Before the Invasion: Hunt Forward Operations in Ukraine

Before the Invasion: Hunt Forward Operations in Ukraine
Before the Invasion: Hunt Forward Operations in Ukraine

By Cyber National Mission Force Public Affairs / Published Nov. 28, 2022
FORT GEORGE G. MEADE, Md.,

U.S. joint forces, in close cooperation with the government of Ukraine, conducted defensive cyber operations alongside Ukrainian Cyber Command personnel from December 2021 to March 2022, as part of a wider effort to contribute to enhancing the cyber resiliency in national critical networks.

Late last year with the consent of Ukraine, U.S. Cyber Command deployed its largest hunt forward team yet. The joint team of U.S. Navy and U.S. Marine Corps operators hunted for malicious cyber activity on Ukrainian networks. The operation persisted until days before Russian forces launched a wide-scale invasion of the nation.

The Ukrainian government provided the hunt forward teams with access to multiple networks. Sitting side-by-side Ukrainian and U.S. cyber professionals began a meticulous multi-prong hunt looking for suspected malicious cyber activity. This mission postured our Ukrainian counterparts to identify and address any potential threats on their networks and mitigate in order of severity.

“Cyber National Mission Force was honored to work side-by-side with our Ukrainian partners, hunting adversaries on their networks with them,” said U.S. Army Maj. Gen. William J. Hartman, commander of Cyber National Mission Force. “This sort of mission was critical to both our nations’ defenses in cyberspace – particularly in the face of Russian aggression – and reflects our enduring partnership with Ukraine,” Hartman added.

In addition to conducting a hunt forward on the ground, the team provided remote analytic and advisory support using new and innovative techniques, and conducted network defense activities aligned to critical networks.

The hunt forward team was present in Ukraine when Russia began executing destructive cyber-attacks in mid-January. They worked closely with the Ukrainian partners, and assisted in analyzing the attacks while also sharing that information with U.S. domestic interagency and industry partners for homeland defense.

Although the hunt forward team is no longer deployed to Ukraine, CYBERCOM remains committed and continues to provide support to Ukraine, other allies and partner nations, with U.S. joint forces aligned and supporting the European Theater. This support included information sharing of threats and cyber insights, such as indicators of compromise and malware. For example, in July 2022, CNMF publically disclosed novel indicators to cybersecurity industry partners in close collaboration with the Security Service of Ukraine.

CYBERCOM routinely conducts hunt forward operations globally as part of the Command's "Defend Forward" strategy. By remaining persistently engaged in foreign spaces the command is uniquely positioned with capabilities and insights to learn adversary activities improving collective cybersecurity.

In addition to countering the malicious cyber actors who target partner nations' networks, data and platforms, the U.S. and its allies gain valuable insight into adversaries' tactics, techniques, procedures, plans, capabilities and tools. This further enables the U.S. and its allies and partners to disrupt or halt malicious cyber activity before it reaches friendly networks and causes harm.

Hunt forward operations are purely defensive activities and operations are informed by intelligence. They are key to CYBERCOM's persistent engagement strategy, aimed at defending and disrupting malicious cyber activities and bolstering the homeland defense of U.S. and our partner nations.