Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 6 references coded [ 0.10% Coverage]

Reference 1 - 0.01% Coverage

norms.

Reference 2 - 0.01% Coverage

acceptable legal norms

Reference 3 - 0.02% Coverage

International norms are critical to establishing a secure and thriving digital infrastructure

Reference 4 - 0.01% Coverage

International norms

Reference 5 - 0.01% Coverage

acceptable norms

Reference 6 - 0.06% Coverage

Norms of Behavior: Addresses those elements of law, regulation, and international treaties and undertakings, as well as consensus-based measures, such as best practices, that collectively circumscribe and define standards of conduct in cyberspace.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 20 references coded [ 0.58% Coverage]

Reference 1 - 0.03% Coverage

shortage of political will that has at times stymied the enforcement of international norms

Reference 2 - 0.01% Coverage

strengthening of international norms

Reference 3 - 0.03% Coverage

we are working to strengthen international norms on behalf of human rights, while welcoming all peaceful democratic movements.

Reference 4 - 0.02% Coverage

a handful of states endanger regional and global security by flouting international norms

Reference 5 - 0.04% Coverage

They share common values and a common commitment to international norms that recognize both the rights and responsibilities of all sovereign nations.

Reference 6 - 0.06% Coverage

To adversarial governments, we offer a clear choice: abide by international norms, and achieve the political and economic benefits that come with greater integration with the international community;

Reference 7 - 0.02% Coverage

sustainable because it is based on broadly shared norms

Reference 8 - 0.01% Coverage

enforcing international norms

Reference 9 - 0.04% Coverage

When nations breach agreed international norms, the countries who espouse those norms must be convinced to band together to enforce them

Reference 10 - 0.01% Coverage

states that flout international norms

Reference 11 - 0.05% Coverage

We are strengthening international norms to isolate governments that flout them and to marshal cooperation against nongovernmental actors who endanger our common security.

Reference 12 - 0.06% Coverage

We will draw on diplomacy, development, and international norms and institutions to help resolve disagreements, prevent conflict, and maintain peace, mitigating where possible the need for the use of force.

Reference 13 - 0.02% Coverage

bring them into compliance with international nonproliferation norms.

Reference 14 - 0.01% Coverage

reinforcing norms of safe and responsible conduct;

Reference 15 - 0.04% Coverage

We will also strengthen our international partnerships on a range of issues, including the development of norms for acceptable conduct in cyberspace;

Reference 16 - 0.02% Coverage

Strengthening International Norms Against Corruption

Reference 17 - 0.06% Coverage

those nations that defy international norms or fail to meet their sovereign responsibilities will be denied the incentives that come with greater integration and collaboration with the international community

Reference 18 - 0.03% Coverage

The United States has an interest in a strong, peaceful, and prosperous Russia that respects international norms.

Reference 19 - 0.01% Coverage

strengthening of international norms and standards.

Reference 20 - 0.02% Coverage

We will push for the recognition of norms of behavior in cyberspace

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 2 references coded [ 0.40% Coverage]

Reference 1 - 0.15% Coverage

establishment of international cyberspace norms will also serve to strengthen cyberspace for the benefit of all.

Reference 2 - 0.25% Coverage

DoD will assist U.S. efforts to advance the development and promotion of international cyberspace norms and principles that promote openness, interoperability, security, and reliability.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 2 references coded [ 0.23% Coverage]

Reference 1 - 0.07% Coverage

The cyber threat is expanded and   
3   
exacerbated by lack of international norms

Reference 2 - 0.16% Coverage

We will support whole-of-nation approaches to establishing and promoting norms, enhancing space situational awareness, and fostering greater transparency and information sharing.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 22 references coded [ 1.33% Coverage]

Reference 1 - 0.02% Coverage

Stability Through Norms

Reference 2 - 0.01% Coverage

norms of behavior,

Reference 3 - 0.02% Coverage

norms of responsible behavior

Reference 4 - 0.03% Coverage

internationally agreed norms of state behavior;

Reference 5 - 0.01% Coverage

norms of behavior,

Reference 6 - 0.01% Coverage

norms

Reference 7 - 0.01% Coverage

The Role of Norms~

Reference 8 - 0.05% Coverage

Adherence to such norms brings predictability to state conduct,

Reference 9 - 0.13% Coverage

The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete~

Reference 10 - 0.08% Coverage

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

Reference 11 - 0.01% Coverage

how these norms apply

Reference 12 - 0.08% Coverage

We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace,

Reference 13 - 0.01% Coverage

The Basis for Norms

Reference 14 - 0.02% Coverage

cyberspace norms include

Reference 15 - 0.62% Coverage

Emerging norms, also essential to this space, include: • Global Interoperability: States should act within their authorities to help ensure the end-toend interoperability of an Internet accessible to all~   
• Network Stability: States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure~   
• Reliable Access: States should not arbitrarily deprive or disrupt individuals’ access to the Internet or other networked technologies~   
• Multi-stakeholder Governance: Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders~   
• Cybersecurity Due Diligence: States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse~

Reference 16 - 0.02% Coverage

promulgate positive norms

Reference 17 - 0.05% Coverage

Building broad international understanding about cyberspace norms

Reference 18 - 0.02% Coverage

applying norms of behavior~

Reference 19 - 0.03% Coverage

norms of behavior for states and cybersecurity,

Reference 20 - 0.03% Coverage

key cyberspace activities, including norms

Reference 21 - 0.01% Coverage

international norms

Reference 22 - 0.04% Coverage

international norms of acceptable network management

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 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\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review CLEAN - § 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\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 2 references coded [ 0.30% Coverage]

Reference 1 - 0.26% Coverage

Iran also poses strategic challenges to the international community. It is pursuing   
nuclear and missile delivery technologies despite repeated United Nations Security Council resolutions demanding that it cease such efforts.

Reference 2 - 0.04% Coverage

our commitment to international norms

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 15 references coded [ 1.45% Coverage]

Reference 1 - 0.07% Coverage

It also means holding ourselves to international norms and standards that we expect other nations to uphold, and admitting when we do not

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 - 0.12% Coverage

Russia’s violation of Ukraine’s sovereignty and territorial integrity—as well as its belligerent stance toward other neighboring countries—endangers international norms that have largely been taken for granted since the end of the Cold War

Reference 4 - 0.05% Coverage

imposing costs on those who threaten their neighbors or violate fundamental international norms

Reference 5 - 0.18% Coverage

Globally, cybersecurity requires that long-standing norms of international behavior—to include protection of intellectual property, online freedom, and respect for civilian infrastructure—be upheld, and the Internet be managed as a shared responsibility between states and the private sector with civil society and Internet users as key stakeholders.

Reference 6 - 0.05% Coverage

We will continue mobilizing international support to strengthen and expand global norms of human rights

Reference 7 - 0.13% Coverage

We have an opportunity—and obligation—to lead the way in reinforcing, shaping, and where appropriate, creating the rules, norms, and institutions that are the foundation for peace, security, prosperity, and the protection of human rights in the 21st century.

Reference 8 - 0.13% Coverage

Targeted economic sanctions remain an effective tool for imposing costs on those irresponsible actors whose military aggression, illicit proliferation, or unprovoked violence threaten both international rules and norms and the peace they were designed to preserve.

Reference 9 - 0.10% Coverage

In many cases, our use of targeted sanctions and other coercive measures are meant not only to uphold international norms, but to deter severe threats to stability and order at the regional level.

Reference 10 - 0.13% Coverage

We are committed to strengthening regional institutions such as ASEAN, the East Asia Summit, and Asia-Pacific Economic Cooperation to reinforce shared rules and norms, forge collective responses to shared challenges, and help ensure peaceful resolution of disputes

Reference 11 - 0.11% Coverage

We are also working with our Asian partners to promote more open and transparent economies and regional support for international economic norms that are vital to maintaining it as an engine for global economic growth

Reference 12 - 0.06% Coverage

insisting that China uphold international rules and norms on issues ranging from maritime security to trade and human rights.

Reference 13 - 0.08% Coverage

A strong Europe is our indispensable partner, including for tackling global security challenges, promoting prosperity, and upholding international norms.

Reference 14 - 0.08% Coverage

Russia’s aggression in Ukraine makes clear that European security and the international rules and norms against territorial aggression cannot be taken for granted.

Reference 15 - 0.06% Coverage

We will uphold and refresh the international rules and norms that set the parameters for such collaboration and competition.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 7 references coded [ 1.81% 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 - 0.27% Coverage

Effective international collaboration on cyber deterrence will require the United States to share its perspective on the threat environment with allies and international partners, lead the way in developing and promulgating norms of state behavior in cyberspace, and support international partners’ efforts to secure their own networks.

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 - 0.11% Coverage

By acting together to develop and enforce such norms, the United States and   
16   
its international partners can isolate potential adversaries.

Reference 7 - 0.82% Coverage

 A State should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public.   
 A State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents. A State should also not use CSIRTs to enable online activity that is intended to do harm.   
 A State should cooperate, in a manner consistent with its domestic law and international obligations, with requests for assistance from other states in investigating cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.   
 A State should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.