Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 1 reference coded [ 0.03% Coverage]

Reference 1 - 0.03% Coverage

make certain that regional adversaries gain no advantages from their acquisition of new, offensive military capabilities

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 16 references coded [ 2.09% Coverage]

Reference 1 - 0.06% Coverage

The North Korean attack on Sony was one of the most destructive cyberattacks on a U.S. entity to date.

Reference 2 - 0.07% Coverage

The increased use of cyberattacks as a political instrument reflects a dangerous trend in international relations.

Reference 3 - 0.14% Coverage

A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected.

Reference 4 - 0.12% Coverage

In concert with other agencies, the United States’ Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace.

Reference 5 - 0.08% Coverage

Such information sharing can significantly improve an organization’s ability to defend itself against a broad range of cyberattacks.

Reference 6 - 0.08% Coverage

For its second mission, DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence.

Reference 7 - 0.18% Coverage

While cyberattacks are assessed on a case-by-case and factspecific basis by the President and the U.S. national security team, significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States.

Reference 8 - 0.09% Coverage

National Mission Forces and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence

Reference 9 - 0.12% Coverage

The Defense Department must further develop adequate warning intelligence of adversary intentions and capabilities for conducting destructive and disruptive cyberattacks against DoD and the United States.

Reference 10 - 0.08% Coverage

Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence

Reference 11 - 0.16% Coverage

To conduct a disruptive or destructive cyber operation against a military system or industrial control system requires expertise, but a potential adversary need not spend   
9   
Th e De pa r tme n t o f De f e n s e Cy be r S t r a t e g y   
billions of dollars to develop an offensive capability.

Reference 12 - 0.12% Coverage

In addition to DoD’s own networks, a cyberattack on the critical infrastructure and key resources on which DoD relies for its operations could impact the U.S. military’s ability to operate in a contingency.

Reference 13 - 0.11% Coverage

If directed, DoD should be able to use cyber operations to disrupt an adversary’s command and control networks, military-related critical infrastructure, and weapons capabilities.

Reference 14 - 0.26% Coverage

Assess DoD’s cyber deterrence posture and strategy. Building off of the Defense Science Board’s Task Force on Cyber Deterrence, U.S. Strategic Command (USSTRATCOM), in coordination with the Joint Staff and the Office of the Secretary of Defense, will assess the Department of Defense’s ability to deter specific state and non-state actors from conducting cyberattacks of significant consequence on the U.S. homeland and against U.S. interests

Reference 15 - 0.27% Coverage

In conducting its analysis, USSTRATCOM must determine whether DoD is building the capabilities required for attributing and deterring key threats from conducting such attacks and recommend specific actions that DoD can take to improve its cyber deterrence posture. Careful attention should be devoted also to deterring non-state actors that may fall outside of traditional deterrence frameworks but which could pose a considerable threat to U.S. interests.

Reference 16 - 0.14% Coverage

State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States’ technological and military advantage.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 6 references coded [ 1.18% Coverage]

Reference 1 - 0.11% Coverage

North Korea also has conducted cyber attacks, including causing major damage to a U.S. corporation.

Reference 2 - 0.18% Coverage

attacks on our communications and sensing systems could occur with little to no warning, impacting our ability to assess, coordinate, communicate, and respond.

Reference 3 - 0.21% Coverage

Deterring a direct attack on the United States and our allies is a priority mission,   
requiring homeland and regional defenses tied to secure conventional and nuclear strike capabilities.

Reference 4 - 0.14% Coverage

Should any actor directly attack the United States or our interests, the U.S. military will   
take action to defend our Nation.

Reference 5 - 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 6 - 0.33% Coverage

In the event of an attack against the United States or one of its   
allies, the U.S. military along with allies and partners will project power across multiple domains to decisively defeat the adversary by compelling it to cease hostilities or render its military incapable of further aggression.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 1 reference coded [ 0.06% Coverage]

Reference 1 - 0.06% Coverage

when capture or other actions to disrupt the threat are not feasible, we will not hesitate to take decisive action.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 41 references coded [ 2.65% Coverage]

Reference 1 - 0.26% Coverage

At the same time, cyber attacks and some kinds of malicious cyber activity2 – particularly those conducted by nation-states or highly capable non-state actors and which target critical infrastructures and key industries in the United States – can constitute a significant threat to U.S. national security and economic interests.

Reference 2 - 0.22% Coverage

For the purpose of this document, a cyber attack refers to an attempt to deny access to, disrupt, disable, degrade, destroy, or otherwise render inoperable computers, information or communications systems, networks, or physical or virtual systems controlled by computers.

Reference 3 - 0.33% Coverage

Although cyber attacks can have a range of direct and indirect effects that vary in their severity, U.S. deterrence efforts are particularly focused on those attacks that could result in loss of life, harm to U.S. critical infrastructure, significant damage to property, or significant threats to the national security, foreign policy, or economic health or financial stability of the United States or its interests.

Reference 4 - 0.01% Coverage

cyber attacks

Reference 5 - 0.09% Coverage

the Administration is most concerned about threats that could cause wide-scale disruption, destruction

Reference 6 - 0.06% Coverage

Cyber attacks or other malicious cyber activity intended to cause casualties

Reference 7 - 0.23% Coverage

Cyber attacks or other malicious cyber activity intended to cause significant disruption to the normal functioning of U.S. society or government, including attacks against critical infrastructure that could damage systems used to provide key services4 to the public or the government.

Reference 8 - 0.21% Coverage

Cyber attacks or other malicious cyber activity that threatens the command and control of U.S. military forces, the freedom of maneuver of U.S. military forces, or the infrastructure on which the U.S. military relies to defend U.S. interests and commitments

Reference 9 - 0.09% Coverage

Malicious actors employ various tactics for attacking, exploiting, or disrupting networks, systems, and data.

Reference 10 - 0.12% Coverage

highly capable state and non-state adversaries that have the capability, expertise, and intent to conduct significant cyber attacks against us.

Reference 11 - 0.01% Coverage

cyber attack

Reference 12 - 0.01% Coverage

attacks

Reference 13 - 0.01% Coverage

cyber attacks

Reference 14 - 0.01% Coverage

cyber attacks

Reference 15 - 0.04% Coverage

conducting offensive and defensive cyber operations

Reference 16 - 0.01% Coverage

cyber attacks

Reference 17 - 0.07% Coverage

potential cascading effects from a cyber attack against their networks and systems.

Reference 18 - 0.03% Coverage

reconstitute rapidly if attacks succeed

Reference 19 - 0.02% Coverage

prepare for attacks

Reference 20 - 0.03% Coverage

defend the nation from cyber attacks.

Reference 21 - 0.01% Coverage

cyber attacks

Reference 22 - 0.01% Coverage

cyber attack

Reference 23 - 0.01% Coverage

cyber attacks

Reference 24 - 0.01% Coverage

attacks.

Reference 25 - 0.01% Coverage

attack)

Reference 26 - 0.02% Coverage

perpetrators of cyber attacks

Reference 27 - 0.03% Coverage

attacks on computers and networks

Reference 28 - 0.03% Coverage

respond to a cyber attack on the nation.

Reference 29 - 0.04% Coverage

could rapidly react to a cyber attack on the nation.

Reference 30 - 0.03% Coverage

defend the nation from cyber attacks

Reference 31 - 0.11% Coverage

Further, the Department of Defense is able, if directed, to conduct operations in cyberspace, including offensive cyber operations.

Reference 32 - 0.35% 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. Cyber operations can be narrowly tailored to target the precise system or systems that are perpetrating an attack against the United States. Further, the methods for neutralizing a malicious system can be sufficiently precise so as to minimize collateral effects.

Reference 33 - 0.02% Coverage

defend against cyber attacks

Reference 34 - 0.01% Coverage

cyber attacks

Reference 35 - 0.02% Coverage

destructive cyber attacks

Reference 36 - 0.01% Coverage

attacks

Reference 37 - 0.01% Coverage

cyber attacks

Reference 38 - 0.02% Coverage

crippling cyber attacks

Reference 39 - 0.02% Coverage

intentions to attack

Reference 40 - 0.01% Coverage

cyber attacks

Reference 41 - 0.01% Coverage

cyber attacks

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 26 references coded [ 1.38% Coverage]

Reference 1 - 0.04% Coverage

And we will pursue threats to their source, so that jihadist terrorists are stopped before they ever reach our borders

Reference 2 - 0.04% Coverage

We will target jihadist terrorists and transnational criminal organizations at their source and dismantle their networks of support.

Reference 3 - 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 4 - 0.04% Coverage

We will direct counterterrorism operations against terrorist WMD specialists, ﬁ nanciers, administrators, and facilitators.

Reference 5 - 0.08% Coverage

Pursue Th reats to Th eir Source   
There is no perfect defense against the range of threats facing our homeland. That is why America must, alongside allies and partners, stay on the offensive against those violent non-state groups that target the United States and our allies.

Reference 6 - 0.08% Coverage

Many of these jihadist terror-   
10   
P I L L AR I : PROTECT THE AMER ICAN PEOPL E , THE HOMEL AND, AND THE AMER ICAN WAY OF L I F E   
ists are likely to return to their home countries, from which they can continue to plot and launch att acks on the United States and our allies.

Reference 7 - 0.08% Coverage

e campaigns against ISIS and al-Qa’ida and their aﬃ liates demonstrate that the United States will enable partners and sustain direct action campaigns to destroy terrorists and their sources of support, making it harder for them to plot against us.

Reference 8 - 0.09% Coverage

Cyberattacks offer adversaries lowcost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.

Reference 9 - 0.03% Coverage

DEFEND IN DEPTH: U.S. agencies and foreign partners will target TCO leaders and their support infrastructure.

Reference 10 - 0.03% Coverage

As our reliance on computers and connectivity increases, we become increasingly vulnerable to cyberattacks.

Reference 11 - 0.05% Coverage

We will assess where cyberattacks could have catastrophic or cascading consequences and prioritize our protective efforts, capabilities, and defenses accordingly.

Reference 12 - 0.06% Coverage

They also enable adversaries to att empt strategic att acks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.

Reference 13 - 0.03% Coverage

Deterrence must be extended across all of these domains and must address all possible strategic attacks.

Reference 14 - 0.05% Coverage

Others believe that the ability to att ack space assets oﬀ ers an asymmetric advantage and as a result, are pursuing a range of anti-satellite (ASAT) weapons.

Reference 15 - 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 16 - 0.04% Coverage

Malicious state and non-state actors use cyberattacks for extortion, information warfare, disinformation, and more.

Reference 17 - 0.05% Coverage

Such att acks have the capability to harm large numbers of people and institutions with comparatively minimal investment and a troubling degree of deniability.

Reference 18 - 0.03% Coverage

These attacks can undermine faith and confidence in democratic institutions and the global economic system.

Reference 19 - 0.02% Coverage

Cyberattacks have become a key feature of modern conflict.

Reference 20 - 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 21 - 0.09% Coverage

The United States will, in concert with allies and partners, use the information-rich open-source environment to deny the ability of state and non-state actors to attack our citizens, conduct offensive intelligence activities, and degrade America’s democratic institutions.

Reference 22 - 0.05% Coverage

America’s competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information.

Reference 23 - 0.04% Coverage

Russia uses information operations as part of its offensive cyber efforts to influence public opinion across the globe.

Reference 24 - 0.09% Coverage

With its invasions of Georgia and Ukraine, Russia demonstrated its willingness to violate the sovereignty of states in the region. Russia continues to intimidate its neighbors with threatening behavior, such as nuclear posturing and the forward deployment of offensive capabilities.

Reference 25 - 0.06% Coverage

Attacks by ISIS and other jihadist groups in Spain, France, Germany, Belgium, the United Kingdom, and   
N A TI O N A L S E C U R IT Y S TR A TE G Y   
other countries show that our European partners continue to face serious threats.

Reference 26 - 0.06% Coverage

ISIS, al-Qa’ida, and their affi l iates operate on the cont inent and have increased the lethality of their attacks, expanded into new areas, and targeted U.S. citizens and interests.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 6 references coded [ 1.11% Coverage]

Reference 1 - 0.18% Coverage

Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and inter-   
I N T R O D U C T IO N   
national businesses and our allies and partners without paying costs likely to deter future cyber aggression.

Reference 2 - 0.18% Coverage

— including   
Non-state actors terrorists and   
criminals — exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states.

Reference 3 - 0.17% Coverage

We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war.

Reference 4 - 0.10% Coverage

As these sectors have modernized,   
N AT I O N A L C Y BE R S T R AT E G Y   
they have also become more vulnerable to cyber exploitation or attack

Reference 5 - 0.32% Coverage

Equipped with sizeable funds, organized criminal groups operating abroad employ sophisticated malicious software, spearphishing campaigns, and other hacking tools — some of which rival those of nation states in sophistication — to hack into sensitive financial systems, conduct massive data breaches, spread ransomware, attack critical infrastructure, and steal intellectual property.

Reference 6 - 0.16% Coverage

The United States Government will promote foundational engineering practices to reduce systemic fragility   
and develop designs that   
degrade and recover effectively when successfully attacked.