Vermont National Guard Cyber Capabilities Overview November 2025

Overall Classification: UNCLASSIFIED

COL Hazel Kreider
VTARNG Chief Information Officer
hazel.e.kreider.mil@army.mil
802-338-3834

MAJ Bryan Geraci
Commander
158th Communications SQDN
bryan.geraci@us.af.mil
802-660-5496

MAJ Thomas Ledwidge
Operations Officer
229th Cyber Operations SQDN
thomas.ledwidge@us.af.mil
802-338-4319

Agenda

- Cyber Citizen Soldier
- Vermont National Guard Cyber Units, Capabilities, and Training
  - Army
  - Air
- Flexible Response Framework
- Administrative & Logistics
- Questions

Cyber Citizen Soldier

- Works in the civilian cybersecurity industry
- Highly trained, skilled, and experienced
- Civilian education and industry certifications
- Top Secret government security clearance
- Available to reinforce government and critical infrastructure upon request of the Governor or at the direction of DOD authority

Vermont National Guard Cyber Capabilities

- Detachment 2 (Critical Infrastructure Team) 136th Cyber Security Company, 126th Cyber Battalion, 91st Cyber Brigade (9 Soldiers)
- Defensive Cyberspace Operations Element (9 Soldiers)
- 3-124th Information Operations Battalion
- 229th Cyberspace Operations Squadron (67 Airmen)
- 158th Communications Squadron (46 Airmen)

Critical Infrastructure Team (CIT)

- **Mission:** Conduct Defensive Cyberspace Operations (DCO) in support of Department of Defense Information Network (DODIN) and non-DODIN critical infrastructure.
- **Employment**
  - Expertise in Industrial Control Systems and Supervisory Control and Data Acquisition (SCADA)
  - Cyber operations planning, vulnerability assessments, ICS system hardening recommendations, and threat identification and response
  - Hands-on keyboard Incident response in support of state if requested by civilian authorities (based on legal guidance and MOU / MOA establishment)
  - Can be deployed out of state to support federal cybersecurity missions
- **Resources**
  - 9 personnel
  - May require Judge Advocate General (JAG) legal augmentation on site
  - Reach back support from Cyber Security Company (Massachusetts ARNG) and U.S. Army Cyber Command

Defensive Cyberspace Operations Element (DCOE)

Mission: Conducts Defensive Cyberspace Operations (DCO) to secure Vermont's portion of the Department of Defense Information Network. In State Active-Duty status can protect State critical infrastructure, provide cybersecurity compliance and readiness support, and respond to state cyberspace emergencies as directed by Governor or Adjutant General.

- **Employment**
  - Operate networks
  - Cybersecurity compliance and readiness
  - Cyber operations planning, network vulnerability assessments, network hardening recommendations, and forensic analysis
  - Hands-on keyboard Incident response in support of state if requested by civilian authorities (based on legal guidance and MOU / MOA establishment)
- **Resources**
  - 9 personnel
  - May require Judge Advocate General (JAG) legal augmentation on site
  - Reach back support from U.S. Army Cyber Command and Army National Guard Common Cybersecurity Provider

3-124th Information Operations Battalion

Mission: Provides realistic, robust and relevant Information Operations and Cybersecurity training to prepare students to perform in an ever-changing operational environment.*

Cybersecurity Courses:

- **Incident Response Hander (IRH)**
  - 40-hour, web based asynchronous course focused on defensive cyber operations
  - Based on a cybersecurity incident scenario with incident response planning requirements
  - Students gain familiarity with UNIX and Windows vulnerabilities
- **Operational Training Experience (OTE)**
  - 14-day hands on resident course focused on defensive cyberspace operations
  - Based on National Institute of Standards and Technology cybersecurity framework core
  - Utilizes hardware and software to include Kali-Linux, WireShark, Nessus, Metasploit, Unix, Security Onion, Digital Forensics, Windows and Active Directory

** 3-124th IO BN personnel have the training, certifications, and skill sets to augment other VTNG units during a cybersecurity incident response.*

VTARNG Cyber Training & Experiences

- Cyber Yankee Exercise (2026 will be the 12th year)
  - Federal Region 1 (New England States)
  - Hands on keyboard exercise with a live opposing force using realistic threat tactics and conducted at the unclassified level
  - Exercising National Guard reinforcement of response to cyber attack against State Government and Critical Infrastructure
  - Whole of Government / CI approach: State Government, National Guard/DoD, Utilities, DHS CISA, FEMA, DOJ, FBI, FERC, NERC, Sector ISACs
- Cyber Shield Exercise (National Guard Bureau Exercise)
- Cyber Tatanka Exercise
- Locked Shields Exercise (NATO Exercise)
- DEFCON Hacking Convention
- HammerCon Military Cyber professionals Association Convention
- Department of Defense Persistent Cybersecurity Training Environment
- State Active-Duty support to UVM during response to ransomware attack
- Multiple deployments in support of federal missions

229th Cyberspace Operations Squadron

Mission: Provide professional threat-aware forces to defend the Department of Defense Information network (DoDIN) and the State of Vermont ‘s cyberspace terrain from malicious actors through data driven Defensive Cyberspace Operations.

- **Employment**
  - Force provider to Cyber Command for Cyberspace Protection Team
  - Conduct intelligence-enabled hunt operations on specified terrain
  - Counter and clear adversary activity on specified terrain
  - Enable hardening of specified terrain in cyberspace
  - Assess effectiveness of response actions against current and future risk
- **Resources**
  - 67 personnel
  - Air Force Cyber Vulnerability Assessment/Hunt (CVA/H) weapon system
  - May require Judge Advocate General (JAG) legal augmentation on site

158th Communications Squadron

Mission: To provide the cyber capabilities needed to ensure our warfighter's success through Confidentiality of critical information, the Integrity of data, and the Availability of the cyber resources needed for the successful completion of our federal missions across the globe and for the citizens of the State of Vermont.

- **Employment**
  - Operate networks
  - Cybersecurity compliance and readiness
  - Secured communications capabilities
  - Hands-on communications support of state if requested by civilian authorities (based on legal guidance and MOU / MOA establishment)
- **Resources**
  - 46 personnel
  - Radios
  - Civilian SatComm
  - May require Judge Advocate General (JAG) legal augmentation on site

VTANG Cyber Training & Experiences

- Cyber Yankee Exercise
- Locked Shields International Exercise
- Cruz Ex International Exercise
- Department of Defense Persistent Cybersecurity Training Environment
- Deployed members in support of Cyber Command on Cyber Protection Teams

Flexible Response Framework

- Most likely that a combination of Soldiers and Airmen from various VTNG units would be needed to respond to a cybersecurity incident
- Individual capabilities-based response as opposed to a military unit-based response
- Cyber Advisory Team
  - Made up of experts from various units; selected based on the incident
  - Assess the situation (with individual non-disclosure agreements in place)
  - Recommend needed resources and correct response package to the VTNG Chief Information Officer
  - May include JAG augmentation on site for MOA / MOU establishment and refinement
  - Reach back support to National Cyber Mission Force, CISA, Army Cyber Command, or FBI if necessary
- Cost per day for response team estimated to range between $2k - $4k depending on response team composition
- How to request

Administrative & Logistics

- How to request support
- Army teams have some organic computer equipment
- Time from request to boots on ground varies based on which skill sets / personnel are needed
- Development of a MOA/MOU with left and right limits is essential
- Cost per day for response team estimated to range between $2k - $4k depending on response team composition

Questions?