Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 5 references coded [ 0.22% Coverage]

Reference 1 - 0.03% Coverage

Thus, we are working with partners abroad to confront threats that often begin beyond our borders.

Reference 2 - 0.02% Coverage

Their support networks have global reach and are not contained by national borders

Reference 3 - 0.07% Coverage

Pandemics and Infectious Disease: The threat of contagious disease transcends political boundaries, and the ability to prevent, quickly detect and contain outbreaks with pandemic potential has never been so   
★ 48 ★   
I I I . advaNCINg Our INTereSTS   
important.

Reference 4 - 0.05% Coverage

These threats cross borders and continents and undermine the stability of nations, subverting government institutions through corruption and harming citizens worldwide.

Reference 5 - 0.06% Coverage

These shared areas, which exist outside exclusive national jurisdictions, are the connective tissue around our globe upon which all nations’ security   
★ 49 ★   
NaTIONal SeCurITy STraTegy   
and prosperity depend

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 1 reference coded [ 0.12% Coverage]

Reference 1 - 0.12% Coverage

extend across national boundaries and through multiple components of the global economy.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 7 references coded [ 0.91% Coverage]

Reference 1 - 0.11% Coverage

Technical challenges can be equally disruptive, as one country’s method for blocking a website can cascade into a much larger, international network disruption~

Reference 2 - 0.15% Coverage

These challenges transcend national borders; low costs of entry to cyberspace and the ability to establish an anonymous virtual presence can also lead to “safe havens” for criminals, with or without a state’s knowledge~

Reference 3 - 0.14% Coverage

Computers can communicate with one another across a seamless landscape of global networks permitting trusted, instantaneous communication with friends and colleagues down the block or around the world~

Reference 4 - 0.13% Coverage

Content is offered in local languages and flows freely beyond national borders, as improvements in digital translation open to millions a wealth of knowledge, new ideas, and rich debates~

Reference 5 - 0.20% Coverage

We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense~ Likewise, interconnected networks link nations more closely, so an attack on one nation’s networks may have impact far beyond its borders~

Reference 6 - 0.06% Coverage

The benefits of an interconnected world should not be limited by national borders~

Reference 7 - 0.11% Coverage

Equally important is the expectation that under normal circumstances, data will flow across borders without regard for its national origin or destination~

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 3 references coded [ 0.18% Coverage]

Reference 1 - 0.09% Coverage

“[M]ultiple vendors’products are used to configure U.S. telecommunications infrastructure and deliver services … that cross provider boundaries. As a result of the industry’s shift to a horizontal structure and its fragmentation into a large number of firms, neither vendors nor service providers are prepared to take responsibility for end-to-end systems design.”

Reference 2 - 0.06% Coverage

movement of data across jurisdictional boundaries presents challenges for law enforcement, the protection of privacy and civil liberties as defined by different countries, and liability decisions in the event of data or network breaches

Reference 3 - 0.03% Coverage

The United States cannot succeed by acting in isolation, because cyberspace crosses geographic and jurisdictional boundaries.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 3 references coded [ 0.39% Coverage]

Reference 1 - 0.08% Coverage

Computer code blurs the line between the cyber and physical world and connects millions of objects to the Internet or private networks.

Reference 2 - 0.12% Coverage

And an actor in one region of the globe can use cyber capabilities to strike directly at a network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems.

Reference 3 - 0.20% Coverage

The pursuit of security in cyberspace requires a whole-of-government and international approach due to the number and variety of stakeholders in the domain, the flow of information across international borders, and the distribution of responsibilities, authorities, and capabilities across governments and the private sector.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 1 reference coded [ 0.13% Coverage]

Reference 1 - 0.13% Coverage

Combating cybercrime is not only a domestic issue. Many adversaries use foreign-based infrastructure to stage their intrusions or disruptive activities.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 3 references coded [ 0.17% Coverage]

Reference 1 - 0.06% Coverage

Today, cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders.

Reference 2 - 0.07% Coverage

Since threats transit globally, passing through communications backbones without challenge, the U.S. Government will work with the private sector to remediate known bad activities at the network level to improve the security of all customers.

Reference 3 - 0.04% Coverage

the use of cyber tools have allowed state and non-state competitors to harm the United States across various domains.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 5 references coded [ 0.64% Coverage]

Reference 1 - 0.13% Coverage

The borderless nature of cybercrime, including state-sponsored and terrorist activities, requires strong international law enforcement partnerships.

Reference 2 - 0.18% Coverage

The United States will also lead in developing interoperable and mutually beneficial systems to encourage efficient cross-border   
information exchange for law   
enforcement purposes and reduce barriers to coordination.

Reference 3 - 0.04% Coverage

PROMOTE THE FREE FLOW OF DATA ACROSS BORDERS

Reference 4 - 0.11% Coverage

The United States will continue to lead by example and push back against unjustifiable barriers to the free flow of data and digital trade.

Reference 5 - 0.19% Coverage

Collaboration with allies and partners is also essential to ensure we can continue to benefit from the cross-border communications, content creation, and commerce generated by the open, interoperable architecture of the Internet.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Defense Strategy Summary - § 2 references coded [ 0.61% Coverage]

Reference 1 - 0.26% Coverage

We face an ever more lethal and disruptive battlefield, combined across domains, and conducted at increasing speed and reach—from close combat, throughout overseas theaters, and reaching to our homeland.

Reference 2 - 0.35% Coverage

It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Military Strategy Description - § 4 references coded [ 6.46% Coverage]

Reference 1 - 1.40% Coverage

From its global perspective, the NMS premises an adaptive and innovative Joint Force capable of employing its capabilities seamlessly across multiple regions and all domains -- continuing the transition from a regional to a global mindset and approach.

Reference 2 - 1.43% Coverage

In a security environment where the homeland is no longer a sanctuary and every operating domain is contested, competitors and adversaries will continue to operate across geographic regions and span multiple domains to offset or erode Joint Force advantages.

Reference 3 - 2.09% Coverage

To achieve military advantage over competitors and adversaries, the NMS introduces the notion of joint combined arms, defined as the conduct of operational art through the integration of joint capabilities in all domains. The Joint Force and its leaders must be as comfortable fighting in space or cyberspace as they are in the other three traditional domains of land, sea, or air.

Reference 4 - 1.54% Coverage

By proactively shaping the security environment through identifying and exploiting strategic opportunities, DFE aligns Joint Force actions across multiple global campaign plans, defense critical missions, time horizons, warfighting domains, and geographic boundaries.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 4 references coded [ 0.39% Coverage]

Reference 1 - 0.06% Coverage

Integrated deterrence entails working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of U.S. national power, and our network of Alliances and partnerships.

Reference 2 - 0.13% Coverage

Now and over the next two decades, we face strategic challenges stemming from complex interactions between a rapidly changing global balance of military   
capabilities; emerging   
technologies; competitor doctrines that pose new threats to the U.S. homeland and to strategic stability; an escalation of competitors’ coercive and malign activities in the “gray zone”; and transboundary challenges that impose new demands on the Joint Force and the defense enterprise.

Reference 3 - 0.14% Coverage

Competitor strategies seek to exploit perceived vulnerabilities in the American way of war, including by creating anti-access/area-denial environments; developing conventional capabilities to undertake rapid interventions; posing all-domain threats to the U.S. homeland in an effort to jeopardize the U.S. military’s ability to project power and counter regional aggression; and using the cyber and space domains to gain operational, logistical, and information advantages.

Reference 4 - 0.07% Coverage

The Department will improve its ability to operate in the face of multi-domain attacks on a growing surface of vital networks and critical infrastructure, both in the homeland and in collaboration with Allies and partners at risk.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 2 references coded [ 2.12% Coverage]

Reference 1 - 1.00% Coverage

The current environment requires the Joint Force to strengthen and integrate deterrence across domains, theaters, and the spectrum of conflict; modernize the nuclear enterprise; assure allies and partners; and prepare to prevail in great power conflict.

Reference 2 - 1.12% Coverage

Integrated Deterrence, the NDS’ principal strategic approach, generates warfighting advantages by synchronizing operations across warfighting domains, theaters, the spectrum of conflict, instruments of national power, the interagency, private sector, and allies and partners.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 7 references coded [ 0.43% Coverage]

Reference 1 - 0.05% Coverage

The second is that while this competition is underway, people all over the world are struggling to cope with the effects of shared challenges that cross borders

Reference 2 - 0.04% Coverage

The other is shared challenges—or what some call transnational challenges—that do not respect borders and affect all nations.

Reference 3 - 0.11% Coverage

Infectious diseases, terrorism, violent extremism, irregular migration, and other threats often emerge or accelerate due to deeper development challenges, and once they do, they do not recognize national borders. Transnational threats, in turn, undermine development, fuel poverty and human suffering, and feed a vicious circle.

Reference 4 - 0.07% Coverage

Integration across domains, recognizing that our competitors’ strategies operate across military (land, air, maritime, cyber, and space) and non-military (economic, technological, and information) domains—and we must too.

Reference 5 - 0.05% Coverage

We recognize that we must engage with all countries on global public health, including those with whom we disagree, because pandemics know no borders.

Reference 6 - 0.07% Coverage

Many of the biggest challenges in our world today—such as pandemics and health, climate change, fragility, migration and refugee flows—cross borders and disproportionately affect the poorest, most vulnerable populations.

Reference 7 - 0.04% Coverage

In today’s globalized world, international financial systems are used to stash illicit wealth abroad and to send bribes across borders.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 1 reference coded [ 0.22% Coverage]

Reference 1 - 0.22% Coverage

It undertakes cyber intrusion and surveillance efforts against individuals living beyond its borders, including U.S. citizens, whom it considers enemies of the state.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 10 references coded [ 1.31% Coverage]

Reference 1 - 0.16% Coverage

But they also have been misused to enable transnational repression and digital authoritarianism; steal data and intellectual property; distribute disinformation; disrupt critical infrastructure; proliferate online harassment, exploitation, and abuse; enable criminals and foster violent extremism; and threaten peace and stability.

Reference 2 - 0.12% Coverage

An attack on one organization, sector, or state can rapidly spill over to other sectors and regions, as happened during Russia’s 2017 “NotPetya” cyberattack on Ukraine, which spread across Europe, Asia, and the Americas, causing billions of dollars in damage.

Reference 3 - 0.08% Coverage

Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and exposing some of our most essential systems to disruption.

Reference 4 - 0.13% Coverage

Having successfully harnessed the Internet as the backbone of its surveillance state and influence capabilities, the PRC is exporting its vision of digital authoritarianism, striving to shape the global Internet in its image and imperiling human rights beyond its borders.

Reference 5 - 0.11% Coverage

Like its 2017 “NotPetya” attack, Russia’s cyberattacks in support of its 2022 brutal and unprovoked invasion of Ukraine have resulted in irresponsible spillover impacts onto civilian critical infrastructure in other European countries.

Reference 6 - 0.08% Coverage

When necessary, the United States will pursue cross-border regulatory harmonization to prevent cybersecurity requirements from impeding digital trade flows.

Reference 7 - 0.13% Coverage

Building on this momentum, the Administration will drive long-term efforts to defend the Federal enterprise and modernize Federal systems in accordance with zero trust principles that acknowledge threats must be countered both inside and outside traditional network boundaries.

Reference 8 - 0.10% Coverage

As ransomware is a borderless challenge requiring international cooperation, the White House has convened the Counter-Ransomware Initiative (CRI) with participation from more than thirty countries.

Reference 9 - 0.24% Coverage

The Indo-Pacific Economic Framework for Prosperity (IPEF) and the Americas Partnership for Economic Prosperity (APEP) create opportunities for the United States and regional governments to collaborate in setting rules of the road for the digital economy, including facilitating the development of technical standards, mechanisms to enable cross-border data flows that protect privacy while avoiding strict data localization requirements, and actions to foster supply chain security and resilience.

Reference 10 - 0.16% Coverage

The United States will work with our allies and partners, including through regional partnerships like IPEF, the Quad Critical and Emerging Technology Working Group, and the TTC, to identify and implement best practices in cross-border supply chain risk management and work to shift supply chains to flow through partner countries and trusted vendors.