Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 1 reference coded [ 0.20% Coverage]

Reference 1 - 0.20% Coverage

We will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment and improving our ability to attribute and defeat attacks on our systems or supporting infrastructure.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 4 references coded [ 1.22% Coverage]

Reference 1 - 0.64% Coverage

Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source   
11   
Airman 1st Class Nate Hammond adjusts the frequency of a Roll-On Beyond Line of Sight Enhancement, or ROBE, data link system at the Transit Center at Manas, Kyrgyzstan. A ROBE connects manpower assets on the ground to other ground or airborne units. (U.S. Air Force photo/Senior Airman Brett Clashman)   
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   
collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor’s cyber persona, identify the attack’s point of origin, and determine tactics, techniques, and procedures. Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.

Reference 2 - 0.08% Coverage

Public and private attribution can play a significant role in dissuading cyber actors from conducting attacks in the first place.

Reference 3 - 0.22% Coverage

For example, the United States used verifiable and attributable data to engage China about the risks posed by its economic espionage. The attribution of this data allowed the United States to express concerns regarding the impact of Chinese intellectual property theft on U.S. economic competitiveness, and the potential risks posed to strategic stability by Chinese activity.

Reference 4 - 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.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 1 reference coded [ 0.08% Coverage]

Reference 1 - 0.08% Coverage

We will also develop technologies and tactics to deter and defeat efforts to attack our space systems; enable indications, warning, and attributions of such attacks;

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 4 references coded [ 0.79% Coverage]

Reference 1 - 0.17% Coverage

For the purpose of this document, attribution is defined as the capability to determine the identity or location of those responsible for conducting or directing cyber attacks or other malicious cyber activity.

Reference 2 - 0.20% Coverage

Although achieving a high degree of certainty in a timely manner can prove difficult, the United States is continually improving our ability to attribute malicious cyber activities and will hold malicious actors accountable for their actions.

Reference 3 - 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 4 - 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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 1 reference coded [ 0.09% Coverage]

Reference 1 - 0.09% Coverage

We will also invest in capabilities that improve the ability of the United States to attribute cyberatt acks. In accordance with the protection of civil liberties and privacy, the U.S. Government will expand collaboration with the private sector so that we can bett er detect and att ribute att acks.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 2 references coded [ 0.29% Coverage]

Reference 1 - 0.12% Coverage

We have publicly attributed malicious activity to the responsible adversaries and released details of the tools and infrastructure they employed.

Reference 2 - 0.17% Coverage

The IC will continue to lead the world in the use of all-source cyber intelligence to drive the identification and attribution of malicious cyber activity that threatens United States national interests.