The Minnesota National Guard
Cyber Coordination Cell

Our Mission

ENSURE THE MINNESOTA NATIONAL GUARD CYBER OPERATIONS FORCES ARE PREPARED TO RESPOND TO STATE OR FEDERAL REQUESTS FOR MILITARY CYBER OPERATIONS SUPPORT.

The Minnesota National Guard Cyber Coordination Cell

We accomplish our mission through *three* primary lines of effort:

→ **Optimize** MNNG cyber force training activities through development of cyber skills planned against our most significant risks
(train for the most likely scenarios: incident/ransomware response; vulnerability assessments; network security monitoring; threat hunting & clearing; Critical Infrastructure Operational Technology response)

→ **Cultivate** and maintain strong relationships built on mutual trust with relevant state and federal departments, agencies, and groups
(participate in state and federal Table-Top Exercises & cyber live environment training exercises, cyber intel-sharing partnerships, and validate/codify partner expectations)

→ **Equip** MNNG cyber forces with state-owned and C3 managed "always ready" cyber incident response equipment, connectivity, software, and tools capable of immediate response
(maintain and deploy incident response endpoints, software, network taps, high-computer and high-capacity servers, out-of-band internet FirstNet connectivity, and peripherals to emergency teams)

About The C3

The C3 is not a cyber incident response team itself

- It is a planning, coordination, and strategy development office.
- Activities sets the conditions to enable MN military cyber forces to respond effectively.
- Serves as the primary coordination office for military cyber response events.
- Acquires and maintains always-ready cyber incident response equipment for cyber forces.

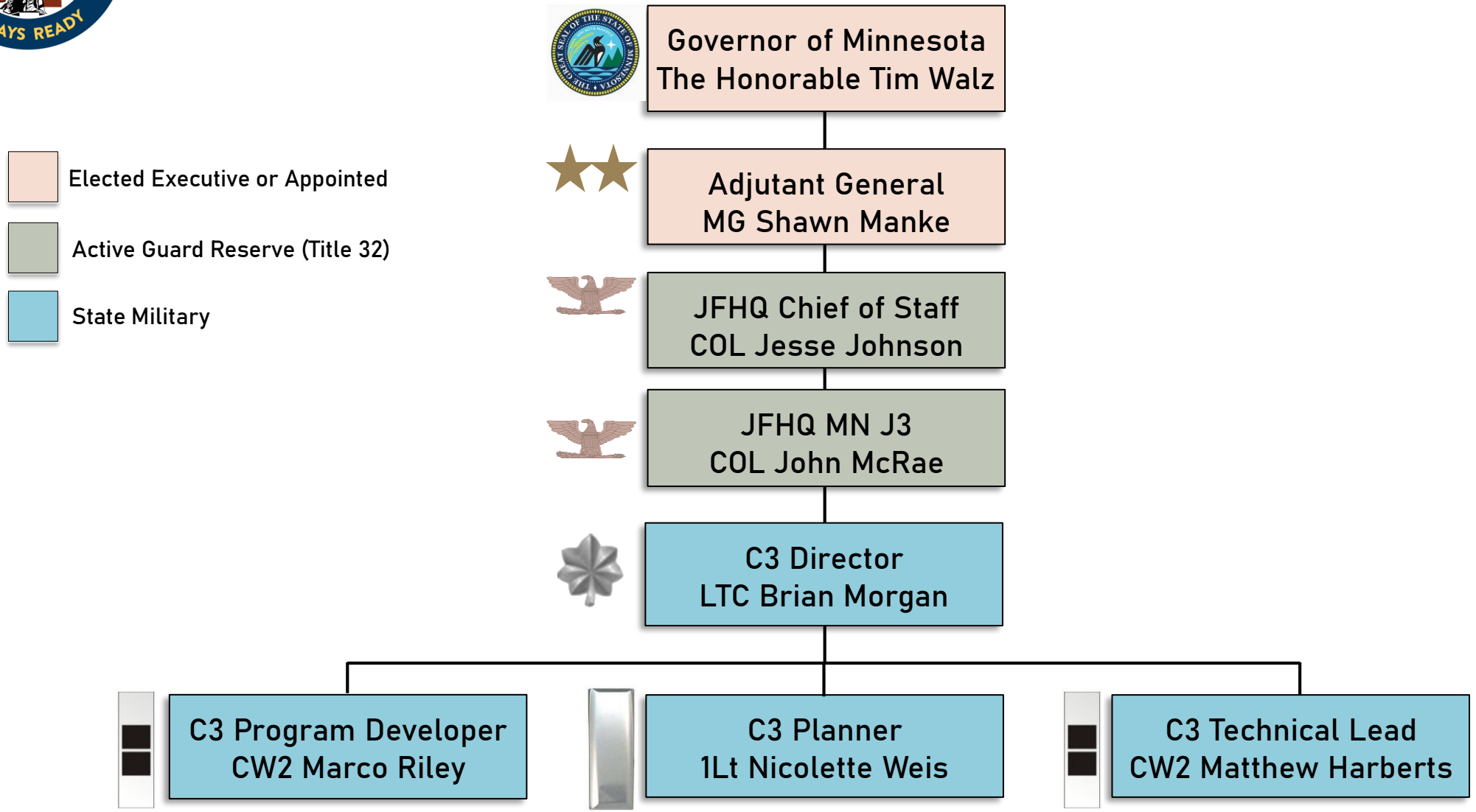
The C3 establishes partnerships with relevant stakeholders who may be involved in cyber response

- Prepare to support Dept of War operations in a federal capacity during an emergency.
- Enhance cyber force readiness and skillsets through academic partnerships
- C3 **supports** the state's Whole of State Cybersecurity Plan through various mechanisms, including configuration hardening tools to State, Local, Tribal, and Territorial (SLTT) entities.
- Encourage SLTT adoption of state-subsidized security resources i.e. MNIT platforms.

The C3 coordinates cyber-operations related efforts for:

- State Partnership Program cyber exercises and knowledge sharing events
- Involvement in regional cyber exercises, events, rehearsals, and Table-Top Exercises.
- Cyber officer career management and navigation of the federal cyber branch acceptance process.

Cyber Coordination Cell (C3) Hierarchy

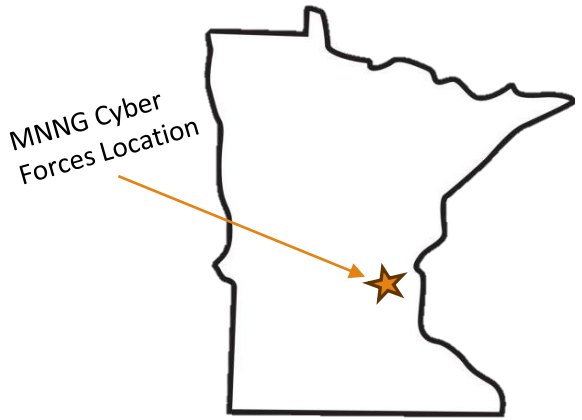


MN Cyber Forces

177th Cyber Protection Team		Defensive Cyber Ops Element		Cyber Coordination Cell	
Status:	**Part-time**	Status:	**Part-time**	Status:	Full-time
Role:	Cyber Response	Role:	Cyber Response	Role:	Cyber Coordination
#	40 Soldiers	#	5x Soldiers / Airmen	#	4x Soldiers / Airmen

- Total Cyber Forces = ~50
  - **<u>90% of which have full-time civilian jobs outside of the MNNG</u>**
  - Most members work full-time in corporate or government roles

- Specialized cyber training takes anywhere from ~7 months to ~2 years



Ready-To-Deploy Incident Response Equipment

Laptops -jump servers (VM-ready + storage + compute) – FirstNet cellular internet
network taps – backpacks – transit cases – forensic software – host/network analysis software

The Power of Partnership

Lessons from a Citywide Cyber Incident

Partnerships and Relationship Building is our Strategic Foundation

- 200+ engagements in 2024-2025 with State, DoD, Critical Infrastructure, Federal and Academic Partners

2025 Minnesota Military Cyber Symposium

Presentations by FBI, NGB, CISA, INFRAGARD, MNIT, 177 CPT, DMA C3

Conferences

- Spoke or participated at 34 Conferences
- Spearheaded first ever Cyber Village at the 2025 Cyber Security Summit, connecting local public entities with state cyber support

ST PAUL CYBER RESPONSE MISSION (*Executive Order 25-08*)

State
Active
Duty

A Historical First: The Minnesota National Guard Cyber Forces were activated in response to a ransomware attack which crippled the city's IT

C3 provided mission coordination between city, state, and federal agencies, operational support, resource fulfillment, public affairs support, command and control support, and a comprehensive post-mortem for record.

Cyber Shield ‘25

- C3 played a key coordination role in Cyber Shield 2025, the DoD's largest cyber exercise, with over 900 participants, 15 countries (SPP) , 38 U.S states & territories

- Fostered partnership combining Minnesota and Norwegian cyber forces into a single team.

WE EDUCATE SLTT ENTITIES ON THE **CONDITIONS** AND **PROCESS** TO REQUEST NATIONAL GUARD EMERGENCY SUPPORT

Criteria and Process for State Emergency Activation

As with any Minnesota emergency…

- The situation is beyond the capacity of tribal, local and state government to control and all civil resources have been exhausted.
- Required resources are not available from commercial sources, including contracted (if it's a public entity with a strict fixed budget, this criteria can be simple to meet).
- When public service is lost or withdrawn and an immediate substantial threat to public health, safety or welfare is evident.
- Assistance is limited to tasks that the National Guard can perform more efficiently and effectively than any other agency.

WE EDUCATE SLTT ENTITIES ON THE **CONDITIONS** AND **PROCESS** TO REQUEST NATIONAL GUARD EMERGENCY SUPPORT

State Emergency Activation Process

Cyber Incident (Ransomware, etc.)

SHERIFF → Minnesota BCA Bureau of Criminal Apprehension → HSEM Homeland Security and Emergency Management → Governor's Office

*OR

MINNESOTA IT SERVICES

* If affected entity uses MNIT services, they should contact MNIT SOC first

Remember - The National Guard is the Last Resort, but Always Ready, Always There in times of true emergency

***State Duty Officer**	**(651) 649-5451**
MNNG Joint Operations Center	**(651) 268-8860**
MNIT SOC	**(651) 297-1111**


MNNG
CYBER COORDINATION CELL