Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 2 references coded [ 0.06% Coverage]

Reference 1 - 0.03% Coverage

Malicious activity must be defeated within a network and not be passed on to its destination whenever possible.

Reference 2 - 0.02% Coverage

This will require a resilient forward posture and agile global mobility forces.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 DoD Cyber Strategy Summary - § 5 references coded [ 3.17% Coverage]

Reference 1 - 0.37% Coverage

We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.

Reference 2 - 0.49% Coverage

We must assertively defend our interests in cyberspace below the level of armed conflict and ensure the readiness of our cyberspace operators to support the Joint Force in crisis and conflict.

Reference 3 - 0.38% Coverage

Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets.

Reference 4 - 0.78% Coverage

Persistently contest malicious cyber activity in day-to-day competition: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions.

Reference 5 - 1.15% Coverage

The 2018 DoD Cyber Strategy directs the Department to defend forward, shape the day-to-day competition, and prepare for war by building a more lethal force, expanding alliances and partnerships, reforming the Department, and cultivating talent, while actively competing against and deterring our competitors. Taken together, these mutually reinforcing activities will enable the Department to compete, deter, and win in the cyberspace domain.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 5 references coded [ 1.29% Coverage]

Reference 1 - 0.37% Coverage

The 2023 DoD Cyber Strategy is grounded in real-world experience. Since 2018, the Department has conducted a significant number of cyberspace operations through its policy of defending forward, actively disrupting malicious cyber activity before it can affect the U.S. Homeland.

Reference 2 - 0.31% Coverage

1. Defend the Nation. The Department will campaign in and through cyberspace to generate insights about cyber threats. We will defend forward, disrupting and degrading malicious cyber actors’ capabilities and supporting ecosystems.

Reference 3 - 0.23% Coverage

In cyberspace, the Department will harness outwardfacing capabilities to enable internal defense, identifying and mitigating threats before they can harm the American people.

Reference 4 - 0.19% Coverage

The Department will continue to defend forward by disrupting the activities of malicious cyber actors and degrading their supporting ecosystems.

Reference 5 - 0.20% Coverage

We will defend forward, disrupting and degrading malicious cyber actors, and help ensure the resilience of the homeland with all tools at our disposal.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 1 reference coded [ 0.10% Coverage]

Reference 1 - 0.10% Coverage

The Department of Defense’s strategic approach of defending forward has helped generate insights on threat actors, identify and expose malware, and disrupt malicious activity before it could affect its intended targets.