Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 4 references coded [ 0.16% Coverage]

Reference 1 - 0.03% Coverage

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

Reference 2 - 0.02% Coverage

Nations must have incentives to behave responsibly, or be isolated when they do not.

Reference 3 - 0.05% Coverage

Credible and effective alternatives to military action—from sanctions to isolation—must be strong enough to change behavior, just as we must reinforce our alliances and our military capabilities.

Reference 4 - 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 - § 18 references coded [ 2.58% Coverage]

Reference 1 - 0.12% Coverage

In reality, good cybersecurity can enhance privacy, and effective law enforcement targeting widely-recognized illegal behavior can protect fundamental freedoms~

Reference 2 - 0.17% Coverage

Risk reduction on a global scale will require effective law enforcement; internationally agreed norms of state behavior; measures that build confidence and enhance transparency; active, informed diplomacy; and appropriate deterrence~

Reference 3 - 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 4 - 0.14% Coverage

The United States will work with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships~

Reference 5 - 0.08% Coverage

These events have not been matched by clearly agreed-upon norms for acceptable state behavior in cyberspace~

Reference 6 - 0.15% Coverage

To bridge that gap, we will work to build a consensus on what constitutes acceptable behavior, and a partnership among those who view the functioning of these systems as essential to the national and collective interest~

Reference 7 - 0.15% Coverage

In other spheres of international relations, shared understandings about acceptable behavior have enhanced stability and provided a basis for international action when corrective measures are required~

Reference 8 - 0.08% Coverage

Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace~

Reference 9 - 0.19% Coverage

We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace~

Reference 10 - 0.15% Coverage

While cyberspace is a dynamic environment, international behavior in it must be grounded in the principles of responsible domestic governance, peaceful interstate conduct, and reliable network management~

Reference 11 - 0.19% Coverage

We will engage the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace and the actions necessary, both domestically and as an international community, to build a system of cyberspace stability~

Reference 12 - 0.10% Coverage

Building broad international understanding about cyberspace norms of behavior must begin with clear agreement among like-minded countries~

Reference 13 - 0.15% Coverage

Regional organizations have been particularly effective at tackling cybersecurity problems specific to their members~ They will play an increasingly important role in developing and applying norms of behavior~

Reference 14 - 0.20% Coverage

The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate~

Reference 15 - 0.15% Coverage

Our Nation can and will play an active role in providing the knowledge and capacity to build and secure new and existing digital systems, and in so doing, build consensus among states to behave as responsible stakeholders~

Reference 16 - 0.13% Coverage

Promote cyberspace cooperation, particularly on norms of behavior for states and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships.

Reference 17 - 0.11% Coverage

Criminal behavior in cyberspace should be met with effective law enforcement, not policies that restrict legitimate access to or content on the Internet~

Reference 18 - 0.20% Coverage

By developing a shared understanding of standard operating procedures, our armed forces can enhance security through coordination and greater information exchange; these engagements will diminish misperceptions about military activities and the potential for 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 DoD Cyber Strategy Summary - § 3 references coded [ 1.75% Coverage]

Reference 1 - 0.48% Coverage

Reinforce norms of responsible State behavior in cyberspace: The Department will reinforce voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime.

Reference 2 - 0.69% Coverage

The United States has endorsed the work done by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) to develop a framework of responsible State behavior in cyberspace.

Reference 3 - 0.59% Coverage

The Department will work alongside its interagency and international partners to promote international commitments regarding behavior in cyberspace as well as to develop and implement cyber confidence building measures (CBM).

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.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 4 references coded [ 0.26% Coverage]

Reference 1 - 0.03% Coverage

Meanwhile, Russia’s unprovoked, unjust, and reckless invasion of Ukraine underscores its irresponsible behavior.

Reference 2 - 0.06% Coverage

In the cyber and space domains, the risk of inadvertent escalation is particularly high due to unclear norms of behavior and escalation thresholds, complex domain interactions, and new capabilities.

Reference 3 - 0.07% Coverage

Our competitors, particularly the PRC, are pursuing holistic strategies that employ varied forms of coercion, malign behavior, and aggression to achieve their objectives and weaken the foundations of a stable and open international system.

Reference 4 - 0.10% Coverage

U.S. leadership in shaping norms for appropriate conduct in the cyber, space, and other emerging technology domains will reinforce deterrence by increasing international consensus on what constitutes malign and aggressive behavior, thereby increasing the prospect of collective attribution and response when these norms are violated.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 6 references coded [ 0.34% Coverage]

Reference 1 - 0.07% Coverage

The most pressing strategic challenge facing our vision is from powers that layer authoritarian governance with a revisionist foreign policy. It is their behavior that poses a challenge to international peace and stability

Reference 2 - 0.03% Coverage

Many non-democracies join the world’s democracies in forswearing these behaviors.

Reference 3 - 0.04% Coverage

The PRC’s assertive behavior has caused other countries to push back and defend their sovereignty, for their own, legitimate reasons.

Reference 4 - 0.06% Coverage

As a result, the United States and our allies and partners have an opportunity to shape the PRC and Russia’s external environment in a way that influences their behavior even as we compete with them.

Reference 5 - 0.07% Coverage

More capable competitors and new strategies of threatening behavior below and above the traditional threshold of conflict mean we cannot afford to rely solely on conventional forces and nuclear deterrence.

Reference 6 - 0.07% Coverage

We will continue to promote adherence to the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, which recognizes that international law applies online, just as it does offline.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 4 references coded [ 0.54% Coverage]

Reference 1 - 0.19% Coverage

We will reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms.

Reference 2 - 0.07% Coverage

Reinforce Norms of Responsible Behavior in Cyberspace

Reference 3 - 0.10% Coverage

The Department will reinforce norms of responsible behavior in cyberspace.

Reference 4 - 0.18% Coverage

We will bolster the cyber capability and capacity of our Allies and partners and reinforce norms of responsible behavior in cyberspace.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 7 references coded [ 0.88% Coverage]

Reference 1 - 0.08% Coverage

The United States seeks a world where responsible state behavior in cyberspace is expected and rewarded and where irresponsible behavior is isolating and costly.

Reference 2 - 0.06% Coverage

For decades, we have worked through international institutions to define and advance responsible state behavior in cyberspace.

Reference 3 - 0.08% Coverage

We will do so by demonstrating to economies and societies the value of openness and jointly imposing consequences for behavior that runs counter to agreed norms of state behavior.

Reference 4 - 0.22% Coverage

We will expand coalitions, collaboratively disrupt transnational criminals and other malicious cyber actors, build the capacity of our international allies and partners, reinforce the applicability of existing international law to state behavior in cyberspace, uphold globally accepted and voluntary norms of responsible state behavior in peacetime, and punish those that engage in disruptive, destructive, or destabilizing malicious cyber activity.

Reference 5 - 0.21% Coverage

We must enable our allies and partners to secure critical infrastructure networks, build effective incident detection and response capabilities, share cyber threat information, pursue diplomatic collaboration, build law enforcement capacity and effectiveness through operational collaboration, and support our shared interests in cyberspace by adhering to international law and reinforcing norms of responsible state behavior.

Reference 6 - 0.10% Coverage

Close cooperation with an affected ally or partner demonstrates solidarity in the face of adversary activity and can accelerate efforts to expose counternormative state behavior and impose consequences.

Reference 7 - 0.14% Coverage

Every member of the United Nations has made a political commitment to endorse peacetime norms of responsible state behavior in cyberspace that includes refraining from cyber operations that would intentionally damage critical infrastructure contrary to their obligations under international law.