“Committed Partners in Cyberspace”: Following cyberattack, US conducts first defensive Hunt Operation in Albania

Hunt Forward Albania
Combined American/Albanian flag with CNMF logo

By Cyber National Mission Force Public Affairs / Published March 23, 2023

FORT GEORGE G. MEADE, Md. / TIRANA, ALBANIA—“Following a significant cyberattack on Albania in 2022, a team of cyber operators from the U.S. Cyber National Mission Force (CNMF) conducted their first-ever defensive cyber operation there, returning recently with a strengthened partnership with Albania and unique insights into malicious cyber activity.”

U.S. Cyber Command’s CNMF deployed a Hunt Forward team in collaboration with Albania to conduct network defense activities alongside the partner nation to identify, monitor, and analyze adversary tactics, techniques, and procedures.

Hunt Forward Operations are defensive missions that allow countries to better understand the shared threats and to enhance the security of critical networks that the U.S., allies, and partners depend on.

“We are looking forward to increased collaboration with AKSHI [The National Agency for Information Society] in order to establish a resilient ecosystem and a green zone in our public infrastructures,” said Dr. Igli Tafa, General Director and National Cyber Coordinator in the National Authority for Electronic Certification and Cyber Security (NAECCS) of Albania, and is responsible for supervising the law and policies on cybersecurity and trusted services.

In July 2022, Iranian cyber actors launched a cyberattack against the Government of Albania. According to U.S. Cybersecurity & Infrastructure Security Agency (CISA), these same Iranian actors used similar tactics, techniques, and procedures in another wave of cyber-attacks against the Government of Albania in September 2022. Following the cyberattacks, the U.S. strongly condemned Iran's cyberattack against its NATO ally, and reaffirmed its support to Albania’s efforts to strengthen its cybersecurity.

“The United States is committed to working with Albania on securing its digital future, and ensuring that connectivity is a force for innovation, productivity, and empowerment,” said Nathaniel Fick, U.S. Ambassador at Large for Cyberspace and Digital Policy. “We will continue to support our NATO ally Albania’s remediation efforts, and invite partners to join us alongside our NATO allies in holding Iran accountable for its destructive cyberattacks against Albania in July and September 2022.”

Over the course of the three-month deployment, CNMF cyber operators worked closely with Albanian cyber partners, hunting for malicious cyber activity and identifying vulnerabilities on networks of Albania’s choice.

“The cooperation with U.S. Cyber Command was very effective and made us feel safe by assuring that we have followed all the right steps in responding to these sophisticated attacks,” said Mirlinda Karçanaj, General Director of National Agency of Information Society (AKSHI), an institution of the Albanian Government that coordinates the development and administration of state information systems. “We hope that this cooperation will continue in the future so that we can further exchange experiences and increase our capacities to another level.”

The U.S. cyber operators provided technical findings from their network hunt to the Government of Albania, enabling the partner to take steps toward bolstering their network defense. Those insights have proven invaluable to defending the United States from outside aggression and malicious cyber behavior in cyberspace.

Hunt Forward Operations are conducted collaboratively with the partner nation and with elite military and federal civilian cyber operators from CYBERCOM. During the operation, U.S. operators sit side-by-side with host nation counterparts, hunting only on those networks the partner has identified and provided access to.

“The partnerships we build will enable better cyber defense in the future-- they strengthen our ability to defend our Nations,” said U.S. Army Maj. Gen. William J. Hartman, commander of Cyber National Mission Force. “These hunts bring us closer to adversary activity to better understand and then defend ourselves, but they also bring the U.S. closer to our partners and allies. These relationships are key to protecting our networks and critical infrastructure against shared threats.”

When hunting on partner networks, Albanian and U.S. cyber operators can observe malicious cyber actors’ TTPs in real-time. With the nation’s permission, the U.S. team can then bring those insights back to the U.S. to share across the private and public sector, hardening defenses before adversaries can target U.S. networks.

While critical to strengthening U.S. cybersecurity, Hunt Forward Operations also develop and build strategic relationships with key allies and partners. These activities enhance allies’ and partners’ cybersecurity posture, which makes it more difficult for foreign adversaries to operate on networks globally.

“In an increasingly dynamic environment where malicious cyber actors attempt to exploit our networks, data, and critical infrastructure, we have a key asymmetric advantage that our adversaries don’t have: enduring partnerships like this one with Albania,” said Hartman. “When we are invited to hunt on a partner nations’ networks, we are able to find an adversary's insidious activity in cyberspace, and share with our partner to take action on. We can then impose costs on our adversaries by exposing their tools, tactics and procedures, and improve the cybersecurity posture of our partners and allies. When we share information, we are all more defended from those who seek to do us harm."

In cybersecurity, ‘hunting’ is a proactive cyber defense activity, to observe and mitigate threats that are undetected on a network or system. While HFO teams do not mitigate threats on partner networks, they enable their counterparts to pursue and address the threats found.

CNMF has deployed 44 times to 22 countries and conducted hunt operations on nearly 70 networks around the world. In addition to Albania, teams have deployed to Ukraine, Estonia, Lithuania, Croatia, Montenegro, North Macedonia, and other nations since 2018.

On December 19, 2022, CNMF was elevated to a subordinate unified command highlighting the evolution of a persistent, professional cyber force today and into the future. Since its inception in 2014, CYBERCOM’s CNMF has rapidly evolved to meet the needs of the Nation, and has participated in, or responded to almost every national crisis the United States has faced.