THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 141-158
https://doi.org/10.55682/cdr/r5tj-8fph

PROFESSIONAL COMMENTARY

Voices from Cyber Yankee: Lessons for Strengthening Critical Infrastructure Cyber Protection

Sarah J. M. Lohmann[1,2], Jason C. Brown*†[1]

[1]Army Cyber Institute, United States Military Academy, West Point, NY, USA
[2]University of Washington, Seattle, WA, USA

Cyberattacks on critical infrastructure increasingly threaten national security, public safety, and economic stability. This commentary analyzes Cyber Yankee—a regional, multi-agency cyber exercise in New England (United States)—as a model exercise for the U.S. Department of War (DoW) and its partners. Drawing on perspectives from senior military and National Guard leaders, it traces the evolution of the exercise since 2014 and examines its distinctive integration of utilities and operational technology (OT) operators through a collaborative Blue–Orange Team format. The paper situates Cyber Yankee within the broader cyber Unified Coordination Group (UCG) framework and identifies opportunities to adapt its principles for active-duty operations under the Defense Support of Civil Authorities (DSCA) model. Findings highlight the enduring value of long-term public–private partnerships, the cultivation of trust and interoperability before crises, and the replicability of the UCG model for coordinated cyber response. The commentary concludes with recommendations to enhance readiness nationwide, including deeper engagement with critical-infrastructure operators in exercise design, routine practice of Request for Support and Cyber 9-Line processes, expanded OT- and ICS-focused training for Guard cyber teams, alignment of these skills within Joint Qualification Records, and the development of flexible, modular response packages that reflect real-world incident needs.

Keywords: cyber defense readiness, cyber defense exercise, U.S. National Guard cyber operations, critical infrastructure protection, unified coordination group (UCG), Operational Technology (OT) security

* Corresponding author: jason.brown@westpoint.edu
† Both authors contributed equally to this research.

INTRODUCTION

When the University of Vermont Medical Center was unable to provide critical patient services for over two weeks due to a massive cyber-attack in 2020, Emergency Services called the Vermont National Guard to help with incident response (Barry and Perlroth 2020; Leffler 2023). Responding to this kind of cyber emergency that impacts critical infrastructure was something the Guardsmen had already trained for together in a training exercise called *Cyber Yankee*. It is the involvement of the utilities and critical service operators in the exercises that makes Cyber Yankee stand apart from others.

"*There was a personal relationship between the National Guard and the municipal level and the infrastructure partners. They understood the capabilities, the experience and the exposure,*" said Col. (Ret.) Richard Berthao. "*It is not just the value of the point-in-time training. The cyber-attack on the Vermont hospital with ransomware where the Vermont National Guard helped, is a demonstration of a coordinated response of how the exercises help provide training and support for assessments and resiliency work.*"

Col. (Ret.) Berthao, then the IT Director for the Massachusetts National Guard, started Cyber Yankee in 2014 as a regional exercise among the six New England states. He designed it to simulate cyber-attacks on civilian infrastructure. Unlike traditional military cyber drills, Cyber Yankee focuses on real-world systems—power plants, water treatment facilities, hospitals, and transportation networks—that make up the systems and assets essential to national security, public health, and economic stability.

In this paper, we share a "voice from the field" that demonstrates how New England states collaborate across the public-private divide to secure and defend critical infrastructure from cyber threats. As part of the team that supported training the Unified Coordination Group (UCG) portion of the exercise, we provided unique and experimental modules on futures-oriented thinking and a roleplaying cyber tabletop workshop that generated many insightful comments about the readiness of the UCG to respond to local and state-level cyber incidents. As we will demonstrate later, personal involvement, either as an observer or as a participant, is the most impactful factor in developing the relationships that make the UCG, and Cyber Yankee, a model exercise. We also share challenges and points of friction that make this kind of collaboration *hard*, but *necessary*.

Our observations are based on semi-structured interviews with several founders of Cyber Yankee, senior cyber leaders within both Active and Guard organizations, and on personal attendance at Cyber Yankee 2025. In these conversations, we explored questions such as:

- What are best practices and coordination frameworks for active duty military to train and be prepared to provide cyber incident response together with utilities and civil institutions?

- Can the Unified Coordination Group concept as defined by CISA's recently released Cyber Incident Response Plan (CISA 2025)[1] and also practiced by Cyber Yankee serves as a model, and how can this be improved?
- Does NORTHCOM (U.S. Northern Command)[2] already have coordination frameworks in place for U.S. active duty military defense support of civil authorities that could serve as a training and preparedness model?

In addition, the authors developed and delivered hands-on workshops for participants in the Unified Coordination Group track. These workshops facilitated Chatham House rules conversations about the opportunities and challenges that arise when cyber incident response spans public, private, government, and military responsibilities, and how the collective cyber force can address these issues in the future. While Cyber Yankee is not the *only* way to train for a compromising cyber event on defense critical infrastructure, its experiments with Orange Teams, operational technology, joint and multi-national partnerships, and the Unified Coordination Group track are demonstrably worth sharing with the rest of the cyber force.

Cyber Yankee represents a distinctive innovation within the National Guard's cyber readiness program, offering realistic, experimental training that directly addresses the growing threat to critical infrastructure. Drawing on insights from participating leaders and organizers, the paper argues that the exercise's principal contribution lies in its deliberate incorporation of the Unified Coordination Group framework into regional training. Embedding this UCG component across future National Guard and interagency exercises would significantly enhance the coherence and effectiveness of Defense Support to Civil Authorities (DSCA) during complex and large-scale cyber incidents.

CYBER YANKEE: A MODEL FOR PUBLIC–PRIVATE CYBER COLLABORATION

How the Cyber Yankee Exercise Unfolds

Cyber Yankee is an annual, multi-state cyber defense exercise hosted by the National Guard across the New England region. Established in 2014, it brings together military cyber units, federal agencies, state partners, and critical infrastructure utilities to rehearse coordinated responses to complex cyber incidents. Designed to strengthen public–private collaboration and to integrate operational technology environments into training, Cyber Yankee serves as one of the most advanced regional exercises in the United States.

Cyber Yankee typically unfolds over several days and follows a structured progression from individualized training, team-level orientation, then full-scale operations. The exercise begins

1. The National Cyber Incident Response Plan (NCIRP) describes a national approach to handling significant cyber incidents. It addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents. It also describes how the actions of all these stakeholders fit together to provide an integrated response.

2. U.S. Northern Command is the Department of War combatant command responsible for homeland defense, civil support, and security cooperation within its area of responsibility, which includes the continental United States, Alaska, Canada, Mexico, and surrounding waters.

with a scenario briefing, during which cyber teams of the National Guard, utility partners, and state/federal observers receive intelligence updates, threat indicators, and operational constraints that frame the simulated crisis. The teams then move into network familiarization and baseline establishment, analyzing the exercise environment—an emulated but functionally realistic network with industrial control system (ICS) components representing power, water, and oil/gas infrastructure.

Daily activities often include situation updates, interagency coordination meetings, and facilitated discussions with observers from the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Cyber Command (USCYBERCOM), state fusion centers, and private-sector utilities. The final day typically involves a culminating event—a coordinated multi-vector attack designed to stress-test response capacity—followed by an after-action review (AAR) where teams identify gaps, lessons learned, and recommendations for real-world improvements.

Cyber Yankee uses a red team (cyber adversary) vs. blue team (cyber defender) format for training the "on keyboard" skills of cyber operators. Once the exercise transitions into active play, the red team mimics real-world adversaries using tactics like phishing, malware, and exploitation of industrial control systems (ICS). Blue teams, composed of cyber units-including members of cyber protection teams (CPTs)-individuals, and civilian defenders of the National Guard, must detect, respond to, and recover from these attacks.

Blue teams also advise a unique arrangement of Orange Teams, which represent real utility operators like power and water, and must approve, deny, or request support in accordance with the current cyber national response framework. Orange teams are normally used as security educators and knowledge managers to build a culture of good code reviews and develop training workshops (Mag 2025). At Cyber Yankee, cyber response experts from an actual utility fill the Orange team and become the person receiving daily situation updates from the Blue team assigned to their sector. This framework requires that utility owners make a formal request for assistance to the National Guard just as they would in a real incident (CISA, n.d.). During this phase, participants must submit Cyber 9-Line reports, escalate incidents to federal partners, and practice collaborative decision-making under time pressure.

Exercise scenarios are structured to evaluate the effectiveness of incident response coordination [3], the robustness of legal and policy frameworks, the quality of public–private communication, and the technical resilience of Operational Technology (OT) systems. Cyber Yankee's Blue Team–Orange Team configuration has increasingly attracted participants from across the nation to play roles or assess the exercise, including officials from the U.S. Army, Air Force, Navy, Space Force, Coast Guard, Department of Homeland Security, FBI, and a range of critical infrastructure utilities. In recent years, organizers have also made deliberate efforts

3. Research on cyber defense teams provides validated metrics to assess team performance during exercises (Maennel, Ottis, and Maennel 2017; Granåsen and Andersson 2016).

to expand participation among industry partners and utilities—particularly in the energy and water sectors—to strengthen realism and foster broader engagement. Cyber Yankee also extends participation to State Partnership Program countries that are aligned to the New England states. In 2025, eleven partner nations sent participants to join Blue teams or to observe and prepare to join teams in future exercises.

Landscape of National Guard–Led and Participatory Cyber Exercises

Across the United States, comparable cyber exercises are conducted annually at the national level and in regional formats, as shown in Table 1. These cyber exercises are led either by National Guard units or are characterized by strong National Guard participation. Collectively, these initiatives reflect the varied approaches adopted across states and international partnerships to address evolving cybersecurity challenges. Each exercise is shaped by its regional context, operational objectives, and the specific capabilities of participating organizations, illustrating the adaptive nature of cyber readiness training within the United States.

While these initiatives share similar goals, Cyber Yankee remains distinctive in its integration of diverse stakeholders and experimental objectives. An international review of sixteen cyber defense exercises published in 2019 already identified Cyber Yankee as having a high level of maturity (Brajdić, Kovačević, and Groš 2021). The broader literature also contrasts multiple exercises, drawing out insights into how they differ in scope, design, and impact on cyber preparedness (Dewar 2018).

Over time, these exercises illustrate a clear evolution in U.S. and allied cyber defense readiness. Early initiatives such as *Locked Shields* (CCDCOE) and *Cyber Guard* focused primarily on building technical proficiency, multinational interoperability in simulated environments, and NATO's collective defense doctrine (Smeets 2022). Mid-decade efforts, including *Cyber Yankee* and *Jack Voltaic* (ACI 2025), expanded the scope to include public–private collaboration and the protection of critical infrastructure, highlighting the growing role of the National Guard as a bridge between federal and state authorities. More recent exercises, such as *Cyber Discovery* and *Balikatan*, demonstrate a shift toward realistic, live-network testing and international coalition building across the Indo-Pacific. Taken together, these developments reveal a trajectory from technical training toward integrated resilience-building—linking military, civil, and industry actors in a unified approach to cyber defense.

As Maj. Gen. Terin Williams, the Special Assistant to the Director of the Army National Guard for U.S. Army Cyber Matters observed: "*What sets Cyber Yankee apart from other non-Guard cyber exercises is that you have critical infrastructure partners, private, state, and local entities and the Guard*". She participated in the most recent Cyber Yankee exercise by roleplaying as an operational technology (OT) operator for the scenario's fictional city. She emphasized the importance of maintaining this collaborative model: "*That needs to continue with the other regional exercises.*"

Table 1. Chronological Overview of Major Cyber Defense Exercises Involving the U.S. National Guard and Partners

Exercise	Started	Lead / Host Organization(s)	Geographic Scope	Core Focus / Features	Recent Developments (2024–2025)
Locked Shields	2010	NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)	International	Live-fire cyber defense; multinational interoperability; complex joint operations	U.S. contingent led by West Virginia National Guard (2025); emphasis on rapid decision-making under attack (Bodker 2025).
Cyber Guard	2012	U.S. Cyber Command (CYBERCOM), DHS, FBI	National / International	Offensive and defensive operations; federal–state coordination; interagency readiness	22 countries represented (2017); globally coordinated, multi-domain training event (2025) (R. Johnson 2012; U.S. Department of War 2017).
Cyber Flag	2011	U.S. Cyber Command (CYBERCOM)	National / International	Training for Cyber Mission Force (CMF) teams; advanced defensive and offensive cyberspace operations; federal-level readiness	Cyber Flag 24-2 was the first iteration to integrate Offensive Cyberspace Operations (OCO); Guard participation occurs only when activated under Title 10.
Cyber Shield	2013	National Guard Bureau	National / State Partner Program	Education, defensive skills, and capture-the-flag events; validation of Cyber Protection Teams (CPTs)	>42 states and partner nations participating (2025) (Martin 2025; Roudabush 2025; Tarkelly 2025); expanded CPT validation framework (Estrada 2022).
Cyber Yankee	2014	Six New England State National Guards	Regional (USA)	Protection of critical infrastructure; integration of utilities and Operational Technology (OT) systems; Unified Coordination Group (UCG) training	Linked with U.S. CYBERCOM via Cyber 9-Line (2022); expanded OT simulation and interagency interoperability (2023) (Pomerleau 2022).
Jack Voltaic™	2016	U.S. Army Cyber Institute (West Point)	National / Public–Private	Cyber preparedness and critical infrastructure interdependencies; multi-city, public–private collaboration	5.0 iteration (2025) advancing toward a Homeland Defense cyber readiness ecosystem (ACI 2025).
Vigilant Guard	2017	U.S. Northern Command and State National Guards	Regional (Hawai'i / Alaska)	All-hazards incident response integrating cyber and physical disruptions	2025 exercise combined environmental and cyber crises; linked to *Jack Voltaic*™ methodology (Bedard 2025).
Cyber Tatanka	2019	Nebraska National Guard	Regional (Midwest USA)	Anomaly detection and incident response on simulated networks; collaboration with public power utilities	Continued partnerships with utilities; expanded red-team training modules (Hynes 2025).
Cyber Dawn	2019	California National Guard	Regional (West USA)	Red-vs-blue competitions; simulated attacks on public services and essential digital infrastructure	Added municipal and smart-city scenarios (2025) (A. H. Johnson 2022; Loeffler 2025).
Cyber Fortress	2022	Virginia Defense Force, 91st Cyber Brigade	State	Simulated attacks on state level infrastructure	Validation exercises for state cyber protection teams (CPT) (Puryear 2023; StateDefenseForce.com 2025).
Cyber Discovery	2022	Idaho National Guard	State / Regional	Controlled attacks on real networks; high-fidelity incident response training	Expanded to private-sector networks (2025) (Edinger 2025; Eisenbrandt 2025).
Balikatan / CYDEX	2023	Guam & Hawai'i National Guards / Philippine Armed Forces	Multinational (Indo-Pacific)	Cyber defense, threat hunting, education, and critical infrastructure protection	Ongoing CYDEX series reinforcing regional partnerships (2025) (Scott 2025; Jeney 2025).

UNDERSTANDING THE CYBER UNIFIED COORDINATION GROUP (UCG)

In 2021, the Cyber Yankee organizers increased the level of inter- and intragovernmental cooperation by formally incorporating and exercising the concept of a Cyber Unified Coordination Group (UCG)—the national mechanism through which federal lead agencies coordinate their response to a significant cyber incident. A UCG brings together the three federal leads identified in U.S. cyber incident doctrine: the FBI as the lead for threat response, CISA as the lead for asset response, and the Office of the Director of National Intelligence (ODNI) through the Cyber Threat Intelligence Integration Center as the lead for intelligence support.

When an incident affects a specific industry, the relevant Sector Risk Management Agencies (SRMAs) also join the UCG, along with state, local, tribal, territorial, and affected private-sector partners as needed. Examples of these SRMAs include the Department of Energy for the Energy Sector, the Department of Homeland Security for sectors such as Communications and Critical Manufacturing, the Environmental Protection Agency for Water and Wastewater Systems, the Department of War for the defense industrial base, and the Department of the Treasury for Financial Services.

The federal framework underpinning these roles (Table 2) was first established in Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, which clarified federal and sector responsibilities and formalized the role of Sector Risk Management Agencies (Executive Office of the President 2013). Subsequent legislation, including the National Cybersecurity Protection Act of 2014 (United States Congress 2014), reinforced the need for adaptable national cyber incident response structures.

Building on this foundation, Presidential Policy Directive 41 (PPD-41) issued during the Obama administration in 2016 (Executive Office of the President 2016) defined the federal government's approach to coordinating responses to major cyber incidents and formally established the UCG as the mechanism for integrating threat, asset, and intelligence response functions. CISA's most recent National Cyber Incident Response Plan (NCIRP) (CISA 2025), further operationalizes this model, describing the UCG as the primary forum for ensuring unity of effort during a cyber crisis. By integrating a UCG-like structure into its design, Cyber Yankee provides participants with the opportunity to rehearse these national coordination processes on a regional scale and under realistic operational conditions.

According to CISA, these Sector-Specific Agencies (SSAs)—the predecessors to today's SRMAs [4]— are incorporated into a Cyber UCG whenever a cyber incident affects or is likely to affect the sectors they represent. SSAs were directed through Presidential Policy Directive 21 in 2013 to ensure that "institutional knowledge and specialized expertise about the sector" is

4. Although the 2013 Presidential Policy Directive 21 referred to federal sector-leads as "Sector-Specific Agencies (SSAs)", subsequent legislation and policy clarified and codified the term "Sector Risk Management Agencies (SRMAs).

available to the President to "carry out incident management responsibilities" and "mitigate incidents" (Executive Office of the President 2013).

Table 2 provides an overview of these key federal policies and laws—ranging from PPD-21 to the National Cyber Incident Response Plan—that establish the legal and operational foundations for the UCG model.

Table 2. Key U.S. Policy and Legal Foundations for Cyber Incident Coordination

Document	Year	Focus
Presidential Policy Directive 21 (PPD-21): *Critical Infrastructure Security and Resilience*	2013	Establishes the modern federal framework for critical infrastructure security and resilience; clarifies federal roles and defines Sector Risk Management Agencies (SRMAs).
National Cybersecurity Protection Act	2014	Requires development and regular updating of adaptable cyber incident response plans for critical infrastructure; provides statutory support for national cyber incident coordination.
Presidential Policy Directive 41 (PPD-41): *United States Cyber Incident Coordination*	2016	Defines federal agency roles in significant cyber incidents; formalizes the Unified Coordination Group (UCG) as the mechanism for integrated threat, asset, and intelligence coordination.
National Cyber Incident Response Plan (NCIRP)	2016–2024	Operational plan implementing PPD-41; details how UCGs function, including activation criteria, membership, and coordination processes for major cyber incidents.

CYBER YANKEE AND THE UCG APPLICABILITY FOR ACTIVE-DUTY FORCES

The U.S. National Guard within the UCG

Because Cyber Yankee incorporates federal, state, military, and private-sector partners, it raises the question of whether its coordination model could inform active-duty approaches to cyber incident response. Could this format work as a tool for active-duty military to train, mitigate and respond to cyber threats impacting the Department of War?

"*Yes, it can,*" said Brig. Gen. Christine Rummel, the J-6 director of cyberspace operations at the North American Aerospace Defense Command (NORAD) and USNORTHCOM. "*At the heart of all incident response, regardless of domain, is trust... The benefit of the National Guard's cyber exercises, such as Cyber Yankee, is that it builds that trust; develops tactics, techniques, and procures (TTPs); builds relationships; and develops contact rosters all before a disaster occurs so that teams are not trying to determine who is who and what capabilities are available to bring to bear on the problem set.*" Rummel's emphasis on pre-established trust highlights a core advantage of National Guard-centric training models: their ability to build interpersonal and interorganizational relationships long before a crisis.

These relationships are most effective when they are developed and exercised well in advance of a cyber incident. During the 2020 SolarWinds attack and subsequent federal response, the National Security Council did not enlist the National Guard Bureau to respond. According to one analysis, "This failure likely stemmed from a lack of knowledge of the capabilities of or the process for engaging National Guard entities" (Ihme et al. 2025). Ihme

et al. (2025) describe the actions the federal C-UCG (Cyber UCG) took in response to SolarWinds, and they point out that there was some amount of dysfunction within the federal government's post-SolarWinds reporting requirements. They state,

> Conducting regular interagency training exercises among cyber response agencies, such as the National Guard's Cyber Yankee exercise, can simulate real-world cyber responses, enhance interagency coordination and communication, and promote a culture of collaboration across all levels of government that breaks down silos and fosters transparency. Finally, by leveraging Department of War (DoW) entities under Title 32 and defense support to civil authorities, the National Guard can assist state and federal governments in cyber protection, detection, and red teaming" (Ihme et al. 2025).

This is precisely the type of assistance the National Guard is meant for.

Under the current NCIRP, CISA may serve as the executive secretariat for a Cyber UCG, coordinating with the FBI, ODNI's Cyber Threat Intelligence Integration Center, Sector Risk Management Agencies, and affected federal departments as needed (CISA 2025). National Guard support to these efforts is usually authorized under U.S. Code Title 32 (*U.S. Code* 1956b), which allows National Guard forces to remain under state control while being federally funded. Activation under Title 10 authorities (*U.S. Code* 1956a), which governs federal active-duty military forces and are used during war or national emergencies, is reserved for rare cases (see Figure 1).

One such case occurred during the COVID-19 pandemic, when Title 10 authorities were used to activate both active-duty forces and the National Guard during Operation Warp Speed: "*We were activated on Title 10 during Operation Warp Speed and deputized under DHS Title 6 to protect networks associated with the distribution of COVID [vaccines] to protect the Industrial Control Systems of American manufacturers of the vaccine,*" said Lt. Col. Peter Kurek, a member of the Massachusetts National Guard. Having been involved with the Cyber Yankee exercise for years, he noted that the level of trust developed in the exercise helped execute the mission more effectively.

Active Duty Support to Domestic Cyber Incidents

Although Cyber Yankee incorporates elements of the UCG model, active-duty involvement in domestic incidents follows a different mechanism. For missions outside the Department of War Information Network (DoWIN), USNORTHCOM operates under the Defense Support of Civil Authorities (DSCA) framework, which governs how and when DoW forces may assist civil agencies. The Cyber DSCA process includes participation from CISA, the Department of War, USCYBERCOM, and USNORTHCOM, and reflects legal authorities distinct from those used by National Guard units.

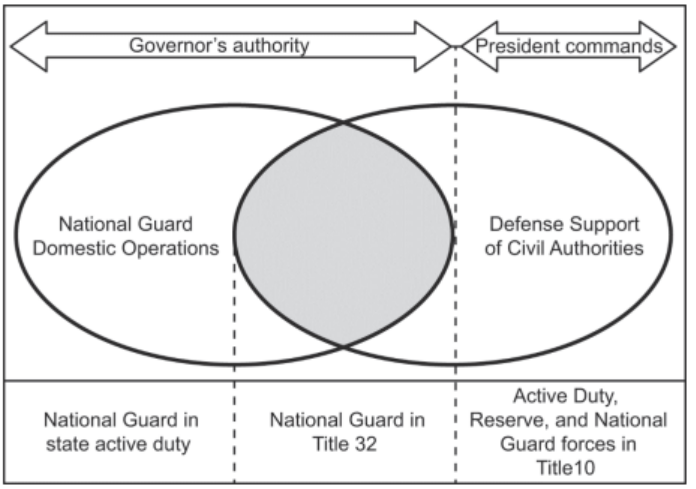

Figure 1. National Guard T10/T32 Authorities, (reproduced from Air Land Sea Application Center (2021)

.

Fortunately, the legal structure for active-duty military to support a cyber incident response effort if asked already exists. The National Cybersecurity Protection Act of 2014 (Public Law 113-282) stipulates that:

> "Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 226) to critical infrastructure" (United States Congress 2014).

The Department of War's Role within the Cyber UCG

The Department of War's role within the Cyber UCG can be even more far-reaching. It provides cybersecurity assistance to the Defense Industrial Base, helps during civilian emergencies, and supports civil authorities. US Cyber Command, as the main cyber action arm for the DoW is directed to exercise with DoW component cyber incident response organizations, and to train their incident response teams (including assigned cyber protection teams) (DoD 2023). However, only in rare cases do active duty military provide such assistance if the impact is outside the DoWIN. An exception occurs when requested by the DoW, a federal lead agency, or the President, and provides mitigations and threat reports via the National Security Agency and the DoW Cyber Crime Center (CISA 2025).

Maj. Gen. Terin Williams emphasized this distinction, noting that the UCG model cannot be applied identically to active-duty forces because their mandates differ. Active-duty military personnel are usually asked, using DSCA authorities, to come in once for a particular industry

or utility cyber incident, whereas the National Guard maintains enduring relationships with utilities and state agencies. These longstanding partnerships, cultivated through exercises like Cyber Yankee, enable smoother coordination during an incident.

However, PPD-41 defines the UCG as "the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts" (Executive Office of the President 2016). This means that the military, both active and Guard, should be skilled at navigating a cyber UCG during operations in which Title 10 forces are acting in a DSCA capacity.

"*Just as with any other domain or response action, participants need to understand their left and right limits, and what authority they are operating under. It's expected that if called to participate in a Cyber UCG, that the platform the personnel are responding on is off-DoWIN, where military have no authority unless requested to provide specific support,*" Brig. Gen. Rummel said.

Operating under that authority is especially important in the exercises, Lt. Col. Kurek said. "*In a realistic scenario, military members are not likely to get the direct access to a network as they do in most current exercises.… Somebody from the Guard or the military will not be allowed to touch the network in the case of an actual cybersecurity incident. To make it more realistic, you need to have more industry participation where business and utilities are at the keyboard and to transfer that knowledge from soldiers or airmen to the utilities, to industry,*" he said. "*In Operation Warp Speed, we used strategically placed sensors in the industrial networks that fed into our own monitoring tools and worked with company personnel to address detected activity.*" In this way, military responders can train, assist, and advise their industry partners.

In 2025, Army Cyber Command (ARCYBER) sent several observers from its Future Plans Directorate to examine how Cyber Yankee's methods might translate into active-duty formations. According to Col. Dave McNatt, ARCYBER's chief of plans and strategy, "*Real crisis response will almost always start off-DoWIN. [Cyber Yankee] is one of the few mature exercises that exposes Title 10 folk to the system of leaders, planners, operators, and coordinators that would deal with those incidents. Like the [ancient] Greeks taught us, you have to seek exposure to get better at your job. Without that experience, everything is theory.*" His point underscores a central benefit of Cyber Yankee: well-developed exercises provide both craft knowledge—familiarity with DSCA and UCG processes—and the practical judgment that comes only from repeated exposure to realistic, cross-sector coordination. This experiential learning is especially critical as ARCYBER expands its operational technology (OT) defense capabilities, an area that increasingly defines national-level cyber response. Col. McNatt also emphasized the broader implications for force readiness: "*There is value in [active duty] participation, but there would be even greater value if the rest of the regions in this Union did something at the same level of sophistication (and ideally, calibrated to the [Cyber Yankee] standard).*" His comments highlight Cyber Yankee's role not only as a regional exercise, but as a benchmark for the level of complexity, realism, and interagency integration needed across the country.

LOOKING AHEAD: THE FUTURE OF CYBER YANKEE

As cyber threats evolve, so will Cyber Yankee. According to Col. (Ret.) Woody Groton, who led Cyber Yankee 25's UCG training and exercising, there are three future areas within the exercise that could be war-gamed more specifically: (1) the usability of technology systems during a cyber crisis, (2) communications and operations between different agencies, and (3) state-specific cyber response plans and exercises.

In Cyber Yankee 2025, the Army Cyber Institute provided two workshops to address a whole-of-government response that is central to the UCG. The first workshop used threatcasting (Johnson and Vanatta 2017)—strategic foresight methodology used to envision and systematically plan for potential threats (typically 10 years in the future)— to imagine future scenarios in which the UCG might need to respond. These science-fact–based fictional scenarios emphasized how human factors shape incident communication. The second workshop demonstrated an experimental cyber tabletop (CTT), inspired by role-playing game mechanics, developed at the University of Indiana. This CTT used a simplified scenario involving a fictitious military installation affected by cyber disruptions in a nearby city's traffic and emergency systems, assigning participants unfamiliar roles to highlight interdependencies and the complexity of coordinated response.

Future Cyber Yankee exercises are expected to include AI-driven cyberattacks, quantum computing vulnerabilities, supply chain compromises, and deepfake-enabled social engineering. The exercise is also likely to expand its focus on resilience and recovery, ensuring that systems can not only withstand attacks but also bounce back quickly.

Technologies such as Hive IQ-a software that automates malware analysis, manages collaboration across teams of the cyber response, and keeps decision makers informed-could be tested to see how well they work during specific scenarios. In 2025, an experimental AI-enabled network sensor virtual machine was installed on the Cyber Yankee network to mirror traffic and conduct further analysis. The red team was able to test cyber effects before presenting them to blue teams (Cashman et al. 2025). These examples could include how Operational Technology operators respond to crisis and demonstrate how Cyber Yankee can serve as a testbed for AI technologies.

Communication and response across USCYBERCOM, the military, critical infrastructure entities, state governments, and the National Guard during a cyber incident could also be practiced in a more detailed manner, ensuring incident response occurs smoothly and quickly. This is a general challenge for cyber incident response. "*We need a platform for both communication and operational coordination between all parties involved in cyber incident response and right now we do not have it,*" Maj. Gen. Williams said.

Finally, specialized state-specific tabletop exercises supported by academics and legal and policy experts could help improve the training so that an actual incident response runs

more smoothly. Brig. Gen. Rummel recommended that states that do not currently have Cyber Protection Teams (CPTs), such as Alaska, would benefit from starting them. Formally established CPTs, such as those assigned to the 91st Cyber Brigade (Virginia), or Guardsmen assigned to work with state CIO/CISOs are at the frontlines of state cybersecurity protection. Every state is varied in its cybersecurity risk profile, but all states have experienced, and will continue to experience, cyber-enabled attacks and disruptions to normal operations that could be partially mitigated through prior exercising of the incident response process.

LESSONS FROM PRACTICE: CYBER YANKEE'S IMPACT ON REAL-WORLD INCIDENT RESPONSE

The Guard's Response to the UVM Medical Center Attack

The response of the National Guard to the 2020 UVM Medical Center ransomware attack illustrates how Cyber Yankee's practices translate into real-world incident response. It was based directly on the skills, relationships, and coordination patterns strengthened through the exercise. The Cyber Yankee's structure—bringing together National Guard cyber teams, state agencies, federal partners, and operators of critical infrastructure—mirrors the multi-stakeholder environment that emerged during the UVM response. Through repeated exposure to complex, multi-vector attacks and sustained coordination with private-sector operators, Guard personnel had already rehearsed the types of decisions required in large-scale recovery efforts. These included restoring compromised endpoints, reestablishing trust across hybrid IT–OT systems, and integrating with external cybersecurity contractors. During the UVM Medical Center incident, these capabilities translated into effective support as Guard teams helped review and rebuild affected systems, restore functionality in phases, and assist the hospital in reestablishing critical clinical and administrative services during the following weeks. The exercise's emphasis on UCG-style coordination also meant that Guard teams were familiar with rapid information-sharing protocols, escalation pathways, and cross-organizational communication, all of which proved essential during the hospital's prolonged recovery. In this way, the operational readiness built through Cyber Yankee materially supported the Guard's ability to assist effectively in Vermont's real-world crisis.

After the hospital networks were restored, the Vermont National Guard conducted several after-action reviews to capture lessons. The most important finding was that pre-existing relationships with UVM leadership significantly sped up response time and allowed National Guard volunteers to be available to the hospital system within 24 hours. However, not everything was as straightforward and quick as an incident response rehearsed in exercises. According to Col. (ret.) Chris Evans, who was then the unit's CIO, and dual-hatted as the state J6, the way the UVM IT staff used the Guardsmen was not the way they trained during Cyber Shield and Cyber Yankee. Instead, the team was assigned tasks according to individual skills,

rather than operating as a unified group. As a result, the Vermont Guard refined their state emergency response procedures to create different "packages" of assistance, formalizing the process to provide a tailored team or individual skill sets. They also updated their mobilization procedures to allow for flexible response packages.

Two other key lessons from the UVM incident have shaped the design of the UCG portion of Cyber Yankee. Col. Evans led the UCG training for Cyber Yankee 21, the year following UVM and noted that his experiences reinforced the move towards a civilian-led UCG model. This emphasized his observations that the military was not (and should not be) in the lead for a cyber incident response on state infrastructure, which was "*challenging for type-A people in the military,*" Evans said. "*It was in Cyber Yankee 22 when they actually started getting more civilian agencies and federal agencies... it's really hard. You do these exercises and it's so hard to have the military in the background... We're supposed to be there in a support role and you know, that's really, really hard.*" In Cyber Yankee 25, over half of the UCG attendees were civilians from federal and state agencies and regional utilities.

Scaling Cyber Yankee Insights: Recommendations for States and Regions

Cyber Yankee's evolution and successes offer several practical recommendations for other regions and for active-duty organizations seeking to enhance their cyber incident response capabilities. These recommendations translate Cyber Yankee's regionally tested practices into actionable guidance for other states, regions, and active-duty partners.

Proactively build relationships with critical infrastructure operators. Seek out, meet, and invite the leadership and cyber technicians who provide critical infrastructure services (especially power, water, gas/oil, and medical) to military installations to join conversations and exercises. Often, these have local or county offices with the responsibility to service bases. These partners can be incorporated into short, scenario-based cyber tabletop exercises (from one hour to half a day) or invited as full participants in large-scale training events. Military teams should also train utilities on the federal Request for Support (RFS) process.

Use National Guard exercises to practice real-world coordination mechanisms. Exercises should explicitly rehearse the initiation and processing of utility RFSs and the use of the Cyber 9-Line to communicate with U.S. Cyber Command. States should refine timelines for standing up a cyber UCG and share their best practices with sector-based Information Sharing and Analysis Centers (ISACs). Even small utilities—such as a one-person municipal water IT team—should understand how to initiate an RFS and who their state UCG coordinator is.

Adopt and adapt the Blue Team–Orange Team construct. When designing regional, state, or city-wide cyber exercises, replicate the Blue team / Orange team structure that pairs defensive cyber teams with utility and industry operators on their own networks. This construct teaches

cyber protection teams and incident responders about the unique operational constraints that private utilities face within their own networks.

Develop scenarios that stress Operational Technology (OT) environments. Create scenarios that force incident responders to protect OT systems. Provide training and education opportunities to Guardsmen prior to or as part of an annual exercise, such as industrial control systems and OT courses from SANS. Other scenarios might involve exercising plans for a state's defensive continuity of operations plan (COOP) or how a statewide cybersecurity service provider might integrate multi-sector challenges with OT systems.

Integrate OT Knowledge, Skills, and Abilities (KSAs) into the Joint Qualification Records (JQRs). Include OT-specific knowledge, skills, and abilities (KSAs) in appropriate Joint Qualification Records (JQRs) for cyber protection teams assigned to the National Guard. This ensures that the KSAs are aligned with the legal authorities and mission expectations to respond to a domestic cyber incident.

Build flexible mobilization and response structures. Create procedures that allow flexible mobilization and response options. If a state normally trains only as a single defensive element, or in collaboration with another state during exercises, consider how to also exercise individual mobilization requests for specialized security skills.

CONCLUSION

Despite the efforts of the National Guard, state cybersecurity teams, and even the FBI and U.S. Cyber Command, adversaries of the U.S. will still find targets to hack and exploit. This makes it all the more important for all regional National Guard entities, and the government agencies and the utilities they work with, to continue to practice close cooperation and train to defend against cyber threats to critical infrastructure. The mandate for a UCG to protect the nation's safety and security, and the regional National Guard response groups such as Cyber Yankee, has never been more urgent.

The evidence of Cyber Yankee's long-term impact will be in its replicability beyond New England and in its continued use to prepare industry, utilities, and government and state entities to respond quickly and effectively to cyber emergencies and future threats. The expertise gained through deliberate and repeated coordination, especially Cyber Yankee's unique use of the Orange Team and the exercise goals for the UCG, is achievable by active duty and the National Guard alike. Simulating real-world threats and fostering collaboration across sectors, it ensures that the nation is prepared to defend its most vital systems.

ABOUT THE AUTHORS

Dr. Sarah Lohmann teaches cybersecurity policy and emerging technology ethics at the University of Washington. She is a coauthor of the books The Weaponization of AI: The Next Stage of Terrorism and Warfare (2025), Emerging Technologies and Terrorism: An American Perspective (2024), and the editor and coauthor of the books What Ukraine Taught NATO about Hybrid Warfare (2022) and Countering Terrorism on Tomorrow's Battlefield (2022).

Lt. Col. Jason C. Brown is a research scientist and assistant professor at the Army Cyber Institute at West Point. He teaches risk management, organizational security, and systems-based decision making. As a futurist, he studies emerging threats, technological and social trends, and responses to those threats. He also leads a research team investigating critical infrastructure resilience on behalf of Army and other defense stakeholders. LTC Brown has worked within the intelligence, information operations, and cyber career fields. He has authored technical reports on the future of extremism, information warfare, cyber enabled financial crimes, microtargeting, and Chinese soft power.

ACKNOWLEDGMENTS

The authors thank the National Guard leaders, cyber operators, and emergency management professionals who shared their time and insights, as well as the Cyber Yankee organizers and participants whose collaboration and expertise made this analysis possible. The authors also extend their sincere appreciation to Prof. Carine Lallemand for the expertise and thoughtful feedback that greatly enriched the quality of this work.

REFERENCES

ACI (Army Cyber Institute). 2025. *Jack Voltaic Research Reports Series.* https://cyber.army.mil/Our-Work/Jack-Voltaic/Research-Reports/.

Air Land Sea Application Center. 2021. *Multi-Service Tactics, Techniques, and Procedures for Defense Support of Civil Authorities (DSCA).* Technical report. February 2021. https://www.alssa.mil/Portals/9/Documents/mttps/dsca_2021.pdf.

Barry, Ellen, and Nicole Perlroth. 2020. "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack." *The New York Times* (November 26, 2020). https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

Bedard, David. 2025. *Alaska National Guard Exercises Disaster Response During Vigilant Guard.* National Guard News, April 4, 2025. https://www.nationalguard.mil/News/Article-View/Article/4145804/alaska-national-guard-exercises-disaster-response-during-vigilant-guard/.

Bodker, Erica. 2025. "Locked Shields 2025: West Virginia National Guard Hosts NATO's Largest Live-Fire Cyber Resilience Exercises in the World," May 23, 2025. https://www.wv.ng.mil/News/Article/4195018/locked-shields-2025-wva-guard-hosts-natos-largest-live-fire-cyber-resilience-ex/.

Brajdić, Ivona, Ivan Kovačević, and Stjepan Groš. 2021. "Review of National and International Cybersecurity Exercises Conducted in 2019." In *International Conference on Cyber Warfare and Security,* 28–36. Reading, UK: Academic Conferences International Limited. https://doi.org/10.34190/IWS.21.034.

Cashman, William, Chasen Milner, Michael Houle, Michael Jones, Hayden Jananthan, Jeremy Kepner, Peter Michaleas, and Alex Pentland. 2025. *Accelerating AI Development with Cyber Arenas.* arXiv preprint. https://doi.org/10.48550/arXiv.2509.08200.

CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). *Locked Shields.* https://ccdcoe.org/exercises/locked-shields/.

CISA (Cybersecurity and Infrastructure Security Agency). 2025. *The National Cyber Incident Response Plan (NCIRP).* https://www.cisa.gov/national-cyber-incident-response-plan-ncirp.

CISA (Cybersecurity and Infrastructure Security Agency). n.d. *Emergency Services Sector.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructuresectors/emergency-services-sector.

Dewar, Robert S. 2018. *Cyber Security and Cyber Defense Exercises.* Cyber Defense Report. Center for Security Studies (CSS), ETH Zürich, September.

DoD (Department of Defense). 2023. *DoD Instruction 8530.03, Cyber Incident Response,* August 9, 2023. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853003p.PDF?ver=XPp9bgbmddCqR7gokbskWg%3d%3d.

Edinger, Julia. 2025. *Idaho Takes a Hands-On Approach to State Cybersecurity,* August 7, 2025. https://www.govtech.com/security/idaho-takes-a-hands-on-approach-to-state-cybersecurity.

Eisenbrandt, Jadyn. 2025. *Guard Soldiers Train with Civilian Experts in Cyber Discovery Exercise.* National Guard News, June 23, 2025. https://www.nationalguard.mil/News/Article-View/Article/4223483/guard-soldiers-train-with-civilian-experts-in-cyber-discovery-exercise/.

Estrada, Clarissa. 2022. *VNG's 91st Cyber Brigade Makes History at Cyber Shield.* Virginia National Guard News, June 29, 2022. https://va.ng.mil/News/Article/3078575/vngs-91st-cyber-brigade-makes-history-at-cyber-shield/.

Executive Office of the President. 2013. *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience,* February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Executive Office of the President. 2016. *Presidential Policy Directive 41 – United States Cyber Incident Coordination,* July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-unitedstates-cyber-incident.

Granåsen, Magdalena, and Dennis Andersson. 2016. "Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study." *Cognition, Technology and Work* 18 (1): 121–143. https://doi.org/10.1007/s10111-015-0350-2.

Hynes, Kevin. 2025. *Cyber Tatanka Gives Network Defense Specialists Opportunity to Refine Their Skills in Safe yet Realistic Virtual Environment,* July 7, 2025. https://www.dvidshub.net/news/542196/cyber-tatanka-gives-network-defense-specialists-opportunity-refine-their-skills-safe-yet-realistic-virtual-environment.

Ihme, Kelly R. M., Patrick O'Brien Boling, Michael Zimmerman, and Timothy G. McCormick. 2025. "Who Is in Charge of Cyber Incidence Response in the Homeland?" *Parameters* 55 (3). https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3359&context=parameters.

Jeney, Carson. 2025. "Balikatan 25: Strengthening Cyber Security Ties with the Philippines," May 8, 2025. https://www.pacom.mil/Media/NEWS/News-Article-View/Article/4179489/balikatan-25-strengthening-cyber-security-ties-with-the-philippines/.

Johnson, Amanda H. 2022. "Joint Task Force Cyber Hosts Cyber Dawn 2022," July 27, 2022. https://grizzly.shorthandstories.com/california-national-guard-hosts-cybersecurity-exercise/.

Johnson, Brian David, and Natalie Vanatta. 2017. "What the Heck Is Threatcasting?" *Future Tense,* https://threatcasting.asu.edu/sites/g/files/litvpz1036/files/2019-11/what-the-heck-is-threatcasting.pdf.

Johnson, Rivers. 2012. "Cyber Guard Exercise Focuses on Defensive Cyberspace Operations," August 17, 2012. https://www.army.mil/article/85786/cyber_guard_exercise_focuses_on_defensive_cyberspace_operations.

Leffler, Stephen. 2023. *Written testimony to the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, and the Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs,* September 27, 2023. https://oversight.house.gov/wp-content/uploads/2023/09/Steve-Leffler-written-testimony.pdf.

Loeffler, David. 2025. *Cyber Dawn 2025.* https://grizzly.shorthandstories.com/cyber-dawn-2025/.

Maennel, Karin, Rain Ottis, and Oliver Maennel. 2017. "Improving and Measuring Learning Effectiveness at Cyber Defense Exercises." In *Secure IT Systems,* edited by Helger Lipmaa, Aikaterini Mitrokotsa, and Raimundas Matulevičius, vol. 10674. Lecture Notes in Computer Science. Cham: Springer. https://doi.org/10.1007/978-3-319-70290-2_8.

Mag, Stephen. 2025. *What Is the Cybersecurity Color Wheel? Roles & Teams Explained.* Cybersics, July 24, 2025. https://www.cybersics.com/blog/cybersecurity-color-wheel/.

Martin, Will. 2025. "Cyber Shield 2025 Trains Guardsmen for Borderless Threats," July 22, 2025. https://reservenationalguard.com/unit-training/cyber-shield-2025-trains-guardsmen-for-borderless-threats/.

Pomerleau, Mark. 2022. "Cyber Yankee Exercise Helps National Guard Mature Partnership with Cyber Command," June 30, 2022. https://defensescoop.com/2022/06/30/cyber-yankee-exercise-helps-national-guard-mature-partnership-with-cyber-command/.

Puryear, Cotton. 2023. "Cyber Fortress 2.0 Tests Virginia's Cyber Response Plan," August 10, 2023. https://va.ng.mil/News/Article/3501226/cyber-fortress-20-tests-virginias-cyber-response-plan/.

Roudabush, Joe. 2025. "Cyber Shield 2025: A Joint Force Exercise," June 10, 2025. https://www.dvidshub.net/news/501314/cyber-shield-2025-joint-force-exercise.

Scott, Mark. 2025. *Guam Guard Participates in Balikatan 2025 Cyber Defense Exercise.* National Guard News, May 28, 2025. https://www.nationalguard.mil/News/Article-View/Article/4198937/guam-guard-participates-in-balikatan-2025-cyber-defense-exercise/.

Smeets, Max. 2022. "The Role of Military Cyber Exercises: A Case Study of Locked Shields." In *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon),* 700:9–25. https://doi.org/10.23919/CyCon55549.2022.9811018.

StateDefenseForce.com. 2025. *Cyber Fortress 25 Unites Virginia Defense Force, National Guard, Marines, and NATO Partners Against Cyber Threats.* StateDefenseForce.com, August 18, 2025. https://statedefenseforce.com/2025/08/18/cyber-fortress-25-unites-virginia-defense-force-national-guard-marines-and-nato-partners-against-cyber-threats/.

Tarkelly, Hannah. 2025. *Cyber Shield 2025 – Coding Collaboration on a Global Scale.* DVIDS, June 12, 2025. https://www.dvidshub.net/news/500415/cyber-shield-2025-coding-collaboration-global-scale.

U.S. Code Title 10: Armed Forces. 1956a. https://uscode.house.gov/view.xhtml?path=/prelim@title10&edition=prelim.

U.S. Code Title 32: National Guard. 1956b. https://uscode.house.gov/view.xhtml?path=/prelim@title32&edition=prelim.

U.S. Department of War. 2017. *Allies, Partners Observe Cyber Guard Exercise.* U.S. Department of War News, July 5, 2017. https://www.war.gov/News/News-Stories/Article/Article/1238082/allies-partners-observe-cyber-guard-exercise/.

United States Congress. 2014. *National Cybersecurity Protection Act of 2014,* Public Law 113-282. https://www.congress.gov/bill/113th-congress/senate-bill/2519/text.

Received 7 August 2025; Revised 27 September 2025; Accepted 19 November 2025