Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 2 references coded [ 0.36% Coverage]

Reference 1 - 0.26% Coverage

Cyberspace also has distinctive characteristics – including its global and interconnected nature, largely private ownership, potential for anonymity, and low barriers to entry for those who wish to cause damage – that pose challenges for deterrence that are different in kind and scope than deterrence in more traditional areas.

Reference 2 - 0.10% Coverage

The asymmetric advantages granted to malicious cyber actors reward competition, not cooperation, among nation-states.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 3 references coded [ 0.43% Coverage]

Reference 1 - 0.14% Coverage

Every day, cyber defenders foil state-backed attacks and prevent criminal plots around the world. But the underlying structural dynamics of the digital ecosystem frustrate their efforts. Its components remain prone to disruption, vulnerable to exploitation, and are often co-opted by malicious actors.

Reference 2 - 0.21% Coverage

Defending critical infrastructure against adversarial activity and other threats requires a model of cyber defense that emulates the distributed structure of the Internet. We will realize this distributed, networked model by developing and strengthening collaboration between defenders through structured roles and responsibilities and increased connectivity enabled by the automated exchange of data, information, and knowledge.

Reference 3 - 0.08% Coverage

The Internet is critical to our future but retains the fundamental structure of its past. Many of the technical foundations of the digital ecosystem are inherently vulnerable.