Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 3 references coded [ 0.13% Coverage]

Reference 1 - 0.03% Coverage

drew a swift and forceful response from the United States and our allies and partners in Afghanistan

Reference 2 - 0.01% Coverage

response to cyber attacks

Reference 3 - 0.10% Coverage

Our strategy to attack these networks must respond in kind and target their illicit resources and access to the global financial system through financial measures, administration and enforcement of regulatory authorities, outreach to the private sector and our foreign partners, and collaboration on international standards and information sharing.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

supporting a response to an attack

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 3 references coded [ 0.50% Coverage]

Reference 1 - 0.11% Coverage

We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options~

Reference 2 - 0.09% Coverage

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country~

Reference 3 - 0.31% Coverage

As we continue to build and enhance our own response capabilities, we will work with other countries to expand the international networks that support greater global situational awareness and incident response—including between government and industry~ The United States Government actively participates in watch, warning, and incident response through exchanging information with trusted networks of international partners~

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 2 references coded [ 0.19% Coverage]

Reference 1 - 0.17% Coverage

We will, on order, be prepared to respond to any attack across the full spectrum of military capabilities with an appropriate and measured response at a time and place of our Nation’s choosing.

Reference 2 - 0.02% Coverage

threat of retaliation

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 3 references coded [ 0.12% Coverage]

Reference 1 - 0.02% Coverage

prevent, and respond to significant cybersecurity incidents

Reference 2 - 0.07% Coverage

The strategy also must include prevention, mitigation, and response against threats to or subversion of the people who operate and benefit from the infrastructure, the processes that run or take advantage of the infrastructure, and the supply chains used to build and maintain the infrastructure

Reference 3 - 0.03% Coverage

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

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 3 references coded [ 0.09% Coverage]

Reference 1 - 0.03% Coverage

a smaller force strains our ability to simultaneously respond to more than one major contingency at a time.

Reference 2 - 0.04% Coverage

We will continue to maintain a strong military posture in the Gulf region – one that can respond swiftly to crisis, deter aggression,

Reference 3 - 0.02% Coverage

rebalance investments toward systems that are operationally responsive

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 11 references coded [ 1.81% Coverage]

Reference 1 - 0.04% Coverage

This includes incident management and network defense response.

Reference 2 - 0.11% Coverage

If and when DoD detects indications of hostile activity within its networks, DoD has quick-response capabilities to close or mitigate vulnerabilities and secure its networks and systems.

Reference 3 - 0.09% Coverage

Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages

Reference 4 - 0.26% Coverage

As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.

Reference 5 - 0.21% Coverage

The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States’ defenses.

Reference 6 - 0.37% Coverage

Response: The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. The United States has articulated this declaratory policy in the 2011 United States International Strategy for Cyberspace, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense. The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.

Reference 7 - 0.08% Coverage

Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.

Reference 8 - 0.20% Coverage

Finally, cyber capabilities present state and non-state actors with the ability to strike at U.S. interests in a manner that may or may not necessarily warrant a purely military response by the United States, but which may nonetheless present a significant threat to U.S. national security and may warrant a non-military response of some kind.

Reference 9 - 0.10% Coverage

In response to certain attacks and intrusions, the United States may undertake diplomatic actions, take law enforcement actions, and consider economic sanctions.

Reference 10 - 0.11% Coverage

Through the course of this strategy DoD will constantly assess the international environment and develop innovative partnerships to respond to emerging challenges and opportunities.

Reference 11 - 0.24% Coverage

Build partnerships to defend the nation. DoD will have a framework in place to cooperate with other government agencies to conduct defend the nation operations. DoD will work with FBI, CIA, DHS and other agencies to build relationships and integrate capabilities to provide the President with the widest range of options available to respond to a cyberattack of significant consequence to the United States.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 7 references coded [ 0.74% Coverage]

Reference 1 - 0.01% Coverage

respond.

Reference 2 - 0.13% Coverage

Forward deployed, rotational, and globally responsive forces regularly demonstrate the capability and will to act.

Reference 3 - 0.21% Coverage

In the event of an attack, the U.S. military will respond by inflicting damage of such magnitude as to compel the adversary to cease hostilities or render it incapable of further aggression.

Reference 4 - 0.16% Coverage

U.S. strategic forces are kept at the   
highest state of readiness, always prepared to respond to threats to the homeland and our vital interests.

Reference 5 - 0.09% Coverage

positions the Joint Force to execute emergency actions in response to a crisis.

Reference 6 - 0.07% Coverage

Respond to crisis and conduct limited contingency operations

Reference 7 - 0.07% Coverage

Respond to Crisis and Conduct Limited Contingency Operations.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 33 references coded [ 5.15% Coverage]

Reference 1 - 0.07% Coverage

Bolstering “Whole-of-Government” and “Whole of Nation” Response Capabilities

Reference 2 - 0.09% Coverage

United States Government’s ability and willingness to respond to cyber attacks through all necessary means

Reference 3 - 0.24% Coverage

But the United States’ ability to successfully deter state and non-state sponsored cyber threats must also rely at least as much on defensive strategies that raise technological and other barriers as on the credible knowledge that the United States can and will appropriately respond to such threats.

Reference 4 - 0.23% Coverage

In particular, there should be certainty about the fact that, even in the face of sophisticated cyber threats, the United States can maintain robust defenses, ensure resilient networks and systems, and implement a robust response capability that can project power and secure U.S. interests.

Reference 5 - 0.03% Coverage

identify and respond to incidents,

Reference 6 - 0.11% Coverage

Just because an attack takes place in cyberspace does not mean that a lawful and appropriate response must be conducted through cyber means.

Reference 7 - 0.06% Coverage

Nor is a direct response always the most appropriate and proportional response.

Reference 8 - 0.23% Coverage

Instead, the United States must maintain a spectrum of response capabilities that provide the President and senior U.S. leaders with options that can be tailored to   
10   
particular adversaries, the impact of the malicious activities, and the level of certainty regarding attribution.

Reference 9 - 0.08% Coverage

In particular, financial sanctions can offer an effective tool for responding to cyber attacks.

Reference 10 - 0.44% Coverage

In response to North Korea’s destructive and coercive cyber attack in November 2014 – which was intended to harm a U.S. business and suppress free speech – the Administration announced new sanctions on certain North Korean actors. Further, in April 2015 the President issued a new Executive Order authorizing the imposition of sanctions on individuals and entities whose cyberenabled activities have contributed to a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

Reference 11 - 0.15% Coverage

The United States Government has used these tools for many years to address other policy challenges and will continue apply them, as appropriate, to deter and respond to cyber threats as well.

Reference 12 - 0.16% Coverage

Since there is an individual or organization behind every intrusion, U.S. law enforcement agencies are a critical element of the United States Government’s cyber incident response mechanism.

Reference 13 - 0.03% Coverage

respond to a cyber attack on the nation.

Reference 14 - 0.04% Coverage

could rapidly react to a cyber attack on the nation.

Reference 15 - 0.13% Coverage

Even though the United States Government is not limited to responding to a cyber attack through cyberspace, there are unique advantages to such a symmetrical response.

Reference 16 - 0.10% Coverage

Bringing a “whole-of-government” and “whole-of-nation” approach to cyber incident response and national-level events.

Reference 17 - 0.29% Coverage

Promoting a nuanced and graduated declaratory policy and strategic communications that highlight the United States Government commitment to using its capabilities to defend against cyber attacks, but remains ambiguous on thresholds for response and consequences to discourage preemption or malicious cyber activities just below the threshold for response.

Reference 18 - 0.06% Coverage

appropriate responses for cyber attacks against critical infrastructure.

Reference 19 - 0.07% Coverage

Bolstering “Whole-of-Government” and “Whole of Nation” Response Capabilities

Reference 20 - 0.09% Coverage

The Department of State uses its relationships with foreign governments to coordinate policy responses.

Reference 21 - 0.20% Coverage

DHS has an intimate knowledge of U.S. critical infrastructure, significant expertise in incident response and mitigation, and the deep relationships with the private sector necessary to protect critical infrastructure and respond to cyber attacks.

Reference 22 - 0.17% Coverage

In addition, the Administration has put in place mechanisms that ensure departments and agencies are combining their capabilities and resources into effective, coordinated responses to malicious cyber activity.

Reference 23 - 0.18% Coverage

As one example, in 2014, the White House began using the Cyber Response Group, or CRG—modeled on the highly effective and long-standing Counterterrorism Security Group—to handle certain incident response coordination tasks.

Reference 24 - 0.13% Coverage

The CRG focuses on sharing threat information, malware signatures, plans of state and non-state actors, and coordinating responses across the government.

Reference 25 - 0.39% Coverage

Malicious actors are increasingly willing to intrude into public and private networks for the purpose of destructive cyber attacks, and the   
14   
Administration views forums for agile interagency coordination, like the CRG as a linchpin in the government’s response capabilities. In standing up the CRG and similar mechanisms, the Administration seeks to share knowledge about ongoing threats and attacks and coordinate all elements of the government’s response at the highest levels.

Reference 26 - 0.18% Coverage

All of these efforts are aimed at improving the government’s ability to understand the nature of a given cyber incident and to make rapid decisions about whether and how to respond to cyber incidents of significant national concern.

Reference 27 - 0.12% Coverage

The United States has issued clear statements in the past regarding the U.S. intention to respond as necessary and appropriate to cyber threats.

Reference 28 - 0.20% Coverage

However, the United States Government will remain ambiguous in its statements on thresholds for response and consequences of cyber threats in order to discourage preemption or malicious cyber activities just below the threshold for response.

Reference 29 - 0.22% Coverage

The Administration will consider whether to speak more openly about whether and how the United States might respond to malicious cyber activities, although such public discussion will require carefully balancing such transparency against intelligence and military equities.

Reference 30 - 0.20% Coverage

The United States Government may also send messages through diplomatic or other channels to foreign adversaries as a warning that the United States can attribute and will respond to malicious cyber activities as necessary to protect our interests.

Reference 31 - 0.25% Coverage

The United States Government is also working with its counterparts around the world to enhance deterrence by expanding bilateral and multilateral defense and security relationships to include greater cooperation in the areas of network defense, information sharing, incident response, and resiliency.

Reference 32 - 0.21% Coverage

Such dialogues reinforce other policy efforts that support cyber deterrence by creating an environment where parties can explore new avenues of cooperation and build transparency measures to reduce the risk of miscalculation in response to a cyber incident.

Reference 33 - 0.02% Coverage

respond to cyber incidents

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 5 references coded [ 0.32% Coverage]

Reference 1 - 0.04% Coverage

We must also take steps to respond quickly to meet the needs of the American people in the event of natural disaster or attack on our homeland.

Reference 2 - 0.06% Coverage

The ability of the military to surge in response to an emergency depends on our Nation’s ability to produce needed parts and systems, healthy and secure supply chains, and a skilled U.S. workforce.

Reference 3 - 0.07% Coverage

Any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. inter-   
31   
est will be met with a deliberate response at a time, place, manner, and domain of our choosing

Reference 4 - 0.05% Coverage

IMPROVE ATTRIBUTION , ACCOUNTABIL ITY, AND RESPONSE: We will invest in capabilities to support and improve our ability to attribute cyberattacks, to al low for rapid response.

Reference 5 - 0.10% Coverage

China presents its ambitions as mutually beneficial, but Chinese dominance risks diminishing the sovereignty of many states in the IndoPacific. States throughout the region are calling for sustained U.S. leadership in a collective response that upholds a regional order respectful of sovereignty and independence.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 DoD Cyber Strategy Summary - § 1 reference coded [ 0.78% Coverage]

Reference 1 - 0.78% Coverage

The Department must respond to these activities by exposing, disrupting, and degrading cyber activity threatening U.S. interests, strengthening the cybersecurity and resilience of key potential targets, and working closely with other departments and agencies, as well as with our allies and partners.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 11 references coded [ 2.26% Coverage]

Reference 1 - 0.18% Coverage

the United   
States have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and   
data as well responding to, and recovering from incidents

Reference 2 - 0.18% Coverage

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive.

Reference 3 - 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 4 - 0.19% Coverage

REFINE ROLES AND RESPONSIBILITIES: The Admin-   
istration will clarify the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response.

Reference 5 - 0.17% Coverage

It will also identify   
and bridge existing gaps in responsibilities and coordination among Federal and non-Federal incident response efforts and promote more routine training, exercises, and coordination.

Reference 6 - 0.15% Coverage

The United States Government will strengthen efforts to share information with ICT providers to enable them to respond to and remediate known malicious cyber activity at the network level.

Reference 7 - 0.11% Coverage

These principles should form a basis for cooperative responses to counter irresponsible state actions inconsistent with this framework.

Reference 8 - 0.11% Coverage

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

Reference 9 - 0.20% Coverage

The Administration will conduct interagency policy planning for the time periods leading up to, during, and after the imposition of consequences to ensure a timely and consistent process for responding to and deterring malicious cyber activities.

Reference 10 - 0.15% Coverage

The United States will work with partners when appropriate to impose consequences against malicious cyber actors in response to their activities against our nation and interests.

Reference 11 - 0.28% Coverage

The United States will work with like-minded states to coordinate and support each other’s responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Military Strategy Description - § 1 reference coded [ 0.11% Coverage]

Reference 1 - 0.11% Coverage

 Respond to Threats

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 5 references coded [ 0.32% Coverage]

Reference 1 - 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.

Reference 2 - 0.04% Coverage

For Ally and partner countries that border Russia, the Department will support efforts to build out response options that enable cost imposition

Reference 3 - 0.04% Coverage

Competitors increasingly engage in gray zone operations at odds with international norms and below the threshold of a credible military response.

Reference 4 - 0.06% Coverage

The Department will be judicious in its use of defense resources and efforts to counter competitors’ coercive behaviors in gray zone operations, as traditional military tools may not always be the most appropriate response.

Reference 5 - 0.08% Coverage

The Department will conduct campaigning activities from this posture against a clear set of objectives, to include deterring adversary attacks, supporting rapid crisis response with survivable forces, and conducting operations to reinforce internationally-agreed-upon norms.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 1 reference coded [ 0.49% Coverage]

Reference 1 - 0.49% Coverage

 Focus technical and non-technical modernization into a resilient Joint Force and maintain the ability to respond to crises.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 9 references coded [ 0.55% Coverage]

Reference 1 - 0.06% Coverage

We will act decisively to defend, and deter disruptions to our democratic processes, and we will respond to future interference using all appropriate tools of national power.

Reference 2 - 0.07% Coverage

Integrated deterrence requires us to more effectively coordinate, network, and innovate so that any competitor thinking about pressing for advantage in one domain understands that we can respond in many others as well.

Reference 3 - 0.06% Coverage

We are leading a united, principled, and resolute response to Russia’s invasion and we have rallied the world to support the Ukrainian people as they bravely defend their country.

Reference 4 - 0.06% Coverage

The historic global response to Russia’s war against Ukraine sends a resounding message that countries cannot enjoy the benefits of global integration while trampling on the core tenets of the UN Charter.

Reference 5 - 0.06% Coverage

Third, the United States will deter and, as necessary, respond to Russian actions that threaten core U.S. interests, including Russian attacks on our infrastructure and our democracy.

Reference 6 - 0.03% Coverage

That requires building or expanding systems to prevent, detect, and respond to threats as they develop

Reference 7 - 0.07% Coverage

We are working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks.

Reference 8 - 0.08% Coverage

We aim to deter cyber attacks from state and non state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure.

Reference 9 - 0.06% Coverage

Iran’s threats against U.S. personnel as well as current and former U.S. officials will not be tolerated, and as we have demonstrated, we will respond when our people and interests are attacked.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 1 reference coded [ 0.26% Coverage]

Reference 1 - 0.26% Coverage

As the Department campaigns in cyberspace for this purpose, we will develop offensive and defensive options to support the Joint Force so that it is ready to respond rapidly across the spectrum of conflict.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 4 references coded [ 0.47% Coverage]

Reference 1 - 0.08% Coverage

When incidents occur, Federal response efforts must be coordinated and tightly integrated with private sector and State, local, Tribal, and territorial (SLTT) partners.

Reference 2 - 0.08% Coverage

When incidents do occur, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will enhance our awareness and ability to respond effectively.

Reference 3 - 0.14% Coverage

These timely notifications and CISA’s rapid sharing of relevant information with DOJ and other incident response stakeholders will strengthen our collective defense, improve efforts to identify the root causes of incidents, and inform decision-making within government on how to respond.

Reference 4 - 0.18% Coverage

The Federal Government has increased its capacity to respond to cyber incidents; arrested and successfully prosecuted transnational cybercriminals and state-sponsored actors; imposed sanctions on malicious cyber actors, including bans on travel and denying access to money service providers; and deprived threat actors of access to digital infrastructure and victim networks.