Files\\2011 Case Study\\CS1\_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\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 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\\2011 Case Study\\CS1\_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\\CS1\_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\\CS1\_Secondary Sources\_Authoritative\\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\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 1 reference coded [ 0.07% Coverage]

Reference 1 - 0.07% Coverage

The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 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\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 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\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 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

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 21 references coded [ 1.15% Coverage]

Reference 1 - 0.06% Coverage

An America that successfully competes is the best way to prevent conﬂ ict. Just as American weakness invites challenge, American strength and confidence deters war and promotes peace.

Reference 2 - 0.06% Coverage

We must prevent nuclear, chemical, radiological, and biological att acks, block terrorists from reaching our homeland, reduce drug and human trafficking, and protect our critical infrastructure.

Reference 3 - 0.03% Coverage

Building on decades of init iat ives, we wi l l augment mea sures to secure , el iminate, and prevent the spread of WMD

Reference 4 - 0.03% Coverage

We will work with other countries to detect and mitigate outbreaks early to prevent the spread of disease.

Reference 5 - 0.06% Coverage

ENHANCE VETTING: The U.S. Government will enhance vetting of prospective immigrants, refugees, and other foreign visitors to identify individuals who might pose a risk to national security or public safety.

Reference 6 - 0.05% Coverage

Time and territory allow jihadist terrorists to plot, so we will act against sanctuaries and prevent their reemergence, before they can threaten the U.S. homeland.

Reference 7 - 0.07% Coverage

U.S. intelligence and homeland security experts will work with law enforcement and civic leaders on terrorism prevention and provide accurate and actionable information about radicalization in their communities.

Reference 8 - 0.05% Coverage

As it evolves, the government and private sector must design systems that incorporate prevention, protection, and resiliency from the start, not as an afterthought.

Reference 9 - 0.07% Coverage

The Federal Government will ensure that those charged with securing critical infrastructure have the necessary authorities, information, and capabilities to prevent attacks before they affect or hold at risk U.S. critical infrastructure.

Reference 10 - 0.03% Coverage

Despite our best efforts, our government cannot prevent all dangers to the American people.

Reference 11 - 0.07% Coverage

Th e United States wi l l prioritize counterintelligence and law enforcement activities to curtail intellectual property theft by all sources and will explore new legal and regulatory mechanisms to prevent and prosecute violations.

Reference 12 - 0.04% Coverage

The threat from jihadist terrorists will persist, even as we intensify efforts to prevent attacks on Americans, our allies, and our partners.

Reference 13 - 0.06% Coverage

The United States must retain overmatch— the combination of capabilities in sufficient scale to prevent enemy success and to ensure that America’s sons and daughters will never be in a fair fight.

Reference 14 - 0.06% Coverage

While nuclear deterrence strategies cannot prevent all conflict, they are essen-   
30   
tial to prevent nuclear att ack, non-nuclear strategic attacks, and large-scale conventional aggression

Reference 15 - 0.04% Coverage

Fear of escalation will not prevent the United States from defending our vital interests and those of our allies and partners.

Reference 16 - 0.07% Coverage

Intelligence is needed to understand and anticipate foreign doctrine and the intent of foreign leaders, prevent tactical and operational surprise, and ensure that U.S. capabilities are not compromised before they are fielded.

Reference 17 - 0.09% Coverage

To prevent the theft of sensitive and proprietary information and maintain supply chain integrity , the United States must increase our understanding of the economic policy priorities of our adversaries and improve our ability to detect and defeat their attempts to commit economic espionage.

Reference 18 - 0.03% Coverage

Within this framework, the United States will also assist fragile states to prevent threats to the U.S. homeland.

Reference 19 - 0.03% Coverage

For ins t ance, engagement in Afghanistan seeks to prevent the reemergence of terrorist safe havens.

Reference 20 - 0.05% Coverage

The United States must marshal the will and capabilities to compete and prevent unfavorable shifts in the Indo-Pacific, Europe, and the Middle East.

Reference 21 - 0.10% Coverage

U.S. interests in the region include countering terrorist threats that impact the security of the U.S. homeland and our allies, preventing cross-border terrorism that raises the prospect of military and nuclear tensions, and preventing nuclear weapons, technology, and materials from falling into the hands of terrorists.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 11 references coded [ 2.62% Coverage]

Reference 1 - 0.24% Coverage

The Administration also   
recognizes that a purely technocratic approach to cyberspace is insufficient to address the nature of the new problems we confront.   
The   
United States must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation.

Reference 2 - 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 3 - 0.29% Coverage

and communications   
technology (ICT) underlies every sector in America.   
ICT providers are in a unique position   
to detect, prevent, and mitigate risk before it impacts their customers, and the Federal Government must work with these providers to improve ICT security and resilience in a targeted and efficient manner while protecting privacy and civil liberties.

Reference 4 - 0.23% Coverage

Federal law enforcement works to apprehend and prosecute offenders, disable criminal infrastructure, limit the spread and use of nefarious cyber capabilities, prevent cyber criminals and their state sponsors from profiting from their illicit activity, and seize their assets.

Reference 5 - 0.24% Coverage

To effectively deter, disrupt, and prevent cyber threats, law enforcement will work with private industry to confront challenges presented by technological barriers, such as anonymization and encryption technologies, to obtain time-sensitive evidence pursuant to appropriate legal process.

Reference 6 - 0.23% Coverage

The prompt reporting of cyber incidents to the Federal Government is essential to an effective response, linking of   
P I L L A R I: P R O T E C T T H E A M E R I C A N P E O P L E , T H E H O M E L A N D , A N D T H E A M E R I C A N WAY OF L I F E   
related incidents, identification of the perpetrators, and prevention of future incidents

Reference 7 - 0.21% Coverage

The United States Government will promote implementation and   
P I L L A R I I : PROM O T E A M E R I C A N PRO S P E R I T Y   
continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem.

Reference 8 - 0.11% Coverage

we will work to prevent adversarial nation states from gaining unfair advantage at the expense of American research and development

Reference 9 - 0.11% Coverage

All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States.

Reference 10 - 0.21% Coverage

This includes working with foreign government partners as well as the private sector, academia, and civil society to identify, counter, and prevent the use of digital platforms for malign foreign influence operations while respecting civil rights and liberties.

Reference 11 - 0.20% Coverage

We will also work to prevent authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an authoritarian web under their control, under the guise of security or countering terrorism.