Vermont National Guard Cyber Capabilities Overview October 2025

Overall Classification: UNCLASSIFIED

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

Agenda

- Cyber Citizen Soldier
- Vermont National Guard Cyber Units, Capabilities, and Training
  - Army
  - Air
- Flexible Response Framework
- Operations, Admin, & Logistics Considerations
- 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 Cyber Operations Squadron
- 158th Communications Flight

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 (ICS) and Supervisory Control and Data Acquisition (SCADA)
  - Cyber operations planning, vulnerability assessments, ICS system 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)
  - 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: Conduct 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

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
- 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

Vermont Air Guard Cyber Capabilities

- 229th Cyber Operations Squadron
- 158th Communications Flight

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

Operations, Admin, and Logistics Considerations

- How to request support
- Time from request to boots on ground varies based on which skill sets / personnel are needed
- Logistics considerations:
  - Computer equipment use
  - Meals
  - Transportation
  - Communications
- Development of a MOA/MOU with left and right limits is essential
- Cost per day for response team estimated to range between $2k - $5k depending on response team composition

Questions?