“Shared threats, shared understanding”: U.S., Canada and Latvia conclude defensive Hunt Operations

Hunt Forward Latvia
flag graphic
By Cyber National Mission Force Public Affairs / Published May 10, 2023

FORT GEORGE G. MEADE, Md. / RIGA, LATVIA -- A team of cyber experts from U.S. Cyber Command’s Cyber National Mission Force (CNMF) recently returned from a hunt forward operation in Latvia.

During the three-month long operation, the U.S. team worked with CERT.LV, the Information Security Incident Response Institution of the Republic of Latvia – on a defensive cyber threat hunting operation focused on the Latvian critical infrastructure. CERT.LV plays a critical role in safeguarding Latvia's cyber ecosystem and supporting the country's digital transformation.

The U.S. team worked in tandem with Canadian Armed Forces and Latvian allies, to support their defensive operations, as well-- marking the first time American and Canadian forces have conducted hunts simultaneously.

By sharing information about cyber threats in real time, the allied nations can improve their collective cyber resilience and defenses.

“With our trusted allies, the U.S. and Canada, we are able to deter cyber threat actors and strengthen our mutual resilience,” said Baiba Kaškina, General Manager of CERT.LV. “This can only happen through real-life defensive cyber operations and collaboration. The defensive cyber operations conducted allowed us to ensure our state infrastructure is a harder target for malicious cyber actors.”

Hunt Forward Operations are defensive cyber operations, intelligence-driven and partner-requested. CNMF hunt teams operate on a network of the partner’s choosing to detect, monitor and analyze tactics, techniques and procedures of malicious cyber actors.

The Canadian cyber task force has a historic relationship with Latvian cyber security professionals, and work in direct support of their efforts. Canada has been leading NATO’s enhanced Forward Presence (eFP) Battle Group in Latvia since 2017. While the U.S. team was deployed, both U.S. and Canadian teams worked together on different networks, sharing information and threat hunt indicators with each other and Latvian officials.

These operations can help bolster the security of partner nations and provide us advanced notice of adversary tools and techniques.

“Every day, we see malicious cyber actors take deliberate and irresponsible actions to target us, steal from us, and attack our systems. Partnerships like this one with Latvia are key to our defense,” said U.S. Army Maj. Gen. William J. Hartman, commander of Cyber National Mission Force. “We share threats, but more importantly, we share an understanding and strategic relationship in cyberspace that go beyond this hunt forward operation.”

As part of CYBERCOM’s Defend Forward strategy, CNMF has worked with several partner nations as part of hunt forward missions. During these missions, U.S. and partner nation cyber experts are building capacity in cyberspace, sharing threat information, and enhancing network resilience and defense.

Partner nation trust and collaboration often result in CNMF hunt teams returning to the U.S. with additional insights on adversary tools, techniques and procedures (TTPs).

“Latvia has demonstrated incredible resilience for the past year, having been among the most targeted EU states by Russian hacktivists and Russian state-supporting hacking groups,” said Kaškina. “We remain focused on making sure critical infrastructure and e-services are secure and are available for general public and the government.”

During the hunt activities in Latvia, the cyber teams found malware, analyzed it and have an increased understanding of the adversary’s TTPs.

“Adversaries often use spaces outside the U.S. as a testbed for cyber tactics, which they may use later to access U.S. networks,” said Hartman. “But with our hunt forward missions, we can deploy a team of talented people to work with our partners, find that activity before it harms the U.S., and better posture the partner to harden critical systems against bad actors who threaten us all.”

CNMF has deployed 47 times to 22 countries and conducted hunt operations on over 70 networks around the world. This is CNMF’s second deployment to Latvia. Additionally, teams have deployed to Ukraine, Albania, Estonia, Lithuania, Croatia, Montenegro, North Macedonia, and other nations since 2018.

CNMF’s core mission is to defend the nation in and through cyberspace, halting, disrupting, and imposing costs on adversaries who are attempting to interfere in the U.S. democratic processes, steal intellectual property, or attack critical infrastructure. On December 19, 2022, CNMF was elevated to a subordinate unified command under CYBERCOM, and is postured to leverage the speed and unity of effort to defend the U.S. and its partners and allies.

CERT.LV contributes to the global cybersecurity community by participating in international collaboration forums (e.g. FIRST, TF-CSIRT, European CSIRTs Network and others) regularly contributing to exchange of expertise and sharing knowledge. CERT.LV importance lies in providing a coordinated response to cyber incidents and facilitating information sharing among different stakeholders, including governmental institutions, private sector, and academia.

CERT.LV operates under the Ministry of Defence of the Republic of Latvia and is regulated by the Information Technology Security Law.