CYBER 101 - Defend Forward and Persistent Engagement

By U.S. Cyber Command PAO / Published Oct. 25, 2022
FORT GEORGE G. MEADE, Md. ,

Cyberspace is not governed by a central body, but by numerous government and non-governmental organizations across the globe. The cyber domain is not naturally occurring and is wholly dependent upon owned or leased technology on both government and commercial infrastructure providers for its existence and operation. Due to the ever-evolving technological aspects of the information environment, adversaries are continuously looking to disrupt and degrade the integrity of U.S. information networks and those of its allies and partners.

These campaigns can take shape through overt efforts to infiltrate and disrupt U.S. Department of Defense (DOD) networks, steal information and intellectual property from U.S. government and private sector companies, and spread online disinformation campaigns designed to sow division among the American people. These activities present an unacceptable risk to the United States. Without a strategy to defeat these persistent campaigns, the United States risks death by a thousand cuts.

The 2018 Department of Defense Cyber Strategy states the United States will **defend forward** to disrupt malicious cyber activity at its source, including activity that falls below the level of armed conflict. This means if a device, a network, an organization, or adversary nation is identified as a threat to U.S. networks and institutions, or is actively attacking them in or through cyberspace – it can expect the United States to impose costs in response.

Responsibility for defending forward starts with **U.S. Cyber Command (USCYBERCOM)**. As the nation's cyber warriors, USCYBERCOM operates daily in cyberspace against capable adversary nations and non-state actors, such as terrorist groups and transnational criminal gangs. USCYBERCOM's mission is guided by the Command's commitment to intercept

USCYBERCOM's mission is guided by the Command's commitment to **persistent engagement**. Under this operational framework, cyber operators constantly work to intercept and halt cyber threats, degrade the capabilities and networks of adversaries, and continuously strengthen the cybersecurity of the Department of Defense Information Network (DODIN) that supports DOD missions.

Persistent engagement shifts DOD and USCYBERCOM's posture in cyberspace from reactive to proactive. Just as the U.S. Navy keeps the peace by sailing the seas, or the U.S. Air Force secures air space by patrolling the skies, USCYBERCOM actively seeks out threats in cyberspace and eliminates them to defend the United States and its allies. However, just as a navy goes underway from a port or an airplane takes off from a runway, and thus are legitimate targets during times of conflict – persistent engagement involves targeting adversary cyber capabilities and their underlying infrastructure. This approach prevents adversary nations and non-state actors from launching disruptive and destructive cyberattacks in the first place.

Partnerships form an integral component of persistent engagement. For example, USCYBERCOM conducts 'hunt forward operations' (HFOs) at the invitation of partner countries. These operations are strictly defensive and at the invitation of the host nation. During HFOs, USCYBERCOM operators sit side-by-side with partners searching for malicious cyber activities and vulnerabilities in host nation networks. The findings of HFOs, as well as other USCYBERCOM operations, are then shared with the public. These findings then help private sector software companies issue patches and updates as well as eliminate adversary network accesses and capabilities.

Each day, USCYBERCOM demonstrates its value and importance to the DOD and United States by defending the Nation in cyberspace, persistently engaging threats, and continuously upgrading defenses.