THE CYBER DEFENSE REVIEW
In press, 14 pages
https://doi.org/10.55682/cdr/t8xv-pdqx

PROFESSIONAL COMMENTARY

From Workforce to Warfighting: Why State Cyber Reserve Forces Fail

Joshua Copeland*

Louisiana State Guard, Jackson Barracks, LA, USA
Tulane University, New Orleans, LA, USA

Cyber reserve forces are increasingly proposed as a solution to the national cybersecurity workforce gap, particularly at the state level, where critical infrastructure risk is most acute. However, operational experience suggests that current models fall short of delivering consistent, actionable capability. This paper examines the gap between the theoretical promise of cyber reserve forces in the United States and their effective implementation at the state level. Drawing on operational experience, structured exercises, and documented state programs, it identifies three primary failure points: capability without authority, inclusion without operational integration, and detection without execution. The article then examines four State Defense Force (SDF) cyber units—the Louisiana State Guard Cyber Reserve Team, the Texas State Guard Cyber Security Unit, the Virginia Defense Force 31st Cyber Battalion, and the Maryland Defense Force 256th Cyber Defense Unit—as illustrative examples of emerging approaches that are beginning to address the structural gaps that constrain state cyber reserve programs more broadly. The paper concludes by proposing a future-oriented framework, grounded in Emergency Management Assistance Compact (EMAC)-enabled regional scaling, governance integrity, and a three-level maturity model, to help guide the evolution of cyber reserve units into more effective components of national cyber defense.

Keywords: cyber reserve forces, State Defense Forces, incident command, cyber incident response, emergency management, cyber defense

* Corresponding author: jcopeland@tulane.edu

INTRODUCTION

The concept of a cyber reserve force is simple: to leverage part-time personnel with industry experience to augment cyber capability during steady-state operations and incident response. However, implementing this concept presents significant challenges.

In this commentary, "cyber reserve forces" refers to state-level reserve cyber capabilities organized through civilian cyber corps programs, State Defense Forces (SDFs), or hybrid state response structures that draw on part-time or volunteer expertise. Cyber-attacks on state and local systems continue to increase in frequency and impact, particularly across critical infrastructure sectors that function with limited resources and uneven defensive maturity. At the same time, the cybersecurity workforce gap persists, with public-sector organizations facing structural challenges in recruiting and retaining skilled personnel. In response to these challenges, states have begun establishing civilian cyber corps programs and State Defense Force cyber units, drawing on private-sector expertise to expand capability without the cost of full-time staffing. Yet implementation has produced uneven results.

The cyber reserve model is frequently framed as a workforce solution. This framing is incomplete. The limiting factor is not personnel, but the ability to translate personnel into action. Operational and training environments reveal a consistent pattern: cyber reserve teams often know what needs to be done but lack the organizational mechanisms to act swiftly. This commentary examines the gap between technical detection and operational impact and identifies three recurring failure points: capability without authority, inclusion without operational integration, and detection without execution. Addressing these organizational barriers, not simply expanding the workforce, is essential to making cyber reserve forces successful.

The following scenario is drawn from operational exercise experience and illustrates a pattern observed across multiple multi-agency environments. Identifying details have been generalized.

Operational Vignette: Detection Without Action

During a multi-agency cyber exercise simulating a coordinated attack on regional infrastructure, a cyber response team identified multiple externally exposed services during the initial phase of operations. Within minutes, the team had identified vulnerable endpoints, validated exposure paths, assessed potential impact, and prepared a prioritized remediation list. The technical picture was clear. The organizational response was not. Remediation required coordination across system owners, network administrators, procurement channels, and incident command leadership. No predefined authority existed. No escalation pathway had been exercised in advance. Questions accumulated at every level: Who owns this system? Does this require legal review? Who has final approval authority? Exposure persisted throughout the exercise; not because the technical problem was unsolvable, but because the organizational infrastructure required to authorize action had not been established beforehand. The limiting factor was not detection capability. It was the absence of decision authority and execution pathways. This pattern is not isolated. It represents a structural failure mode, not an anomaly.

WHERE THE CYBER RESERVE MODEL BREAKS

Capability Without Authority

Cyber reserve models often succeed at assembling technical capability before they solve the harder governance question: who has the authority to activate, direct, integrate, and sustain that capability during an incident? The result is a capability-to-action gap. Prior federal review of cyber incident civil-support planning similarly concluded that effective response depends on clearly defined roles, responsibilities, expectations, coordination mechanisms, and training requirements (GAO 2017). A state may have skilled cyber personnel, experienced volunteers, or uniformed reserve members available, but that capability remains latent if it is unclear when they may be activated, who may task them, what systems they may touch, and how their work integrates into the broader incident response structure.

This failure is not simply administrative. It is operational. Cyber incidents unfold under time pressure, legal uncertainty, incomplete information, and competing organizational interests. In that environment, unclear authority produces delay. Leaders hesitate to deploy personnel. Technical teams wait for permission. Agencies dispute ownership. Local entities are unsure whether outside cyber support is advisory, operational, investigative, or command-directed. Meanwhile, the incident continues to spread. The practical limitation is not the absence of cyber skill but the absence of a governance framework that converts cyber skill into lawful action.

The first form of authority failure occurs within government. Cyber reserve personnel may exist on paper, yet their operational role remains unclear if activation triggers, command relationships, mission assignment processes, and reporting structures are not defined in advance. A cyber reserve that is not integrated into emergency management, military support to civil authorities, or incident command processes risks becoming an informal talent pool rather than a deployable public capability. During an incident, that ambiguity matters. If cyber personnel do not know whether they report through the State Guard, the state emergency management agency, the state Chief Information Security Officer (CISO), the adjutant general, or an incident commander, technical capability can be slowed by institutional uncertainty.

The second form of authority failure occurs outside government, where many consequential cyber incidents affect systems the state does not own. School districts, municipalities, hospitals, utilities, election vendors, cloud platforms, and private critical infrastructure operators may all be involved in incidents with public consequences. In these environments, the question is not only whether a cyber reserve possesses expertise, but whether it has lawful permission to engage, receive sensitive information, access systems, support containment, coordinate with vendors, preserve evidence, and assist recovery without exceeding its authority. Cyber reserves operate most effectively when these boundaries are established before a crisis through statute, policy, memoranda of understanding, mutual aid processes, or formal request mechanisms.

Ohio illustrates a model that places cyber reserve capability within a clearly defined public authority structure. Ohio law directs the governor to organize and maintain civilian cybersecurity reserve forces capable of educating and protecting state, county, and local government entities, critical infrastructure, election systems, businesses, and citizens from cyberattacks (Ohio Revised Code, § 5922.01). The

same chapter authorizes the governor, as commander-in-chief of the Ohio organized militia, to order Ohio Cyber Reserve (OhCR) individuals or units to state active duty to protect state, county, and local government entities and critical infrastructure, including election systems, and, upon request, to protect a business or citizen (Ohio Revised Code, § 5922.08). That framework matters because it links cyber capability to activation authority, public mission scope, and state command responsibility.

Indiana demonstrates a different approach by emphasizing cyber capability developed through the National Guard and dedicated training infrastructure. The Indiana National Guard describes the Muscatatuck Cyber Program as a cyber-physical training environment that supports research, development, testing, training, and evaluation across physical, logical, and cyber-persona layers. Indiana also activated the 127th Cyber Protection Battalion to provide mission command for National Guard cyber elements (Wenck 2020). While this model shows substantial cyber capability, it also highlights the importance of distinguishing military cyber readiness, training infrastructure, and state-level civilian incident response authority.

Michigan provides another useful example by moving beyond informal volunteerism toward a statutory civilian cyber response framework. The Michigan Cyber Civilian Corps (MiC3) Act authorizes trained volunteers to support organizations to respond to cybersecurity incidents (Michigan Legislature 2017). The Act also authorizes the department, at its discretion, to initiate deployment of Michigan Cyber Civilian Corps volunteers after a cybersecurity incident and permits a client to request deployment of volunteers after such an incident. The National Governors Association further notes that Michigan's codification of MiC3 into law loosened prior activation constraints and allowed the state to begin using volunteers more effectively (National Governors Association 2022). Although statutory authority alone does not eliminate every operational challenge, Michigan demonstrates how authority can be deliberately designed around volunteer cyber capability, client requests, state coordination, liability, and state response governance.

This authority problem is not new. Early computer emergency response was built around coordination rather than command. As Scherlis, Squires, and Pethia (1991) observed in their early account of the CERT Coordination Center, the original model emphasized community coordination and information sharing, not delegated operational authority. That history clarifies the design problem for modern state cyber reserves: coordination may improve situational awareness, but it does not by itself authorize access, direct action, or operational support. If cyber reserve programs are to function as more than advisory networks, authority must be built into the model before an incident begins.

These examples show that the central limitation is not a shortage of cyber expertise but the absence of a governing structure that converts expertise into authorized action. A cyber reserve that cannot be activated clearly, assigned lawfully, directed operationally, or integrated into incident command remains a latent capability rather than a deployable asset. The corrective task is thus not simply to recruit more cyber professionals, but to design authority into the reserve model from the outset.

Inclusion Without Operational Integration

The second failure point is inclusion without operational integration. Cyber reserve units may appear on organizational charts, participate in exercises, and hold formal designations within state emergency management structures, but inclusion is not the same as integration. A unit is *included* when it is

invited to brief, advise, or provide technical input. It is *operationally integrated* when it has a defined role within the command structure, a path to influence response priorities, and the ability to shape or initiate actions within approved authority tiers.

In practice, cyber units often brief leadership, provide situational awareness reports, and produce findings and recommendations. But they do not drive decisions, shape operational timelines, or execute actions. They serve a specialized advisory function. They are consulted when leadership wants technical input and sidelined when decisions are made. By the time recommendations pass through advisory channels, the operational window for maximum impact has closed. This is not an individual leadership failure. If cyber units are given advisory roles instead of operational ones, they function only as advisors, no matter the intent or competence of the people.

Operational integration also depends on trust and procedural alignment. Legal authority and command placement matter, but they are insufficient if full-time staff, emergency managers, and reserve personnel do not understand one another's roles before an incident. The two dynamics below help explain why formal inclusion so often fails to become operational integration.

Cultural Friction and Role Deconfliction. Legal and command barriers often paralyze cyber reserve operations. Human-in-the-loop friction is equally challenging. Successful integration depends on overcoming a trust deficit that can exist between full-time state personnel and 'outsider' reserve experts drawn from the private sector. State employees may perceive reservists as threats to their professional domain or as disruptors to standard workflows. Conversely, the dual identity of reservists—as private-sector experts serving within a State Guard or an emergency management agency—often leads to cultural clashes. A private-sector threat hunter accustomed to independent decision-making and flat structures may find it difficult to adapt to a command hierarchy focused on process compliance and approval chains. Without a culture of mutual trust and clear role deconfliction, even legally empowered reserve units may struggle with morale, retention, and operational effectiveness. Programs that invest in pre-incident joint exercises can provide value beyond technical training by building the relationships and procedural familiarity needed during crisis response (National Governors Association 2022). Trust built in peacetime is the currency spent in crisis.

ICS/NIMS Misalignment. This integration problem becomes most visible when cyber response is mapped onto traditional emergency management structures. The National Incident Management System (NIMS) and Incident Command System (ICS) provide essential coordination frameworks for multi-agency response, but they require adaptation for cyber incidents. NIMS remains the de facto standard for multi-agency incident response in the United States; however, it was built around incidents with clearer geographic boundaries, more visible chains of causation, and decision cycles that generally move at human coordination speed (Federal Emergency Management Agency 2017). Cyber incidents move differently. At the national level, the National Cyber Incident Response Plan likewise emphasizes predefined roles and coordinated responsibilities across federal, state, local, territorial, and private-sector participants during significant cyber incidents (CISA 2016).

A ransomware payload can encrypt thousands of files in seconds. A command-and-control channel can enable rapid data exfiltration before a traditional Incident Action Plan is fully developed. Ownership is also less obvious than in physical incidents. Affected systems may span public agencies,

private infrastructure operators, cloud providers, vendors, and third-party service providers. Determining who owns the system, who can authorize access, and who can approve remediation may itself consume the critical response window.

Cyber response also depends on technical judgments that many incident commanders are not positioned to make alone. Decisions about isolating systems, blocking traffic, disabling accounts, engaging vendors, or preserving forensic evidence require specialized expertise and predefined decision thresholds. If those decisions must be routed through traditional command channels without an embedded cyber role, the result is delay at the exact moment speed matters most. Prior research on cyber incident response and ICS adoption similarly finds that ICS improves outcomes only when cyber personnel are assigned roles with genuine operational authority, and that terminology gaps between emergency managers and cyber practitioners remain a persistent barrier (Hanson 2021).

The problem is not that ICS is wrong for cyber, but cyber is often added to ICS as an advisory function rather than embedded as an operational capability. Colorado Department of Transportation (2018) ransomware incident illustrates both the strengths and limitations of this approach: ICS and Unified Command helped bring structure to the response, but only after initial disorganization consumed valuable time. For cyber reserve forces to be effective, cyber personnel must have defined roles within the command structure, common terminology with emergency managers, and pre-approved authority tiers that allow technical findings to become operational decisions. Without that adaptation, ICS can coordinate the response while still slowing the action the response requires.

Detection Without Execution

The third failure point is detection without execution. Cyber reserve programs often improve visibility before improving an organization's ability to act. The result is a dangerous imbalance: more findings, more alerts, and more technical reports do not automatically produce better security outcomes. Without triage protocols, severity thresholds, escalation pathways, and pre-authorized response options, increased detection can overwhelm decision-makers rather than accelerate response.

Modern cybersecurity tools generate thousands of alerts each day. Most alerts are false positives, low-severity findings, or duplicates. In cyber reserve units, part-time staff, limited technical leadership, and scarce response resources make this volume overwhelming. When everything seems urgent, nothing truly is. Leaders without technical backgrounds cannot tell a critical alert from a routine one. Research on SOC alert fatigue shows that excessive alert volume, false positives, duplicate findings, and weak prioritization can reduce response effectiveness and contribute to analyst fatigue (Tariq et al. 2025). This fatigue grows over time and leads to alert suppression, creating real blind spots. Cyber reserve programs cannot rely solely on detection tools; they must also invest in triage protocols, severity thresholds, and leadership training in technical risk communication. Otherwise, added detection ability only deepens the problem.

The same issue arises when organizations generate findings faster than they can prioritize or remediate them. Audits, assessments, and scans add value only when they feed a defined execution pathway; otherwise, they create the appearance of progress while expanding the backlog of unacted-upon risk.

DESIGNING A FUNCTIONAL CYBER RESERVE FORCE

The failure points identified share a common root: cyber reserve forces are resourced as capabilities but structured as support functions. Closing this gap requires coordinated improvements across three interdependent dimensions: authority design, command integration, and execution capability.

Authority Design

Authority design translates cyber reserve capability into lawful, deployable, and operationally integrated public capacity. If capability without authority creates delay, ambiguity, and underuse, authority design provides the corrective framework. Cyber reserve programs should be designed as operational capabilities with clear activation rules, command relationships, mission boundaries, liability protections, and integration pathways.

First, states should define activation authority before an incident occurs. A cyber reserve model should identify who may activate the force, under what conditions, for what categories of incidents, and through what request process. Activation should not depend on improvised relationships or informal trust during a crisis. Whether authority rests with the governor, adjutant general, state emergency management director, state CISO, or another designated official, the trigger must be clear enough to support timely action and narrow enough to prevent mission creep. Civilian cyber corps programs therefore require legal design before operational design can succeed. Razeeq (2024) argues that effective state frameworks should specify activation authority, volunteer qualifications, beneficiary eligibility, liability protection, confidentiality obligations, permissible services, reimbursement mechanisms, and rulemaking authority. Those statutory choices determine whether a cyber corps can respond quickly or becomes constrained by its own enabling language, particularly when assistance is limited to government entities or when every deployment requires high-level activation.

Second, cyber reserve programs should define command and control relationships. Cyber incidents often involve technical responders, legal counsel, public information officers, emergency managers, elected officials, law enforcement, vendors, and affected system owners. Without a defined command structure, a cyber reserve can become another advisory voice in an already crowded incident. Authority design should specify where cyber reserve personnel fit within incident management structures, how they receive mission assignments, who validates priorities, and how technical findings are elevated to decision-makers.

Third, cyber reserve missions should be bounded in advance. A mature model should distinguish assessment, advisory support, incident triage, containment assistance, recovery planning, communications support, documentation, and coordination with vendors or other agencies. These missions should be written clearly enough to prevent both overreach and underuse. Cyber reserve personnel should not be assumed to have unrestricted authority over public or private systems. Their role should be tied to lawful request, mission assignment, and the consent or authority of the system owner.

Fourth, authority design should address legal boundaries, liability, privacy, and evidence handling. Cyber response activity can expose sensitive data, regulated information, criminal evidence, proprietary systems, and politically sensitive operational failures. A reserve model that ignores those realities

will struggle to gain trust from local governments, private entities, and critical infrastructure partners. Rules of engagement, data handling requirements, nondisclosure obligations, indemnification, reporting requirements, and documentation standards should be established before deployment.

Fifth, cyber reserve authority should account for public-private infrastructure realities. Many incidents with statewide consequences occur in environments owned or operated outside direct state control. Cyber reserve models should therefore include pre-incident agreements, mutual aid mechanisms, memoranda of understanding, request procedures, and defined handoffs with vendors, managed service providers, insurers, law enforcement, and emergency management agencies. The goal is not to give the state blanket control over private systems, but to create a lawful pathway for assistance when affected entities request or require support.

Finally, authority design should align cyber reserve operations with existing emergency management doctrine rather than creating a separate cyber-only response universe. Cyber incidents increasingly create operational consequences for public safety, continuity of government, health care, education, elections, and critical infrastructure. Integrating cyber reserve activity into ICS/NIMS-compatible processes allows cyber expertise to support broader incident objectives, resource coordination, public messaging, and recovery operations. This is especially important when a cyber incident occurs alongside a natural disaster, infrastructure failure, or public safety emergency.

The purpose of authority design is not bureaucracy for its own sake. It is to make action possible. Clear authority allows cyber reserve personnel to move from informal expertise to assigned mission, from volunteer interest to operational support, and from technical capability to public resilience.

Command Integration

Functional integration requires cyber personnel in operational roles, not advisory ones. An advisory role means that they are consulted; their input informs decisions made by others. A functional role means cyber personnel make or directly shape operational decisions within their area of expertise. In a time-sensitive domain like cybersecurity, the difference between these roles is measured in hours, and in incidents where damage accumulates by the minute, hours are not recoverable.

A practical model assigns a Cyber Operations Coordinator to the Operations Section with direct reporting to Incident Command and explicit authority to recommend, initiate, and direct cyber response actions within pre-approved tiers. The National Governors Association's review of Michigan, Wisconsin, and Ohio programs explicitly recommends "merging Incident Command System principles and terminology with the state's cybersecurity tactical operations to lessen confusion and facilitate response and recovery efforts," and notes this integration must be built into organizational design before an incident, not improvised during one (National Governors Association 2022).

The Virginia Defense Force (VDF)'s 31st Cyber Battalion represents the most mature SDF model of this principle in practice. Formally integrated into the Virginia Army National Guard's 91st Cyber Brigade—the Army National Guard's first and only dedicated cyber brigade, which provides training and response readiness oversight for cyber units across 30 states and territories (Puryear 2017)—the 31st participated as Blue Team enclave defenders in *Cyber Fortress 25*, contributed to exercise design, and delivered technical training to National Guard and federal personnel alongside North Atlantic Treaty Organization (NATO) partners (Virginia Defense Force 2025; Puryear 2025). Exercise director

Col. David Garner described Cyber Fortress as "critical training" designed to test the Commonwealth's ability to respond to a cyberattack and to "continuously improve processes and response capability," demonstrating that the VDF's role is operational, not advisory.

The Maryland Defense Force (MDDF) 256th Cyber Defense Unit extends this principle into a whole-of-government model. Integrated into the Maryland Cybersecurity Task Force, MDDF personnel serve on state active-duty status as threat hunters, attack analysts, and penetration testers across a command structure coordinated by the Governor's Office of Homeland Security (Saunders 2024). Reserve personnel are not attached to the task force; they are constitutive members of it. The "integration without embedding" failure mode is resolved by design.

Execution Capability

Execution capability is the practical ability to act once authority has been established. It depends on pre-negotiated access agreements, pre-positioned technical tools, and established relationships with the organizations that cyber reserve forces are expected to support.

Among these elements, pre-negotiated access agreements are the most critical yet most consistently overlooked. Reserve personnel who arrive at an incident without prior access to affected systems encounter an immediate impediment: before they can do anything useful, they must negotiate the terms of their engagement with an asset owner simultaneously managing an active crisis. These negotiations take time, introduce friction, surface liability concerns that should have been resolved in advance, and delay the response at precisely the moment when speed is most valuable.

Execution capability also requires disciplined force utilization. Many cyber reserve programs use personnel during peacetime to conduct cyber hygiene audits, policy reviews, and risk assessments for local governments. This work has value, particularly for under-resourced municipalities, but it should not consume the personnel best suited for high-intensity incident response. If highly skilled threat hunters, malware analysts, and incident commanders spend most of their reserve time performing routine compliance reviews, programs risk skill degradation, mission drift, and burnout.

Ohio illustrates that personnel management is also a structural design issue. Cyber reserve members ordered to State Active Duty receive a rate of pay determined by rule by the adjutant general, underscoring that compensation mechanics are a real design variable rather than an abstract personnel issue (Ohio Revised Code, § 5923.12). This concern is especially acute during State Active Duty, where highly compensated private-sector cyber personnel may accept short-term activation out of public service, but prolonged or pressured retention can create financial strain, morale issues, and long-term retention risk for the reserve force. A mature reserve model should therefore distinguish strategic support functions, such as governance reviews and baseline assessments, from tactical incident-response functions, such as threat hunting, containment support, malware analysis, and incident coordination. Not all reserve capacity is interchangeable. The highest-value operational capability must be deliberately preserved, exercised, and deployed where it produces the greatest incident-response effect.

Wisconsin's Cyber Response Team (CRT) developed a model worth replicating at scale. Recognizing that cyber insurance operations routinely delay action by mandating organizations to engage their

insurer before taking remediation steps, the CRT proactively established relationships with cybersecurity insurance providers statewide, allowing affected organizations to simultaneously engage both the CRT and their insurer after an incident, compressing response timelines by eliminating a sequential dependency (National Governors Association 2022).

The Software Engineering Institute (SEI) reached a similar conclusion at the federal level: the barriers to an effective civilian cyber reserve are not capability or willingness but structural: "government system access, legal authority, logistics, and conflicts of interest" (Baker et al. 2026). These are precisely the execution infrastructure problems that pre-negotiated access agreements are meant to address. The SEI's recommendation, a scoped pilot beginning with sustainment missions before expanding to response, reflects an understanding that execution capability must be built incrementally, through progressive trust development.

Cross-state exercise investments by SDF cyber units represent a parallel form of execution infrastructure. Operation Dark Node, the September 2025 joint exercise between the Louisiana State Guard and the Virginia Defense Force, was designed to test whether SDF cyber units from different states could rapidly synchronize across state lines to defend shared critical infrastructure (Louisiana State Guard 2025). The exercise demonstrated that interoperability is achievable when units invest in compatible procedures and shared training frameworks in advance. CyberSword's cross-state force-on-force between the Texas State Guard (TXSG) and VDF (Brown 2022) and the multi-state participation in Cyber Fortress 25 each represent the same logic: peacetime investment in the relationships on which incident response depends, applied at the interstate level.

FUTURE FRAMEWORKS

Regional Scaling and the EMAC Model

Cyber risks are inherently trans-border, yet the current state-reserve model is largely siloed within individual jurisdictions. A ransomware actor targeting regional water infrastructure does not respect state lines; the organizations it affects may span multiple states simultaneously. Effective response requires cross-jurisdictional coordination, not courtesy notifications between neighboring CISOs, but the ability to deploy trained, credentialed cyber reserve personnel across state lines rapidly and with unambiguous legal standing.

The Emergency Management Assistance Compact (EMAC)[1] provides the existing legal framework for interstate personnel sharing during declared emergencies and has been successfully deployed across emergency management, public health, and law enforcement disciplines for decades. Its application to dedicated cyber reserve units, however, remains largely untested at scale.

ICS and NIMS organize incident management within a jurisdiction; EMAC governs the legal sharing of personnel and resources across jurisdictions after an emergency declaration. A viable cyber reserve model, therefore, requires both in-state command integration and interstate legal interoperability. The legal questions are non-trivial: reimbursement, liability protection, and the scope of authority granted to deployed personnel are manageable for a National Guard engineer unit, but complex for

1. https://www.emacweb.org/index.php/what-is-emac

a cyber reservist whose actions on a private network may implicate computer fraud statutes in the receiving state.

The exercises documented in this paper, Operation Dark Node, CyberSword, and Cyber Fortress 25, demonstrate that operational interoperability is achievable when units invest in compatible procedures and shared training frameworks. But operational interoperability is not legal interoperability. For the cyber reserve to function as a viable component of national defense, there must be intentional movement toward interstate competency standardization: a Tier 3 responder in Louisiana should be instantly recognizable and integrable into a response team in Virginia, requiring common certification frameworks, standardized role definitions, and a shared operating picture that allows incoming personnel to contribute immediately. The Office of the National Cyber Director provides an existing federal focal point for national cyber policy coordination and, in this context, could help convene interstate standards for credentialing, role definitions, exercise design, and baseline interoperability expectations so that cyber reserve personnel can integrate more quickly across jurisdictions, even if deployment authority remains state-based under EMAC and state law (White House, n.d.).

Governance: Navigating Commercial Conflicts of Interest

A distinctive authority-design challenge in state cyber reserve programs is the risk of commercial conflicts of interest. Because these units frequently recruit from leading security vendors, consulting firms, and managed security service providers, states must ensure that operational access during a reserve deployment does not create procurement leverage, privileged market intelligence, or the appearance of vendor-driven response. The issue is therefore not peripheral to the paper's argument; it is integral to how lawful authority and public trust must be built into the model.

State frameworks have to address this proactively through robust firewall protocols. At a minimum, these should mandate that reservists recuse from participating in procurement cycles directly related to systems, vulnerabilities, or incidents they engaged with during reserve service. Stronger protocols might require pre-incident disclosure of commercial relationships and independent review of procurement decisions made within a defined window during a reserve deployment. The goal is not to eliminate private-sector participation; that participation is the source of the model's value, but to ensure that public service remains unsullied by commercial opportunism. Without these protections, the cyber reserve model is vulnerable to the perception, and the reality, that it functions as a taxpayer-funded intelligence gathering service for commercial cybersecurity firms.

The State Cyber Reserve Maturity Model

The examples presented throughout this commentary demonstrate that cyber reserve capability does not exist on a binary spectrum of "present" or "absent," but rather along a continuum of operational maturity. The maturity model proposed in Table 1 supplies a functional framework for assessing that maturity and identifying the structural changes required to progress from advisory capability to effective operations. The model is intended as an assessment tool rather than a taxonomy. Each maturity level is defined by observable indicators across four dimensions: authority, integration, execution capability, and validation.

Table 1. State Cyber Reserve Maturity Model

Maturity Level	Authority and Integration	Execution Capability	Evidence and Examples
Level 1: Advisory	No dedicated cyber-specific legal standing or only broad enabling authority. Activation depends on voluntary cooperation, informal relationships, or ad hoc requests. Cyber personnel operate outside the primary emergency management or operational command structure.	Produces advice, assessments, reports, and limited technical support. No pre-authorized response tiers, access agreements, or defined remediation pathways exist.	Evidence consists primarily of advisory participation, exercise involvement, and technical recommendations, with limited demonstrated operational impact. Examples include early-stage task forces and nascent SDF cyber units operating under broad enabling statutes rather than cyber-specific authority.
Level 2: Integrated	Formal legal status exists through statute, executive order, state cyber corps authority, or State Defense Force authority. Activation pathways are defined but may still depend on high-level approval or emergency thresholds. Cyber personnel are partially embedded in emergency operations, NIMS/ICS structures, or state cyber response organizations.	Cyber teams can coordinate response actions, prioritize findings, support containment, and advise remediation through established channels. Some access agreements, liability protections, and escalation pathways exist, but execution may still depend on external approval.	Evidence includes state-level exercises, defined command relationships, formal activation procedures, partial access agreements, or real-world incident support with measurable operational contribution. Examples include Michigan MiC3, the Virginia Defense Force 31st Cyber Battalion, the Maryland Defense Force 256th Cyber Defense Unit, and Ohio's Cyber Reserve as a transitioning model.
Level 3: Operational	Cyber-specific authority is predefined before an incident. Activation can occur at the operational level appropriate to incident tempo. Liability, access, and deployment authorities are clarified in advance. Cyber personnel are embedded as operational elements with defined roles inside command structures.	Pre-negotiated access agreements, pre-positioned tools, severity thresholds, response protocols, and pre-approved action tiers allow findings to become operational tasks. The force can support containment, threat hunting, malware analysis, incident coordination, and cross-jurisdictional response.	Evidence includes recurring exercises, real-world deployments, after-action reviews, EMAC-capable or cross-state interoperability, recognized competency frameworks, and demonstrated reductions in time from detection to action. No domestic program examined has fully achieved this level, though Virginia, Texas, Wisconsin, and Maryland each demonstrate components of the model.

CONCLUSION

The cyber reserve model does not fail because of a lack of talent, motivation, or relevance. Rather, it too often fails because it is designed to observe rather than to act. The examples discussed throughout this commentary suggest that the most effective programs have made a deliberate shift: authority is predefined, integration is functional, and execution is expected rather than requested.

The remaining programs face a choice. They can continue expanding advisory capacity while accepting limited operational impact, or they can redesign cyber reserve forces as operational capabilities with the authority, integration, and execution mechanisms required to act at the speed of the threat. The distinction is fundamental. It is the difference between a force that reports risk and a force that reduces it. In a threat environment defined by speed, distributed infrastructure, and persistent adversary activity, the ability to operate is no longer optional; it is the defining characteristic of effective cyber defense.

ABOUT THE AUTHOR

CW3 (LA) Joshua Copeland is a cybersecurity leader, practitioner, and educator operating at the intersection of enterprise security and national defense. He serves as Director of Cybersecurity at Crescendo and as a Deputy Commander in the Louisiana State Guard Cyber Reserve, where he has played a key role in building and operationalizing state-level cyber capability. His experience spans enterprise environments, public-sector incident response, and the integration of cyber operations into emergency management frameworks. Copeland has supported real-world cyber incidents and led large-scale exercises focused on coordination among government and private-sector stakeholders. He is also an adjunct professor at Tulane University, where he teaches cybersecurity and enterprise infrastructure. His work focuses on translating technical capability into operational outcomes, with research interests in cyber resilience, governance, and the role of cyber forces in national defense.

REFERENCES

Baker, Marie, Christopher May, Josh Hammerstein, Russell Griffin, Shawn Wray, Daniel Komnick, and Christopher Herr. 2026. *Independent Assessment of Civilian Cybersecurity Reserve for Department of Defense.* Carnegie Mellon University. Software Engineering Institute, January 15, 2026. https://www.sei.cmu.edu/library/independent-assessment-of-civilian-cybersecurity-reserve-for-department-of-defense/.

Brown, David. 2022. "On the Front Lines of the Cyberwars: Texas State Guard Stages Virtual War Games." Texas Military Department, October 12, 2022. https://tmd.texas.gov/on-the-front-lines-of-the-cyberwars-texas-state-guard-stages-virtual-war-games-.

CISA (Cybersecurity and Infrastructure Security Agency). 2016. *National Cyber Incident Response Plan.* U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

Colorado Department of Transportation. 2018. *CDOT Cyber Incident: After-Action Report.* Colorado Department of Transportation. https://hermes.cde.state.co.us/islandora/object/co%3A40685/datastream/OBJ/download/CDOT_cyber_incident.pdf.

Federal Emergency Management Agency. 2017. *National Incident Management System.* 3rd Edition. Federal Emergency Management Agency. https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf.

GAO (Government Accountability Office). 2017. *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements.* GAO-18-47. https://www.gao.gov/products/gao-18-47.

Hanson, Darin. 2021. "Normalizing Cybersecurity: Improving Cyber Incident Response with the Incident Command System." PhD diss., Naval Postgraduate School. https://www.hsdl.org/c/view?docid=854370.

Indiana National Guard. n.d. "Muscatatuck Cyber Program." Indiana National Guard. Accessed May 15, 2026. https://www.in.gov/indiana-national-guard/muscatatuck-training-center/muscatatuck-cyber-program/.

Louisiana State Guard. 2025. "Operation Dark Node: Louisiana State Guard and Virginia Defense Force Joint Cyber Exercise," September 19, 2025. https://www.linkedin.com/posts/louisiana-state-guard_louisiana-state-guard-and-virginia-defense-activity-7374782084697026560-DGsB.

Michigan Legislature. 2017. *Cyber Civilian Corps Act.* Public Act 132 of 2017. Effective January 24, 2018. https://www.legislature.mi.gov/documents/mcl/pdf/mcl-Act-132-of-2017.pdf.

National Governors Association. 2022. *Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening Our Systems.* National Governors Association, June 14, 2022. https://www.nga.org/wp-content/uploads/2022/06/Cyber_Civilian_Corps_14June2022.pdf.

Ohio Revised Code. n.d.(a). *Chapter 5922: Civilian Cyber Security Reserve Forces.* https://codes.ohio.gov/ohio-revised-code/chapter-5922.

Ohio Revised Code. n.d.(b). *Section 5923.12: Pay and allowances for state active duty; pay for Ohio cyber reserve; protections afforded members.* https://codes.ohio.gov/ohio-revised-code/section-5923.12.

Puryear, Cotton. 2017. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." National Guard Bureau, September 19, 2017. https://www.nationalguard.mil/News/Article-View/Article/1315685/91st-cyber-brigade-activated-as-army-national-guards-first-cyber-brigade/.

Puryear, Cotton. 2025. "Cyber Operators Train for Response, Mitigation at Cyber Fortress 25." Army.mil, September 19, 2025. https://www.army.mil/article/288608/cyber_operators_train_for_response_mitigation_at_cyber_fortress_25.

Razeeq, Michael. 2024. "Laying the Legal Foundation for Civilian Cyber Corps." Lawfare, September 19, 2024. https://www.lawfaremedia.org/article/laying-the-legal-foundation-for-civilian-cyber-corps.

Saunders, Enjoli. 2024. “Md. Military Department Task Force Established to Counter Cyber Threats in the State.” Maryland National Guard, March 13, 2024. https://news.maryland.gov/ng/2024/03/13/md-military-department-task-force-established-to-counter-cyber-threats-in-the-state/.

Scherlis, William L., Stephen L. Squires, and Richard D. Pethia. 1991. “Computer emergency response.” In *Computers under Attack: Intruders, Worms, and Viruses,* 495–504. New York, NY, USA: Association for Computing Machinery. ISBN: 0201530678. https://doi.org/10.1145/102616.102654.

Tariq, Shahroz, Mohan Baruwal Chhetri, Surya Nepal, and Cecile Paris. 2025. “Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities.” *ACM Comput. Surv.* (New York, NY, USA) 57, no. 9 (April). https://doi.org/10.1145/3723158.

Virginia Defense Force. 2025. “VDF Cyber Operators Join Multiagency Cyber Fortress 25 Response Exercise,” September 15, 2025. https://vdf.virginia.gov/2025/09/15/vdf-cyber-operators-join-multiagency-cyber-fortress-25-response-exercise/.

Wenck, Oliver. 2020. “IN Guard’s 127th Cyber Protection Battalion Ready for Duty.” National Guard, October 6, 2020. https://www.nationalguard.mil/News/Article-View/Article/2185436/in-guards-127th-cyber-protection-battalion-ready-for-duty/.

White House. n.d. “Office of the National Cyber Director.” Accessed May 15, 2026. https://www.whitehouse.gov/oncd/.

Received 7 April 2026; Revised 16 May 2026; Accepted 1 June 2026