Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 DoD Cyber Strategy Summary - § 1 reference coded [ 0.19% Coverage]

Reference 1 - 0.19% Coverage

Persistently contest malicious cyber activity in day-to-day competition

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 1 reference coded [ 0.05% Coverage]

Reference 1 - 0.05% Coverage

We will conduct cyberspace operations to degrade competitors’ malicious cyber activity and to prepare cyber capabilities to be used in crisis   
12 2022 NATIONAL DEFENSE STRATEGY   
or conflict.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 2 references coded [ 1.55% Coverage]

Reference 1 - 0.73% Coverage

This NMS renews our focus on campaigning now and building and sustaining warfighting advantage in tandem. Both are critical to prevail in war, and both are necessary to preserve the peace.

Reference 2 - 0.82% Coverage

5. LEVERAGE OPPORTUNITIES IN CAMPAIGNING   
Proactively identify and leverage opportunities to frustrate adversaries’ strengths, exploit vulnerabilities, and expand U.S. partnerships, access, and basing.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 2 references coded [ 0.70% Coverage]

Reference 1 - 0.29% Coverage

This malicious cyber activity informs the PRC’s preparations for war. The PRC’s theories of victory rest on the use of cyber means to degrade the combat capability of the Joint Force, as well as that of our Allies and partners.

Reference 2 - 0.41% Coverage

The Department will use cyberspace operations to enable and empower the Joint Force. These efforts will unfold in multiple ways: through persistent campaigning below the level of armed conflict1, through cyber defense and the fostering of cyber resilience, and through support of campaign and contingency planning.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 2 references coded [ 0.21% Coverage]

Reference 1 - 0.07% Coverage

The People’s Republic of China (PRC) now presents the broadest, most active, and most persistent threat to both government and private sector networks

Reference 2 - 0.14% Coverage

Russia remains a persistent cyber threat as it refines its cyber espionage, attack, influence, and disinformation capabilities to coerce sovereign countries, harbor transnational criminal actors, weaken U.S. alliances and partnerships, and subvert the rules-based international system.

**Annotations**

1 First direct linkage between persistence and campaigning.