Unacceptable Behavior in Cyberspace

Reference 7 - 0.20% Coverage

As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners.