Cyber 101: Hunt Forward Operations

Published Nov. 15, 2022

By U.S. Cyber Command Public Affairs

FORT GEORGE G. MEADE, Md. -- Hunt Forward Operations (HFOs) are strictly defensive cyber operations conducted by U.S. Cyber Command (USCYBERCOM) at the request of partner nations. Upon invitation, USCYBERCOM Hunt Forward Teams deploy to partner nations to observe and detect malicious cyber activity on host nation networks. The operations generate insights that bolster homeland defense and increase the resiliency of shared networks from cyber threats.

HFOs are staffed exclusively from USCYBERCOM's Cyber National Mission Force (CNMF), which is comprised of specially trained personnel that secure and defend the Department of Defense Information Network (DODIN) against attacks from malicious cyber actors and foreign state adversaries.

While abroad, CNMF operators sit side-by-side with partners and hunt for vulnerabilities, malware, and adversary presence on the host nation's networks. USCYBERCOM shares insights from the HFO with the host nation, other government agencies like the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS), as well as private industry. These operations generate return on investment for the public because they bolster homeland and network defense while exposing adversary tactics, techniques, and procedures before they can be used against the United States.

HFOs implement USCYBERCOM's **persistent engagement** and **defend forward** strategy. U.S. networks are under constant assault from adversary nations and malicious cyber actors seeking to exploit vulnerabilities and disrupt U.S. society and military capabilities. In response, USCYBERCOM persistently engages adversaries in cyberspace in order to disrupt cyber threats, degrade the capabilities and networks of adversaries, and continuously harden the Department of Defense Information Network (DODIN). Defending forward requires operating as close to the origin of adversary activity as possible, increasing the reach of U.S. cyber operators and neutralizing the threat at its source.

From 2018 through 2022, USCYBERCOM's CNMF conducted more than two dozen HFOs with partner nations. Spanning the globe, CNMF operators deployed to sixteen different nations including Ukraine, Estonia, and Lithuania to name a few. In each instance, these partner-enabled operations have led to the public release of more than 90 malware samples for analysis by the cybersecurity community.

The insights generated from HFOs have proven invaluable to defending the United States from outside aggression and malicious behavior in cyberspace. In 2020, USCYBERCOM conducted eleven HFOs in nine different nations that contributed to the successful defense of the 2020 elections from foreign influence and interference. In 2021, USCYBERCOM conducted a joint HFO with the Cybersecurity and Infrastructure Security Agency (CISA) in response to the SolarWinds supply chain attack that yielded eight files attributed to the Russian Intelligence Service (SVR) APT 29. These operations yielded information about adversary tactics, techniques, procedures, and intentions.

USCYBERCOM is committed to persistently engaging adversaries who would harm the United States and will continue to conduct HFOs at the request of allied and partner nations in order to build a safer, more secure world in cyberspace.