Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 10 references coded [ 0.14% Coverage]

Reference 1 - 0.01% Coverage

prevent

Reference 2 - 0.02% Coverage

help the Federal government prevent as well as detect malicious behavior.

Reference 3 - 0.02% Coverage

pilot deployments of intrusion detection and prevention systems for the benefit of federal networks

Reference 4 - 0.01% Coverage

prevention

Reference 5 - 0.03% Coverage

The U.S. Government should invest in processes, technologies, and infrastructure that will help prevent cyber incidents

Reference 6 - 0.01% Coverage

preventing,

Reference 7 - 0.02% Coverage

Information is key to preventing, detecting, and responding to cyber incidents

Reference 8 - 0.01% Coverage

prevention,

Reference 9 - 0.03% Coverage

Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.

Reference 10 - 0.01% Coverage

prevent,

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 5 references coded [ 0.14% Coverage]

Reference 1 - 0.02% Coverage

prevent the proliferation of the world’s most dangerous weapons

Reference 2 - 0.05% Coverage

Defense: We are strengthening our military to ensure that it can prevail in today’s wars; to prevent and deter threats against the United States, its interests, and our allies and partners;

Reference 3 - 0.04% Coverage

As we do everything within our power to prevent these dangers, we also recognize that we will not be able to deter or prevent every single threat.

Reference 4 - 0.02% Coverage

Security at home relies on our shared efforts to prevent

Reference 5 - 0.01% Coverage

place renewed emphasis on deterrence and prevention

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 3 references coded [ 0.19% Coverage]

Reference 1 - 0.09% Coverage

defeat al Qaida and its affiliates in Afghanistan and Pakistan and prevent their return to either country

Reference 2 - 0.06% Coverage

Preventing wars is as important as winning them, and far less costly

Reference 3 - 0.04% Coverage

preventing Iran from acquiring nuclear arms.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 2 references coded [ 0.08% Coverage]

Reference 1 - 0.05% Coverage

focusing on preventing crime and catching and punishing offenders

Reference 2 - 0.04% Coverage

Preventing terrorists from enhancing capabilities

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 4 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

Prevent Proliferation

Reference 2 - 0.01% Coverage

prevent harmful arms races.

Reference 3 - 0.01% Coverage

prevent

Reference 4 - 0.01% Coverage

prevent-and-deter

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 3 references coded [ 0.19% Coverage]

Reference 1 - 0.07% Coverage

The prevention of catastrophic attack against U.S. territory.

Reference 2 - 0.07% Coverage

the   
prevention of catastrophic attack against U.S. territory

Reference 3 - 0.05% Coverage

Should deterrence fail to prevent aggression,

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 4 references coded [ 0.17% Coverage]

Reference 1 - 0.05% Coverage

we will focus on building the capacity of others to prevent the causes and consequences of conflict

Reference 2 - 0.03% Coverage

We are more responsive and resilient when prevention fails

Reference 3 - 0.06% Coverage

increased efforts to prevent the growth of violent extremism and radicalization that drives increased threats

Reference 4 - 0.04% Coverage

prevent the development, proliferation, or use of weapons of mass destruction.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 4 references coded [ 0.78% Coverage]

Reference 1 - 0.20% Coverage

Pursuing defense, resiliency, and reconstitution initiatives to provide critical networks with a greater capability to prevent or minimize the impact of cyber attacks or other malicious cyber activity, and reconstitute rapidly if attacks succeed.

Reference 2 - 0.28% Coverage

DHS and other elements of the United States Government have developed infrastructure and processes for disseminating specific and targeted cybersecurity threat information to the identified critical infrastructure owners and operators. This information is used to detect and prevent intrusion attempts from a range of cyber adversaries.

Reference 3 - 0.12% Coverage

These efforts are improving the private sector’s ability to detect and prevent intrusion attempts, as well as recover from a range of cyber incidents.

Reference 4 - 0.18% Coverage

The Federal government continues to improve the security of its information and systems through broad implementation of cybersecurity capabilities and services designed to detect and prevent malicious cyber activities