INSTITUTE FOR DEFENSE ANALYSES

Using National Guard Cyber Forces to support Homeland Cyber Defense activities in non–DoD-Owned Cyberspace

James R. Ayers, project lead
Thomas H. Barth
Robert J. Caverly, Jr.
Elizabeth N. Conrad
Claire R. Harrison
Terry C. Heuring
Jessica M. Huckabey
Michael S. Nash

November 2022

Approved for public release;
distribution is unlimited.

IDA Paper P-33082
Log: H 2022-000183

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication
This work was conducted by the Institute for Defense Analyses under contracts HQ0034-19-D-0001/20-F-0003, Project DZ-8-4706 "Use of National Guard Cyber Forces in support to Homeland Defense Mission Areas" for the National Guard Bureau Director of Operations. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements
The IDA research team would like to thank our National Guard Bureau sponsors in the J36 Engagements Branch for their support across the arc of this project. They opened doors for us to the States and to National Guard Cyber units that made this work possible. We would also like to thank all the cyber personnel across the DoD and the National Guard for taking time out of their schedules to speak frankly with us about the challenges and success of the National Guard cyber mission. We hope this work resonates with the work you do on behalf of DoD, your States, and the nation.

For More Information
James Ayers, project lead, Joint Advanced Warfighting Division
jayers@ida.org | 703-845-6721

Daniel Y. Chiu, director, Joint Advanced Warfighting Division
dchiu@ida.org | 703-845-2439

Copyright Notice
© 2022 Institute for Defense Analyses
730 East Glebe Road, Alexandria, Virginia 22305 ▪ (703) 845-2000

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (Feb 2014).

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper-33082

Using National Guard Cyber Forces to support Homeland Cyber Defense activities in non–DoD-Owned Cyberspace

James R. Ayers, project lead
Thomas H. Barth
Robert J. Caverly, Jr.
Elizabeth N. Conrad
Claire R. Harrison
Terry C. Heuring
Jessica M. Huckabey
Michael S. Nash

Executive Summary

The cyberspace domain is constantly evolving, producing new security challenges daily. Within the United States, common cyber incidents involve individual network owners who cannot keep up with the pace of gap growth and advancing threat landscapes. As private- and public-sector cyber infrastructures increasingly intertwine, the U.S. government may be expected to intervene more frequently. To address this domestic challenge while supporting allies and partners globally, the Department of Defense (DoD) must understand how it fits into a comprehensive, whole-of-nation response that includes future sources of demand and trends in cyber support.

This study considered how the National Guard can help address some of these critical gaps. The National Guard has a series of unique existing capabilities and an impressive cadre of cyber professionals who can and do play important roles in addressing and mitigating cyber incidents.

The National Guard originally tasked IDA with analyzing Title 32 authorities, policies, and directives that can be employed across cyber homeland defense missions. The term *cyber homeland defense missions* is not defined in doctrine or policy. Joint Publication 3-27 defines homeland defense as "the protection of U.S. sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats, as directed by the President of the U.S."[1] Joint Publication 3-12 states DoD has three cyberspace missions: offensive cyberspace operations, defensive cyberspace operations, and DoD information network (DoDIN) operations. Mission categorization is based only on the issuing authority's intent or objective, not on cyberspace actions executed, type of military authority used, forces assigned to the mission, or cyberspace capabilities used.[2]

> You may not have been hit yet in your town or in your city. But it's a question of when, not if. And when it [cyber attack] happens it is very, very problematic. If you think this is something that is easily overcome, go talk to one of the eight or 10 school systems that have been hit since last July. Go talk to the city of New Orleans. Go talk to various sheriff departments, or the convention center. They

[1] Joint Publication 3-27, Homeland Defense, 10 April 2018, vii.

[2] Joint Publication 3-12, Cyberspace Operations, II-2.

actually hit the state of Louisiana on the Monday after the election in November. So this is going to happen. —Louisiana Governor John Bel Edwards, Feb 2020[3]

This research originated in part from the increasing cyber threats to the homeland, presaged in Governor Edwards' warning, and from the growing demand for National Guard cyber forces to help defend against and respond to those threats. The cyber threat space spans all sectors of society and all levels of government. Threat actors range from criminal elements to state-sponsored agents, and their targets include both public and private cyber networks. No network is immune.[4]

While larger, well-resourced organizations and some state and local governments can address their network vulnerabilities and respond to cyber events without external help, some must turn to private fixers or to the government. And often, a first stop for government help is the National Guard. With a cyber force of ~3,900 personnel assigned to various units across the states and territories, the National Guard has significant cyber *capabilities* but limited *capacities*.

At state and local levels, the National Guard has experienced a growing demand to support non-DoD cyberspace (hereafter referred to as *support to off-DoD Information Networks*, or succinctly, off-DoDIN). While the National Guard cyber force can make important contributions, neither it nor the entire DoD cyber force alone can solve the breadth and depth of this problem. Yet, given the accumulating threats and vulnerabilities, requests for National Guard cyber forces to support off-DoDIN networks are likely to increase. Tailored, judicious use of the National Guard's cyber force off-DoDIN will be necessary to avoid depleting this force's ability to meet its Title 10 obligations to DoD.

As part of DoD's total force, the National Guard cyber force is principally organized, trained and equipped to support DoD cyber mission requirements. However, the Secretary of Defense can direct any portion of DoD's cyber force, including the National Guard, to support off-DoDIN networks.[5] Depending on multiple factors—including the nature of the cyber event, the type of support required, and the concurrence of the off-DoDIN owner-operator—the National Guard can support off-DoDIN taskings while activated in Title 10, Title 32 or State Active Duty status and with funding from either DoD, a State or territory,

---

[3] Governor Edwards remarks followed a series of cyber attacks across Louisiana in 2019. For more details see Sam Karlin, "Edwards warns local officials of cyber attacks: 'It's a question of when, not if,'" *The Standard*, 5 February 2020. Accessed online, 15 November 2021.

[4] "The 10 Biggest Ransomware Attacks of 2021," Touro College, Illinois, 12 November 2021; "10 High Profile Cyber Attacks in 2021," Cyber Magazine Online, 21 June 2021. Among the high profile victims in 2021 were Colonial Pipeline, Acer (computer manufacturer), JBS Foods, Microsoft's Exchange Server, the National Basketball Association, and the City of Oldmar, Florida (water supply system).

[5] Examples of National Guard off-DoDIN cyber support includes the 2020 U.S. election, Operation WARP SPEED (the accelerated production and delivery of COVID-19 vaccines), various ransomware attacks, and participating in cyber exercises and planning events at federal, state, and local levels.

or another department of the federal government.[6] This inherent flexibility is part of what makes it an attractive option for off-DoDIN support.

Requests for National Guard support to off-DoDIN public and private networks can originate from state or federal levels. The approval authority for using those forces varies. Governors can approve the use of National Guard forces in State Active Duty status for activities on networks where the Governor has the authority to do so—state-owned networks for example. DoD or National Command Authorities can approve using National Guard forces in Title 10 or Title 32 duty status with a designated lead federal agency and with network owner approval. The types of activities National Guard cyber forces perform off-DoDIN vary and can include vulnerability assessments, partnership building exercises, penetration testing, in extremis mitigations during an attack, and post-incident forensics. National Guard cyber forces perform these off-DoDIN activities off-keyboard while they monitor and advise members of the network owner/operator's team.

Research Purpose and Methodology

The National Guard Bureau tasked IDA to examine the off-DoDIN use of National Guard cyber forces in Title 32 status where DoD is funding the activities of those forces. IDA was also asked to examine the capabilities and capacities of the National Guard cyber force to respond, in Title 32 status, to present and future off-DoDIN taskings. To conduct this research, IDA reviewed an array of authorities, policies, and directives that apply to off-DoDIN support. IDA also interviewed stakeholders in the Office of the Secretary of Defense, National Guard Bureau, State information fusion centers and commanders of National Guard cyber units.

Title 32, Homeland Defense Activity

For this study, the National Guard Bureau was particularly interested in the use of Homeland Defense Activity (HDA) authority found in Title 32 U.S.C § 901-908. Enacted in 2004, this chapter of Title 32 allows governors to request, DoD to source, and DoD to fund activities "undertaken for the military protection of the territory or domestic population of the U.S., or of infrastructure or other assets of the U.S. determined by the Secretary of Defense as being critical to national security against the U.S."[7] Although this authority was not specifically written for cyber operations, the language ostensibly gives DoD the opportunity

---

[6] National Guard personnel may operate in a Title 10 status, a Title 32 status or a State Active Duty status. Personnel in a Title 10 Status are federally funded and under the command and control of the President through the Secretary of Defense. Personnel in a Title 32 Status are federally funded but under the control of the state or territorial governor. Personnel in a State Active Duty status are funded by the state or territory and are under the control of the governor.

[7] Title 32, U.S.C. §901-908 can be found on Cornell Law's website.

and flexibility to act in defense of off-DoDIN cyber networks deemed critical to national security. When applied, this statute would give governors control of National Guard cyber forces made available while requiring DoD to pay for the use of those forces.

To date, there have been three cyber-related HDA requests submitted from state governors, all in 2020. None were approved by the Secretary of Defense.[8] This research concluded there is no prototypical scenario to guide governors or DoD on what an HDA-qualifying cyber incident is. DoD has specific criteria for adjudicating HDA requests; based on these criteria, HDA-qualifying events approximate cyber warfare across key sectors where there is both attribution to a specific actor and where that actor may also be engaged in open conflict with the United States. Given this criteria, it is unlikely that DoD will approve HDA requests for using National Guard forces in response to limited attacks on public or private cyber networks.

Recent and related IDA research has expanded on the broader limitations associated with the creative use of National Guard cyber forces in Title 32 status.[9]

> Title 32 allows, but does not require, the Secretary of Defense (SECDEF) to authorize or fund National Guard cyberspace activities. Although Title 32 authorizes a range of National Guard activities, the SECDEF retains control and ultimately decides what activities may be conducted and will be funded under Title 32 authorities, consistent with OSD policy. The state governors retain command and control of National Guard forces acting in Title 32 duty status. The OSD staff expressed concerns about DoD funding the National Guard activities perceived as primarily benefitting the state, local, tribal and territorial (SLTT) governments rather than DoD, and this perspective is likely to continue to influence DoD approval of SLTT-focused initiatives.[10]

Seams in Protection of Homeland Cyberspace

In addition to the limitations on Title 32 use, the challenge of applying HDA authorities is also a reflection of the broader organizational, policy, and definitional seams between homeland defense and homeland security in an era where the homeland is no longer invulnerable. According to statute and policy, homeland defense operations are focused on external threats and are led by DoD. Homeland security operations, according to joint doctrine, orient on protection and recovery from terrorist attacks and are led by agencies other

---

[8] Illinois, Virginia, and Louisiana all submitted cyber-related HDA requests in 2020, discussed in detail later in this report.

[9] W. Thomas Strickland, et al., *Cyber Models for the National Guard*, (Alexandria, VA: Institute for Defense Analyses, November 2019). Report is For Official Use Only.

[10] Strickland, et al. *Cyber Models for the National Guard*. Report is For Official Use Only.

than DoD, often by the Department of Homeland Security. The administrative demarcations between homeland security and homeland defense are complicated in cyberspace where attribution and intent of the bad actors is more opaque.

A New Strategic Approach is Needed

In 2020, the Congressionally chartered Cyberspace Solarium Commission noted "The United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide. Moreover, shortfalls in agility, technical expertise, and unity of effort, both within the U.S. government and between the public and private sectors, are growing."[11] The commission called for a new strategic approach to cybersecurity and for new policies and legislation to implement that approach. While this might point to potential broader use of National Guard cyber forces off-DoDIN, the capacity of those forces to support off-DoDIN taskings remains limited.

The National Guard Cyber Force—Essential, Capable and Limited

The ~6,000 soldiers, sailors, airmen, and marines in DoD's Cyber Mission Force (CMF) constitute "US Cyber Command's action arm…its teams execute the command's mission to direct, synchronize and coordinate cyberspace operations in defense of U.S. national interests."[12] The National Guard has ~3,900 cyber personnel billets nationwide of which ~2,200 are cyber professionals who contribute in Title 10 status to the CMF on a rotating basis.[13] Executing the National Guard's Title 10 mission is the primary purpose for which these National Guard cyber units are organized, trained, equipped, and federally funded. Overuse of National Guard cyber units and personnel for off-DoDIN taskings could erode the National Guard's ability to contribute to DoD requirements.

Many personnel in these National Guard units hold cyber positions in their civilian jobs. They combine an intimate knowledge of leading edge cyber technologies from the private sector with a deep appreciation of cyber attacker's tradecraft that comes from high-level security clearances and years of military training.

The National Guard cyber force, and the talent therein, is spread unevenly across the states and territories; some states have several large units while others have only a 10-person

---

[11] U.S. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report*, March 2020, 1.

[12] U.S. Army Cyber Command, DoD Fact Sheet: Cyber Mission Force, 10 February 2020.

[13] At any given time, the Army National Guard provides 2x Cyber Protection Teams of 39 persons each and a portion of a National Mission Team, that portion being 22 persons. There is a 6:1 ratio of cyber squadrons in the Air National Guard that provide one continuous Cyber Protection Team. This is explained in detail in Chapter 4 of this report.

Defense Cyber Operation Element.[14] Though there are formal burden-sharing arrangements between the states and territories, the magnitude of national shortfalls in skilled cyber personnel along with the growth in threats and vulnerabilities eclipse the limited off-DoDIN support the National Guard can provide. However, it is within the units themselves where the limited capacities of the National Guard's cyber force are most evident.

For example, in extremis requests for off-DoDIN support typically require the most highly qualified guardsmen in the unit. In a typical Air National Guard cyber squadron of about 70 people, there may be 6 who have the requisite skills for an immediate response. Of those six, perhaps only two are available for a short-notice tasking. Those two are typically placed on State Active Duty status to initially assess the incident and recommend follow-on resources. This assessment can last a few days or a few weeks, during which, those responders may have to take leave, perhaps without pay, from their civilian jobs. Though none of the commanders interviewed for this project expressed insurmountable problems with retention or recruiting, several acknowledged the difficulty of supporting more than 1–2 in extremis taskings for off-DoDIN support in any calendar year. Any response tempo higher than this could impact both retention and their ability to support Title 10 Service obligations.[15]

Where to focus National Guard Cyber Forces off-DoDIN

Among National Guard cyber unit commanders interviewed for this research, there was rough consensus that pre-incident activities may constitute a more viable approach for off-DoDIN activities under Title 32 status. Partnership building exercises are one example of a pre-incident tasking where units have the time to effectively plan their actions and can synchronize and deconflict those events with their Title 10 obligations.

OSD staff interviewed for this report stated that DoD would more likely support, and perhaps consider funding, off-DoDIN Title 32 actions when those actions are oriented on DoD mission assurance equities.[16] Mission assurance must address DoD and non-DoD risks as well as cascading downstream effects on DoD mission essential functions.[17] According to the Defense Science Board, "fixed installations are 99% dependent on the commercial power grid and other critical national infrastructure."[18] For example, the National

---

[14] While the Defense Cyber Operation Element concept of operations allows for up to 17 personnel within a state Element, some states that lack other cyber force structure (e.g., Air National Guard Cyber Operations Squadron) may have perhaps as few as 2–4 limited Defense Cyber Operation Element personnel.

[15] This point was emphasized in the IDA study by Thomas Strickland, referenced above.

[16] Mission Assurance is "A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition." DoD Directive 3020.40, Mission Assurance, 11 September 2018.

[17] DoD Mission Assurance Strategy, April 2012.

[18] "More Fight, Less Fuel," Report of the Defense Science Board Task Force on DoD Energy Strategy, February 2008, 20.

Guard might increase collaboration with the Office of the Assistant Secretary of Defense for Defense Continuity and Mission Assurance in contingency response planning with select power grid owner operators immediately outside the perimeter of a DoD installation. The National Guard might also continue working with OSD Homeland Defense and Global Security (HD&GS) to develop a representative HDA scenario where OSD could approve a state's request.

Recommendations

National Guard cyber unit commanders interviewed for this report stated the demand for the National Guard to support off-DoDIN taskings is growing and that growth reflects the broader threats to and vulnerabilities within the nation's cyberspace, both public and private. Governors may well continue to seek DoD to approve and fund National Guard forces in Title 32 status for off-DoDIN support. Statute and policy constrain the off-DoDIN use of those forces in Title 32 status with DoD funding. A more permissive governing framework—one that supports more broadly using the National Guard in support of off-DoDIN activities—may be possible, but the issue remains of the limited capacities of the National Guard cyber forces. The global shortage of cyber talent will impact any efforts to grow the National Guard's contribution to the cyber force.[19]

What follows is a summary of the recommendations for the National Guard sponsors of this research. The expanded list of findings and recommendations is in Chapter 6 of this report. Additional details are in subsequent sections of this report.

- Improve the messaging from the National Guard Bureau to external stakeholders on capability, capacity, and limitations.
  - Encourage a pre-incident focus—planning, partnering, exercising, developing training plans which include Homeland Defense partnership activities
  - Limit expectations for in extremis responses[20]
  - Coordinate this messaging with the Office of the Assistant Secretary of Defense (OASD) HD&GS
- Orient incident responses toward gathering and forwarding indicators of compromise[21]

---

[19] See Joseph Marks and Aaron Schaffer, "The Cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most," *Washington Post*, 2 August 2021.

[20] Commercial entities are likely to be pulling on these same assets for in-extremis responses. Having the National Guard do this deprives other forces of key, structured opportunities to learn important terrain—knowledge that can be used in case the requirement to respond in-extremis arises.

[21] The Cyber nine-line report is an example of a standard tool for collecting initial forensic information, and then sharing it with key stakeholders including CYBERCOM. These stakeholders can then use this early information combined with other reports to identify patterns and glean insights into threat actor attribution and intent.

- Continue to collaborate with OASD HD&GS to develop a scenario where Title 32 HDA approval would be most likely
- Continue to collaborate with OASD Defense Continuity and Mission Assurance and others on off-DoDIN mission assurance equities.
  - Identify DoD priority public and private networks where tailored National Guard support might bolster network resiliency and support mission assurance;
  - Work with state units that might forge links with those priority networks.
- Champion sourcing leveraged billets, i.e., National Guard cyber liaison officers at NORTHCOM and CYBERCOM
- Selectively participate in partner-building events and contingency planning exercises; mine and share best practices from those activities.
- Continue collaborating with the Department of Homeland Security (DHS) regarding National Guard capability that may support updates to the National Cyber Incident Response Plan.
- Develop standardized capabilities for cyber forces as federal/state requirements evolve.

Contents

1. Introduction 1
   A. Scope 1
   B. Tasking 3
   C. Methodology 3
   D. Report Organization 4
2. Strategic Context: Cyberspace Threats and Responses 5
   A. Threat Environment 5
   B. Defending against the Threat 8
   C. 2020 Election Support—Example of National Guard off-DoDIN Responses to the Threat 10
   D. Critical Infrastructure and Mission Assurance 11
   E. Cyber Strategy Documents—Emphasize Partnership Building 12
   F. Global Shortage in Cyber Workforce 13
3. Authorities and Policy Related to Title 32 15
   A. 32 U.S. Code 15
4. The National Guard Cyber Force 19
   A. The National Guard Cyber Force 19
   B. Unique Attributes and Cyber Skills of the National Guard 28
   C. National Guard support off-DoDIN 30
   D. Other Considerations 32
   E. Implications for National Guard Title 32 activity on non-DoD-owned cyberspace 33
5. Opportunities for National Guard to contribute to Defense of non-DoD–owned Cyberspace 35
   A. Framework for off-DoDIN Actions by National Guard Cyber Force 35
6. Findings and Recommendations 39
   A. Finding: DoD's cyber focus is on Title 10 mission: military and national security issues in DoD cyberspace 39
   B. Finding: There are limits to the Guard's capacity to respond to cyber incidents 40
   C. Finding: Policy restrictions on employing the National Guard under Chapter 9 of Title 32 restrain off-DoDIN cyber response options 42
   D. Finding: The legislative branch has limited the expansion of DoD's footprint in non-DoD cyberspace. 43
   E. Finding: There is movement in Congress to refine roles and responsibilities in cyberspace 44
Appendix A: Specified Tasks Cross Reference A-1
Appendix B: Findings and Recommendations Matrix B-1
Appendix C: Homeland Defense Activity Review Process, as Provided by DoD Directive 3160.01, "HomelandDefense Activities Conducted by the National Guard" C-1
Appendix D: References E-1
Appendix E: Abbreviations F-1

1. Introduction

A. Scope

The cyberspace domain is constantly evolving, prompting new security challenges daily. Within the United States, common cyber incidents involve individual network owners who cannot keep up with rapidly growing gaps and advancing threat landscapes. As the private and public sector cyber infrastructure increasingly intertwine, the U.S. government may be expected to intervene more frequently. To fully address this domestic challenge while supporting allies and partners globally, the Department of Defense (DoD) must understand how it fits into a comprehensive, whole-of-nation response that includes future sources of demand and trends in cyber support.

This study emerged from the desire to explore how the National Guard can help address some of these critical gaps. The National Guard has a series of unique existing capabilities and an impressive cadre of cyber professionals who can and do play important roles in addressing and mitigating cyber incidents. Thirty-one states and territories reached out to their National Guard for cyber support on public and private networks between 2019 and 2020, including for university health networks in Vermont,[22] a ransomware attack on a North Carolina school district,[23] cyber resilience reviews of Connecticut local governments in the lead-up to the 2020 presidential election,[24] and engaging allied foreign partners as part of the State Partnership Program. However, the National Guard alone cannot close these critical gaps. The varied nature of cyber incidents, from SolarWinds to ransomware attacks, and the diversity of actors, from rogue untrained individuals to organizations with nation-state ties, require broader U.S. government and defense sector involvement.

The National Guard originally tasked IDA with analyzing Title 32 authorities, policies, and directives that can be employed across cyber homeland defense missions. Yet, *cyber homeland defense missions* is not defined in doctrine or policy. Joint Publication 3-27 defines *homeland defense* as "the protection of U.S. sovereignty, territory, domestic population, and

---

[22] Office of Governor Phil Scott, "Vermont Army National Guard Cyber Response Team to Support UVM Health Network In Response to Ongoing Information Technology System Disruption," *State of Vermont,* November 4, 2020.

[23] Kristy Keply-Steward, "National Guard now involved in school Ransomware attack investigation," *ABC13 News,* August 25, 2020.

[24] Denise W. Merrill, "Secretary Merrill and General Evon Announce Partnership to Evaluate Election Cybersecurity in Each Connecticut Town," *State of Connecticut,* Office of Secretary of the State, June 12, 2020.

critical infrastructure against external threats and aggression or other threats, as directed by the President of the U.S."[25] Joint Publication 3-12 states DoD has three cyberspace missions: offensive cyberspace operation, defensive cyberspace operations (DCO); and DoD information network (DoDIN) operations. However, the mission categorization is based only on the issuing authority's intent or objective not on the cyberspace actions executed, type of military authority used, forces assigned to the mission, or cyberspace capabilities used.[26]

Given that the National Guard was specifically interested in its cyber force's actions while in Title 32 status, the doctrinal definition of DoD cyber missions—which specifically excludes considering the type of military authority used—was inadequate to scope this research. Through continued collaboration with National Guard Bureau sponsors, it became clear that they were interested in cyber activities where DoD might fund the National Guard's assistance to public and private cyber networks at state and local levels. Thus, a more precise replacement for the term *cyber homeland defense missions* is

> *National Guard cyber unit actions taken in non-DoD-owned cyberspace (or off-DoDIN) while those units are activated in Title 32 status and when those unit's actions are funded by DoD.*

- *National Guard cyber unit*—organizations and personnel from the Army and Air National Guard's portion of the DoD cyber operations force
- *actions*—tactical-level activities or tasks that employ cyberspace capabilities to create effects in cyberspace[27]
- *taken in non-DoD-owned cyberspace (or off-DoDIN)*—includes federal, state, local and privately-owned networks, architectures and systems. Some of these networks may be associated with DoD (e.g., a local grid providing power to an installation) while many are not (e.g., sheriff's department undergoing a ransomware attack). Security of this cyberspace is the principal responsibility of the network owner but the capabilities and capacities of those owners can vary greatly. According to doctrine and policy, military cyberspace forces can defend any U.S. or friendly cyberspace when ordered to do so.
- *while those units are activated in Title 32 status*—activated National Guard cyber forces examined in this research are made available by DoD but controlled by the governor. This is distinct from National Guard cyber forces activated under Title 10 or State Active Duty (SAD) status, both of which are discussed in detail in Chapter 3 of this report.

---

[25] Joint Publication 3-27, Homeland Defense, 10 April 2018, vii.

[26] Joint Publication 3-12, Cyberspace Operations, II-2.

[27] Joint Publication 3-12, Cyberspace Operations, 8 June 2018, II-5.

- *and when those unit actions are funded by DoD*—the federal government funds National Guard forces operating in Title 32 status, but this research is explicitly focused on actions funded by DoD. This would exclude actions taken under Defense Support of Civil Authorities (DSCA) where DoD is typically reimbursed by other departments or agencies for contributions made by DoD forces. [28]

B. Tasking

Within the specified scope, this research examined

- current and potential off-DoDIN demands for National Guard cyber support;
- the authorities, policies and directives related to National Guard off-DoDIN support;
- alignment of National Guard's capabilities and capacities against current and projected off-DoDIN demands; and
- the opportunities for National Guard cyber forces to contribute to off-DoDIN taskings in Title 32 status when funded by DoD.

C. Methodology

The IDA research team reviewed current literature related to threats and vulnerabilities confronting public and private cyber networks and related to the government's strategic plans for responding to those challenges. IDA examined the statutory authorities associated with the National Guard as well as the policies and directives that implement those authorities. Interviews with stakeholders with the Office of Secretary of Defense (OSD) and the National Guard Bureau offered insights into implementing those authorities—in particular the challenges of applying U.S.C. 32 §901-908, Homeland Defense Activities (discussed in detail in Chapter 3).

The National Guard Bureau provided detailed information of the National Guard cyber force's organizational structure and of that force's distribution across the states and territories. Interviews with National Guard unit commanders and personnel yielded insights into capabilities, capacities, and recent taskings for off-DoDIN support. IDA interviewed state fusion center officials to better understand origins and processes associated with requests for National Guard cyber support. The results of this research were briefed to leadership and staff at the National Guard Bureau.

[28] Joint Publication 3-28, Defense Support of Civil Authorities, 29 October 2018.

Select list of stake-holding organizations interviewed by IDA

- National Guard Bureau
  - Cyber Ops Division (J36)
  - Legislative Liaison Office
- Air National Guard
  - ANG Readiness Center
- Army National Guard
  - Army Interagency Training and Education Center (AITEC)
- Department of Homeland Security
  - Operation WARP SPEED
  - Cybersecurity & Infrastructure Security Agency (CISA)
- NORTHCOM
- CYBERCOM
- Office of the Under Secretary of Defense (Policy)
  - Homeland Defense and Global Security (HD&GS)
- West Point Army Cyber Institute
- State Guard Headquarters/Cyber Units
  - Connecticut
  - Colorado
  - Illinois
  - Louisiana
  - Maryland
  - South Carolina
  - Virginia
  - Washington
  - Wisconsin
- State Government
  - Virginia

Figure 1. Organizations Interviewed for this Project

D. Report Organization

Chapter 2 explores the unique features of cyberspace as a threat environment that lead to critical capability and capacity gaps for the United States, and explains the utility of a whole-of-nation response. It also explores past key attempts to respond to this new space. Chapter 3 addresses the authorities, policies, and directives related to the National Guard in general, and to the DoD-funded Title 32 use of the National Guard in particular. Chapter 4 explains the National Guard's organization, mission, and activities, detailing the unique capabilities and capacity that make it a valuable actor in cyber defense. Chapter 5 suggests opportunities for the National Guard cyber force to contribute to off-DoDIN cyber taskings in Title 32 status with DoD funds. Chapter 6 outlines the key findings and recommendations emerging from IDA's research.

2. Strategic Context: Cyberspace Threats and Responses

A. Threat Environment

The cyber threat surface is global and ubiquitous, touching every facet of society and every network, public and private. During this research project alone, the United States. witnessed several significant cyber events: the SolarWinds cyber attack, which affected more than 18,000 public and private sector customers; the Microsoft Exchange hack; and numerous ransomware incidents, including the attack on the Colonial Pipeline along the East Coast.

According to Verizon's 2019 Data Breech Investigations Report, within the context of a typical off-DoDIN cyber incident, the timeline from an attacker's first action to breach a network until that network is compromised can be measured in minutes. The time to discover and respond is more likely measured in months. Conducting vulnerability assessments to avoid being penetrated in the first place become crucial.[29]

[29] Verizon Data Breach Investigations Report for 2019, Figure 28.

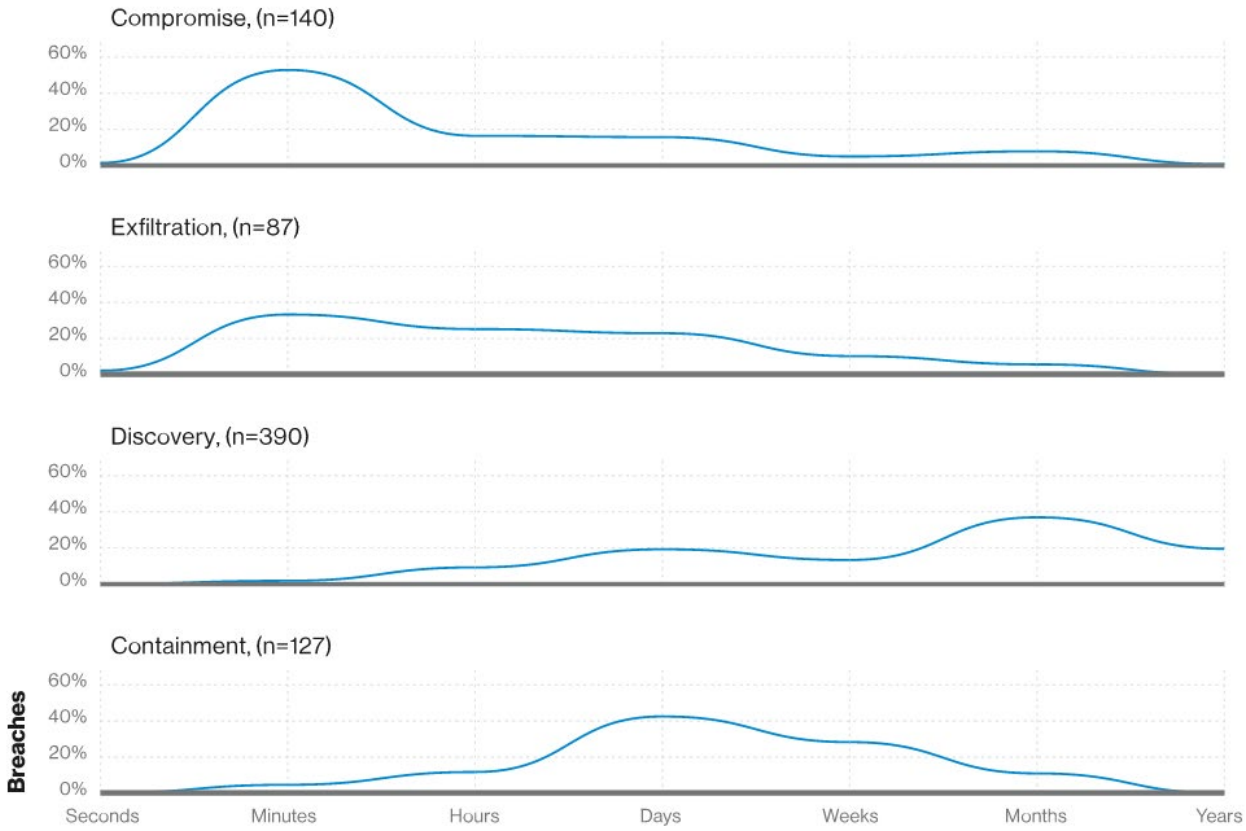

Figure 2. Breach Timelines[30]

Threat actors can range from lone-wolf hackers to criminal enterprises to state-sponsored agencies. Their actions may include hacking a server to install malware or using a phishing attack to influence human behavior.[31] Their objectives range from financial theft to undermining American economic and military power. Despite the range of actors, tactics, and motives, when it comes to off-DoDIN networks, the trends are clear. Verizon reports annual assessments of data breaches on networks across the globe. According to its data, most incidents are perpetrated by organized criminal enterprises that employ ransomware or denial of service actions for financial gain (Figures 3 and 4). [32]

---

[30] Verizon Data Breach Investigations Report for 2019, Figure 28

[31] Verizon Data Breach Investigations Report for 2019, 4.

[32] Among the more comprehensive annual assessments of cyber incidents worldwide is the Verizon Data Breach Investigation Report. This report has been issued annually since 2008. The 2021 report compiled data on 79,365 reported data breach incidents from 88 countries across public and private sectors including law enforcement, research institutions, private security firms, national incident reporting structures and Verizon itself. Verizon then screens the incident data against internal quality assessment standards.

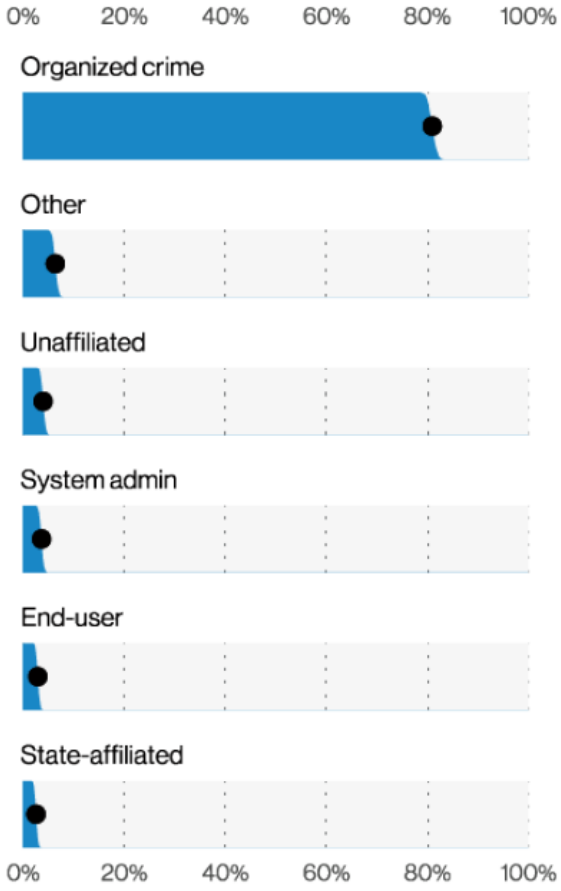

Figure 3. Top Threat Actor Varieties in Data Breaches (n=2,277)[33]

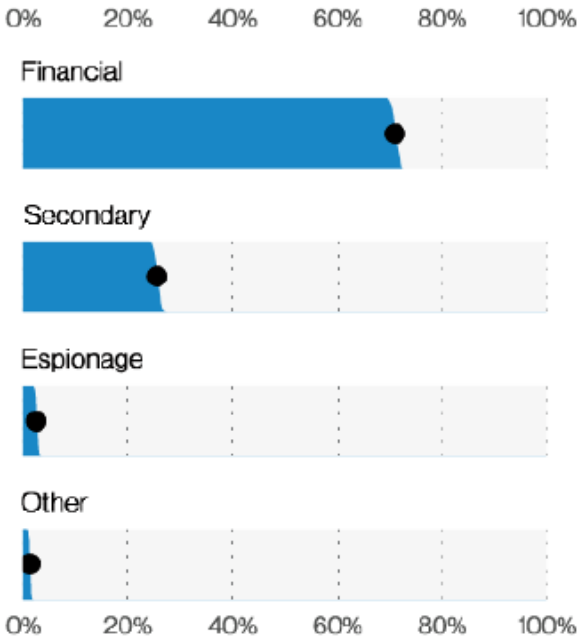

Figure 4. Top actor motives in incidents[34]

Solar Winds, Microsoft, and Colonial Pipeline are examples of well-resourced, capable network owners who still fell victim to cyber attacks. No network is impregnable. Preparation, vigilance, and responsiveness are best practices that are unsupported or unaffordable for many off-DoDIN network owners. Local hospitals, county sheriff departments, and municipal election boards are examples of resource-limited owners of public networks that criminals have targets looking for a quick ransom payment.

In some cases, the criminal enterprise *is* a state actor. For example, the North Korean military was behind a series of recent cyber attacks on sectors ranging from entertainment to banking to law enforcement to defense. In 2021, the U.S. Department of Justice indicted

---

[33] Verizon Data Breach Investigations Report for 2019, 12.
[34] Verizon Data Breach Investigations Report for 2019, 14.

three North Korean military hackers who allegedly conspired to steal or extort $1.3 billion in money and cryptocurrency.[35]

B. Defending against the Threat

Network owners and operators are the first line of defense to shore up their networks' vulnerabilities and respond to cyber incidents, but their ability to protect and respond can vary widely. Private enterprises can help identify and address vulnerabilities before an incident and those that can help restore function after an attack as long as the network owner or operator can pay for these services. State and federal entities such as the Department of Homeland Security's (DHS) Cyberspace and Infrastructure and Security Agency (CISA) may be called on to assist before, during or after a cyber incident—a fundamental question for this research is at what point is DoD obligated to source and fund a cyber action off-DoDIN as part of its Homeland Defense mission? While DoD can be tasked to support any off-DoDIN network, the Department's and the National Guard's off-DoDIN priorities should be (1) to support response planning and partnership building before an incident, and (2) to mine early indicators of compromise in the wake of an incident.

Cyber exercises such as Jack Voltaic and Cyber Yankee are two examples of how DoD and National Guard cyber forces can contribute to off-DoDIN response planning, partnership building, and compromise mining before an incident. Jack Voltaic events are a series of exercises sponsored by the U.S. Army Cyber Institute at West Point that explore how to synchronize DoD, U.S. Government, and private sector capabilities in a cyberspace attack response. Jack Voltaic results enable multiple partners to recognize the defense impacts of cyberspace operations from a municipal and critical infrastructure perspective.[36]

Cyber Yankee events are an example of several regional cybersecurity exercises designed to promote interoperability of National Guard cyber operators among the New England states and to build readiness to respond to network attacks.[37] National Guard cyber responders had to work with their supported mission partners similarly to how they would experience in a real world scenario. Guardsmen analyzed information reported on notional threats according to most likely and most dangerous courses of actions against friendly cyber first responders and their supported mission partners. The scenarios employed in the

---

[35] "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," Department of Justice Press Release, 17 February 2021.

[36] U.S. Army Cyber Institute, Jack Voltaic Critical Infrastructure and Public-Private Partnerships, 18 July 2019, 4.

[37] Other examples include Cyber DAWN (Joint and Multi-agency exercise including National Guard units from California and Washington) and Cyber SHIELD (national level capstone exercise). Both of these incorporate local mission partners and include a focus on state/federal cooperation.

2018 exercise used known realistic threat actions in today's operational environment to support exercising prescribed battle drills.[38]

Every cyber action leaves a trail. Despite the certainty in Verizon's report, it can be difficult to determine who conducted a cyber attack (attribution) and why (intent). The interconnected nature of cyberspace can victimize U.S. networks even when another network or country is the target.[39] Incidents that appear unrelated in time, space, and purpose could be connected with corrosive synergistic impacts on multiple networks. These are all elements that must be weighed when deciding if and how DoD is to respond. While military cyberspace forces will defend any U.S. or other friendly cyberspace when ordered, DoD's statutory obligation is homeland defense.[40]

By law, DoD is responsible for two missions in the homeland: DSCA and homeland defense. DoD supports HS operations through DSCA and through actions taken under Defense Support to Cyber Incident Response (DSCIR).[41] DoD policy authorizes DSCIR within the framework of DSCA. DSCIR may include direct on-location support, remote support, or a combination of both. DSCIR can be provided using DoD military personnel, DoD civilian personnel, and DoD contractor personnel (including National Guard units serving in a Title 32 U.S. Code, duty status).[42]

Although National Guard cyber forces can be activated in Title 32 status to conduct off-DoDIN DSCA-DSCIR operations, those forces are funded by an agency other than DoD, often DHS. This research is focused on Title 32 cyber action off-DoDIN where *DoD* funds those forces. Thus, DSCA and DSCIR are outside the scope of this report.

According to joint doctrine, homeland defense is "the protection of U.S. sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President of the U.S."[43] As the lead agency responsible for homeland defense, DoD's decision to source and fund National Guard cyber forces in Title 32 status must be based on both the nature of the event (i.e., attribution, intent, consequence) and on DoD's assigned missions and functions as defined in statute and implemented through policy directives. Chapter 3 of this report reviews the authorities and policies most relevant to the Title 32 use of National Guard cyber forces for off-DoDIN actions.

---

[38] Cyber Yankee 2018 After Action Report/Improvement Plan, ver. 1.0, 9 July 2018, 5. See also David Pytlik, "New England Guard members train at Cyber Yankee," Connecticut National Guard, 24 June 2021.

[39] Cyberspace Solarium Commission Report, March 2020, 8.

[40] Joint Publication 3-12, II-4; and Joint Publication 3-27, I-1.

[41] Joint Publication 3-27, 10 April 2018, vii.; DoD Directive Type Memorandum (DTM) 17-007, "Interim Policy and Guidance for Defense Support to Cyber Incident Response (DSCIR)," 21 May 2021.

[42] Strategic Cyberspace Operations Guide, U.S. Army War College Center for Strategic Leadership, 1 August 2021, 64.

[43] Joint Publication 3-27, vii.

C. 2020 Election Support—Example of National Guard off-DoDIN Responses to the Threat

In addition to participating in exercises such as Jack Voltaic and Cyber Yankee, the National Guard cyber force is often called for other actions supporting off-DoDIN networks. For example, National Guard cyber forces supported the 2020 U.S. national elections. More than 30 states requested and received varying support from the National Guard that included vulnerability assessments, risk mitigation implementation, and network monitoring. Other support related to the elections included publishing National Guard Bureau election planning guidance and a threat information-sharing concept of operations. They participated in "Table Top the Vote" virtual exercises with mission partners and state election boards. Most often, these responses are in SAD status. By August 2020, this support involved 117 personnel (44 from Army National Guard (ARNG) and 73 from the Air National Guard (ANG)) from cyber units in 9 different states. Of those personnel activated for this support, 110 were in SAD status and 7 were in Title 32 status.[44]

Figure 5 depicts some of the actions and force elements that the National Guard provides to off-DoDIN networks. This particular example is from the Iowa National Guard, but is somewhat representative of capabilities and capacities within other National Guard cyber units. Chapter 4 of this report details the organization of the National Guard cyber force.

[44] National Guard Cyber General Officers Advisory Council (Cyber GOAC) briefing, 19 August 2020, slides 24 and 25. Florida and Illinois National Guard cyber forces provided consulting to state elections boards and Tennessee provided a standing quick response force to county election authorities. As identified in this briefing, none of the personnel in Title 32 status provided direct support to polling locations, an activity DoD prohibits by policy from being done in either Title 10 or Title 32 status.

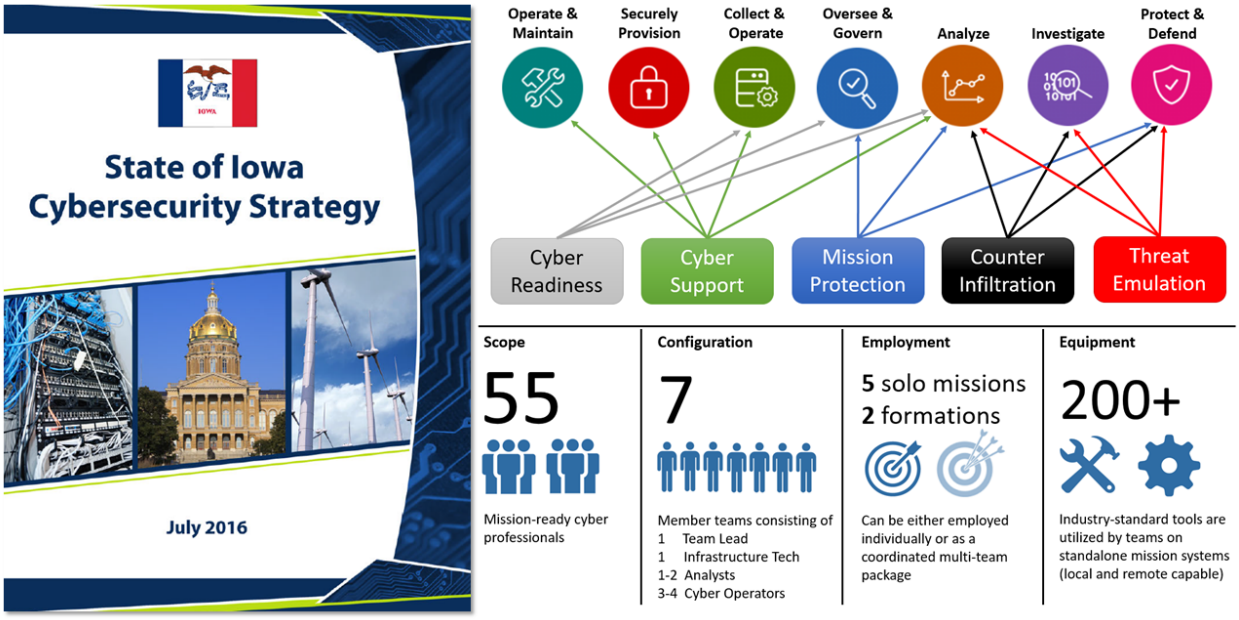

Figure 5. Example of National Guard off-DoDIN Cyber Actions and Force Presentation[45]

D. Critical Infrastructure and Mission Assurance

Homeland defense includes protecting critical infrastructure. Presidential Policy Directive 21 identified 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, were considered so vital to the United States that their incapacitation or destruction would cripple security, national economic security, national public health or safety, or any combination thereof. [46]

An area where DoD's obligations possibly align with select off-DoDIN support is the intersection of critical infrastructure and mission assurance.[47] For example, this might include public and private providers of power and water to military installations or rail operators that load and move military equipment from forts to ports. DoD's mission assurance depends on public and private assets that DoD does not own. DoD recognizes the need to build relationships and promote information sharing with these external stakeholders. The office of the Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance is responsible for developing plans and policies to assure the Department can execute

---

[45] 168th Cyber Operations Squadron, Iowa National Guard, Unit Capstone Review, August 2019.

[46] Presidential Policy Directive 21, 12 February 2013. The sectors are chemical, communications, dams, emergency services, financial services, government facilities, information technology, transportation system, commercial facilities, critical manufacturing, defense industrial base, energy, food and agriculture, healthcare and public health, nuclear, water and wastewater.

[47] According to DoD Directive 3020.40 (29 November 2016), *mission assurance* is a process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition.

its core functions, even in the face of asymmetric military threats. Continued coordination between the National Guard Bureau, OASD for Defense Continuity and Mission Assurance, and OASD Homeland Defense and Global Security (HD&GS) could help identify a set of off-DoDIN networks where the limited cyber forces in the National Guard could best be leveraged, before or after a cyber incident.

E. Cyber Strategy Documents—Emphasize Partnership Building

Using the National Guard cyber force to build off-DoDIN partnerships and advance the national "defend forward" objective is nested in and complementary to recent national strategy documents, as well as to the National Guard's Cyber Strategy (under revision as of this writing). According to the Cyberspace Solarium Commission, defend forward "posits that to disrupt and defeat ongoing adversary campaigns, the U.S. must proactively observe, pursue, and counter adversaries' operations and impose costs short of armed conflict."[48] Closer coordination between government and private networks will be an important part of defending forward. The U.S. National Cyber Strategy called for improving partnerships between pubic and private sectors as a path toward collective risk management approaches.[49] Among the goals in the National Guard Cyber Strategy is "expand and leverage enduring relationships with the Private Sector, Academia and International Partners."[50]

Examples of established relationships between the National Guard and external partners include

- Washington National Guard: Snohomish County Public Utility District
- Maryland National Guard: Exelon Corporation (energy
- Michigan National Guard: State Chief Information Officer and Chief Security Officer, cyber incident response planning (applies to several state Guard units)
- South Carolina National Guard: SCANA Corp (electricity and gas, later acquired by Dominion Energy)
- Tennessee National Guard: Tennessee Valley Authority
- Connecticut National Guard: Metropolitan Water Authority
- Wisconsin National Guard: various utility companies
- North Carolina National Guard: State Department of Transportation
- Montana National Guard: Monsanto Corp.[51]

---

[48] Cyberspace Solarium Commission Report, Executive Summary, March 2020, 2.
[49] U.S. National Cyber Strategy, September 2018.
[50] National Guard Cyber Strategy, January 2018, 16.
[51] National Guard Bureau J36 Cyber Operations Briefing, no date, slide 7, notes section.

F. Global Shortage in Cyber Workforce

As Chapter 4 of this report points out, the National Guard cyber force comprises personnel who work in both civilian and military cyberspace; Chapter 3 describes the authorities that allow them to serve in both federal and state capacities. The National Guard is uniquely positioned to contribute to public-private partnership building; yet, the demands for its help could quickly outstrip its capacities. For example, the 2,200 cyber professionals in the National Guard cyber force are a fraction of the overall national cyber workforce (see Figure 6). Substantial shortages exist across the global cyber workforce. According to (ISC)^2's 2020 report on the cyber workforce, there is a shortage of ~376,000 cyber workers in North America, and of that number, a shortage of nearly 360,000 cyber workers is in the United States. The entire National Guard cyber force is less than one percent of the total shortfall in U.S. cyber workers. Aside from highlighting the scope of the challenge, the workforce gaps also limit the National Guard's ability to grow its cyber force in the near term even if funding were available to support that growth.

Defending forward against growing threats with a shortage of cyber workers will require more than an whole-of-government approach—a whole-of-nation effort is needed. The National Guard cyber force can contribute, but it must be used in select, prioritized ways as the rest of this report attests.

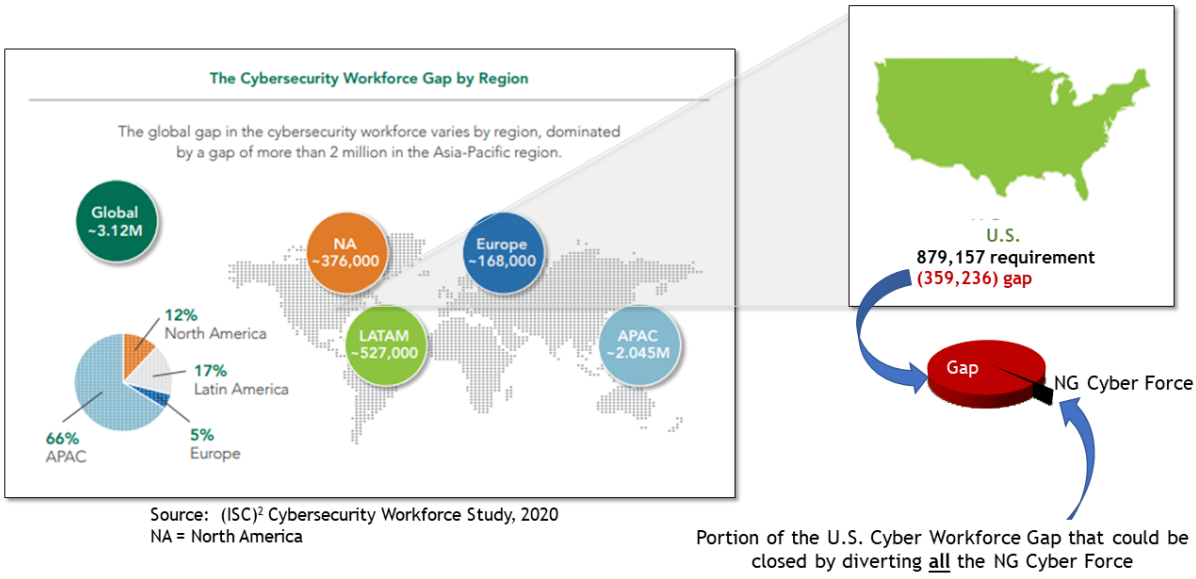

Figure 6. Global Shortages in Cyber Workforce[52]

[52] "Cybersecurity Professionals Standup to a Pandemic," (ISC)^2 Cyber Workforce Study, 2020, 17.

3. Authorities and Policy Related to Title 32

The National Guard is the only U.S. military force that operates across both State and Federal responses, leveraging State Active Duty, National Guard Duty (Title 32), and Active Duty (Title 10). While SAD, Title 32, and Title 10 are different statuses and roles, they are mutually supporting. However, the scope of this research and the content of this chapter is oriented on use of National Guard cyber forces off-DoDIN in Title 32 status where DoD provides the funding for the use of those forces. The headings of this chapter are based on statutory authorities. DoD and National Guard policy documents are discussed within the context of implementing the associated authority.[53]

A. 32 U.S. Code

Title 32 status is intended and used principally for training National Guard members and units for Title 10 missions, but specifically provides authority for off-DoDIN cyber activities. Section 502 (a) and (f), as well as Sections 901–908 in particular encompass Homeland Defense Activities, discussed below.

1. 32 U.S. Code § 502(a)

Section 502(a) prescribes the required annual training for "each company, battery, squadron and detachment of the National Guard" as assembly "for drill and instruction" at least 48 times a year (Inactive Duty Training or IDT) and "encampments, maneuvers, outdoor target practice, or other exercises, at least 15 days each year (Active Training or AT)." This constitutes the basic requirement for National Guard training.

Per National Guard Regulation 350-1, IDT and AT are mandatory duty with a primary purpose of training for unit readiness of the federal mission. National Guard Regulation 350-1 allows for limited DSCA training. Training for these contingencies is integrated with training for wartime missions. The ANG and ARNG conduct this requisite training under § 502(a) through annually approved and published training plans in coordination with the Air Force and Army respectively.

This training is not to be performed in support of civil authorities in response to an emergency ordered by a state or territorial governor, including those emergencies when a

[53] See Appendix B of IDA's 2019 report Strickland, et.al., *Cyber Models for the National Guard* for a comprehensive review of authorities and policies related to the National Guard's cyber enterprise, and for more information on DoD Issuances and Joint Publications.

presidentially declared disaster qualifies a state for reimbursement of associated preparation or recovery costs through a lead federal agency. By exception, AT may be used in response to a State or federal emergency that occurs during a pre-planned annual training event when, at the discretion of the state adjutant general, the work performed satisfies or complements the unit's wartime mission or annual training objectives.[54]

DoD allows supporting mission requirements under circumstances incidental to performing IDT and AT. For example, natural disasters such as flood and hurricane response may be considered part of unit annual training within the purview of 32 U.S.C. §502(a), and federal funds may be used to pay for the actions of those forces, but the expenditure of those funds must still be consistent with established Service-level training objectives.[55]

National Guard personnel participating in their required training under §502(a) may be able to participate in cyber response activities under Immediate Response Authority (IRA). IRA can provide initial response between the onset of an unforeseen circumstance and the availability of forces or capabilities through other mechanisms such as State Active Duty (SAD) or Full-Time National Guard Duty under 32 U.S.C. §502(f). IRA is limited to actions in response to a request from civil authorities designed to save lives, prevent human suffering, or mitigate great property damage. IRA may only be exercised with personnel on-hand at the time of incident; personnel may not be brought on duty for IRA, nor is IRA a tool for sourcing preplanned requirements.[56]

In other words, the window for using §502(a) for *federally-funded* off-DoDIN support is narrow and of limited duration. The planned actions, before or after a cyber incident, must align with planned training objectives, planned dates for training, and planned availability of personnel. Yet, this research is oriented on *DoD-funded* off-DoDIN support. In many cases, the federal funding responsibility under the window described above would fall to DHS or an agency other than DoD. There would need to be definitive links between the incident, the actions taken, and DoD's statutory obligations for homeland defense in order for DoD to fund the tasked elements of the National Guard cyber force. Ostensibly, U.S. Code 32 §§901-908, provides more opportunity for DoD-funded off-DoDIN support.

2. 32 U.S. Code § 502(f)

32 U.S. Code §502(f) is Full Time National Guard Duty for Operational Support (FTNGD-OS) and intended to provide necessary skilled personnel to support existing or emerging requirements. Guardsmen activated under §502(f) are restricted to performing

---

[54] "Domestic Operations Law and Policy," National Guard Judge Advocate General, Second Edition, 2019, 66–67.

[55] "Domestic Operations Law and Policy," 66–67.

[56] See Department of Defense Directive 3025.18, "Defense Support of Civil Authorities" and Joint Publication 3-28, "Defense Support of Civil Authorities," October 29, 2018.

those duties for which they were activated. If circumstances require a change of duty, commanders must amend or curtail the current order. Guardsmen activated in §502(f) status may be used for DSCA/DSCIR if the governor formally requests DSCA authority and if DoD approves that request.[57] DSCA is not a homeland defense mission and is ordinarily not DoD's funding responsibility.

3. 32 U.S. Code §§901–908, Homeland Defense Activity

This section authorizes National Guard homeland defense activities in Title 32 status. Each activity must have the approval of the President or the Secretary of Defense.[58] *Homeland defense activity* is defined specifically: An activity undertaken for the military protection of the territory or domestic population of the United States, or of infrastructure or other assets of the United States determined by the Secretary of Defense as being critical to national security, from a threat or aggression against the United States.[59]

The restrictions on employing the National Guard under this section are significant. (This is discussed further in Chapter 6.) In practice, state requests must be a "military-unique" activity to be "military protection," involving an external threat, possibly only a nation-state action, that broadly targets the United States, not a single state. The request cannot be a DSCA or DSCA-like activity in support of some other entity. Lastly, the Secretary of Defense must determine that affected infrastructure or assets are "critical to national security."

For this research project, the National Guard Bureau was particularly interested in the use of Homeland Defense Activity authority found in Title 32 U.S.C. §§ 901–908. First enacted in 2004, this authority allows Governors to request, DoD to source, and DoD to fund activities "undertaken for the military protection of the territory or domestic population of the U.S., or of infrastructure or other assets of the U.S. determined by the Secretary of Defense as being critical to national security against the U.S."[60] Although this authority was not specifically written for cyber operations, the language ostensibly offers DoD the opportunity and the flexibility to defend off-DoDIN cyber networks deemed critical to national security. When applied, this statute would give governors control of National Guard cyber forces made available, while requiring DoD to pay the cost of using those forces.

To date, there have been three cyber-related HDA requests submitted from state governors, all in 2020. None of them were approved by the Secretary of Defense.[61] In broad

---

[57] DoD Instruction 3025.22, The Use of the National Guard for Defense Support of Civil Authorities, 15 May 2017.

[58] Department of Defense Directive 3160.01.

[59] Title 32 U.S.C. § 901

[60] Title 32, U.S.C. §§901–908 can be found on Cornell Law's website.

[61] Illinois, Virginia, and Louisiana all submitted cyber-related HDA requests in 2020. These are discussed in detail later in this report.

terms, those requests were processed through state information fusion centers and routed through the governor's office for signature. The requests were then forwarded to DoD where they were staffed for OSD's review by the OASD HD&GS.

According to HD&GS, the basis for the denials centered on several factors including the lack of military essentiality (i.e., the response did not exclusively require the use of a military force); the uncertainty that the causal events constituted an attack on the U.S. as a whole rather than an attack on an individual network or series of networks for financial gain or some other disruptive purpose; and the likelihood that a federal agency other than DoD had lead responsibilities for action.

Regrettably, there is no prototypical scenario to guide governors or DoD on what an HDA-qualifying cyber incident might be. This is due, in part, because the qualifying criteria, all of which must be met, closely approximate what would be expected of a Title 10 response, for instance in a conflict with a peer competitor where homeland cyber networks were under broad attack.

4. The National Guard Cyber Force

Principally organized, trained and equipped to serve as a strategic and operational reserve for DoD's cyber force, the National Guard cyber force is a complex mix of 2,200 Soldiers and Airmen assigned to units across the states and territories in both the ARNG and ANG.[62] Most of this force can be mobilized for federal missions including defeating threats to national cyberspace, protecting the DoDIN and the Guard Network (GuardNet), and responding as tasked to the defense of friendly cyberspace. Some units perform scheduled rotations mobilized in Title 10 status.

This chapter begins with a glimpse into the ARNG's and ANG's organization and missions. It then examines the National Guard as part of DoD's total cyber force, and it concludes by assessing the National Guard's off-DoDIN–related taskings, capabilities, and capacities.

A. The National Guard Cyber Force

The National Guard cyber force comprises units drawn from both the ARNG and ANG. It is a capable foundational force with many units having been formed in the past 2–5 years. Several units are still being established and will not reach full operating capability until 2022 or later.

This force includes action units such as the ANG's 70-person Cyber Operations Squadrons (COS) and the ARNG's 39-person Cyber Protection Teams (CPTs) that contribute off-DoDIN in partnership building, response planning, incident assessments, command and control of other National Guard response forces. The force also includes headquarters elements that recruit, train, and certify subordinate units assigned across multiple states. Support units provide action units with forensics analyses, infrastructure maintenance, and other functions.

Many in the Guard cyber force are also cyber specialists in their civilian jobs. The most qualified cyber force in the Guard are perhaps some of the most skilled cyber specialists in DoD. In many cases, they have personal relationships with the private and public

---

[62] The units include the following:
1x Brigade (91st)
5x Battalions within 91st Brigade
3x Cyber Operations Groups
15x Cyber Operations Squadrons
14 Mission Defense Teams
Of note only 100 personnel from the ANG are at any given time serving within the CMF (filling 2x Cyber Protection Teams and a portion of 1x National Mission Team).

network owners with whom they interact in their Guard or their civilian duty—there is an existing level of trust that enables more efficient and effective response. When they are tasked with an off-DoDIN cyber incident response, they may show up in civilian clothes (to avoid the perception of a militarized response). They apply their panoply of skills but do so most of the time off-keyboard for liability and other concerns. They may have tools in their kit that are DoD-only and cannot be used in off-DoDIN activities. Individual skill-sets are not always correlated with rank. Junior- and mid-grade enlisted personnel can be among the highest qualified personnel in a unit.

As Figure 7 illustrates, the National Guard's cyber force is distributed unevenly across the states and territories. Some states—Washington, Maryland, Virginia, all hubs of private and public cyber enterprises—have substantial forces while other states such as Nevada, West Virginia and Florida have only a 10-person Defense Cyber Operations Element (DCOE). Many factors that determine the location and mission of National Guard cyber forces, but individual units tend to recruit personnel locally and this factors into the posture calculus for the force. Through arrangements between states and territories, cyber forces can be tasked to respond across state lines to off-DoDIN assistance requests and units in some states command subordinate units in other states.[63]

[63] National Guard support between and across multiple states is normally captured in standing Emergency Management Assistance Compacts or EMACs.

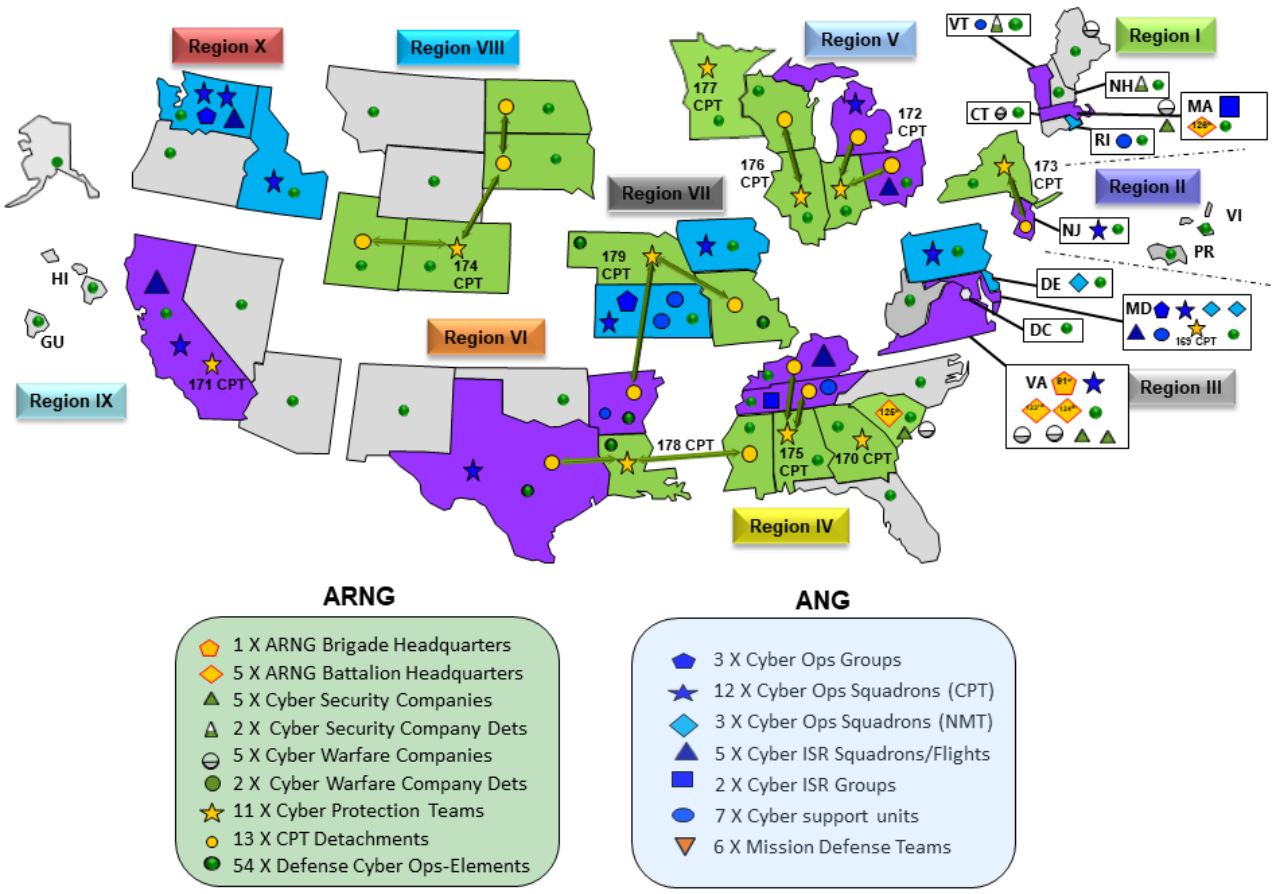

Figure 7. National Guard Cyber Force[64]

Most of the National Guard cyber force can be mobilized for Title 10 missions. Several units such as ANG's Cyber Operations Squadrons fulfill scheduled six-month rotations in Title 10 status as part of U.S. Cyber Command's (CYBERCOM) Cyber Mission Force (CMF). Other units provide Service-retained reserve forces such as the ARNG's CPTs who support U.S. Army Cyber Command's wartime mission.

---

[64] Source: National Guard Bureau J-36. The National Guard cyber force structure continues to evolve; some changes are not reflected on this chart. Among the changes are the exclusion of DCOEs as part of the cyber operations forces. Also excluded from the cyber operations forces are the 5x Cyber ISR Squadrons/Flights, 2x Cyber ISR Groups, and 7x Cyber support units. The latter support intelligence operations. Lastly, as of this writing, 14x Mission Defense Teams are growing to 20 teams by the end of fiscal year 2022. Under the ANG box on Figure 7, 12 Cyber Operations Squadrons contribute to DoD Cyber Protection Teams (CPTs) and 3 contribute to National Mission Teams (NMTs). CPTs defend DoD's information network, protect priority missions and prepare cyber forces for combat. NMTs defend the nation by identifying adversary activity, blocking attacked and maneuvering to defeat them.

The next section of this chapter examines the ARNG and ANG cyber force in more detail.

1. Army National Guard Cyber Force (~980 personnel)[65]

a. 91st Cyber Brigade (~980 personnel)

Most ARNG cyber units are assigned to the 91st Cyber Brigade (Virginia). Figure 8 is an organizational diagram of the 91st Cyber Brigade. The 91st Cyber Brigade was officially activated on 1 September 2017, and is the ARNG's first and only cyber brigade. The brigade consists of five battalions, five cyber security companies, five cyber warfare companies, and 11 cyber protection teams arrayed across 30+ states.[66] Among the brigade's key operating units are

- **Cyber Security Company (CSC)** (36 personnel). The five CSCs conduct DCO in support of Corps and below, other unified land operations, and the Joint Force, which includes Cyber Command readiness inspections, Vulnerability Assessments, forensics analysis, critical infrastructure assessment and support, and Cybersecurity support. Provide Mission Command to Cyber Security Team, Cyber Security Support Team, and Critical Infrastructure Team which includes operational direction and guidance in the conduct of Defensive Cyberspace Operations. Includes: a unit command group (3 personnel); a cyber security (incident response) team (11 personnel); a critical infrastructure protection team (9 personnel); and a security support (forensics) team (13 personnel).[67]
- **Cyber Warfare Company (CWC)** (33 personnel). The five CWCs conduct DCO in support of Corps and below, other unified land operations, and the Joint Force, which includes Cyber Opposition Force support, Network Warfare activities, and Cyberspace Operational Preparation of the Environment actions. Provide Mission Command and operational support to the Network Warfare Team, Cyber Analysis Team, and the Cyber Support Team, which includes orders and guidance in the execution of Cyberspace Operations. Includes: a unit command group (3 personnel); a network warfare team (9 personnel); a cyber analysis team for capability development (10 personnel); and a cyber support team for infrastructure support (11 personnel).[68]

---

[65] Unlike the ANG, the ARNG is not counted as part of the CMF.

[66] Virginia National Guard website description of 91st Cyber Brigade.

[67] Colonel Adam Volant, Army National Guard–Cyber Brigade, AFCEA Industry Day presentation, not dated, slide 6.

[68] Volant, Army National Guard–Cyber Brigade, AFCEA Industry Day presentation, slide 7.

- **Cyber Protection Team** (39 personnel)[69] The 11 CPTs, all ARCYBER-retained units, provide mission assurance and threat mitigation support to the U.S. Critical Infrastructure Key Resources (CI/KR) and U.S. Military Services and Combatant Commands' key terrain. They conduct DCO on military networks to support mission requirements. In compliance with federal and state laws, DCO may be expanded to include Cyber Command Readiness Inspections, Vulnerability Assessments, Cyber Operational Forces (OPFOR support), Critical Infrastructure Assessments, support for Theater Security Cooperation activities, training support, and advisory and assistance support.[70]

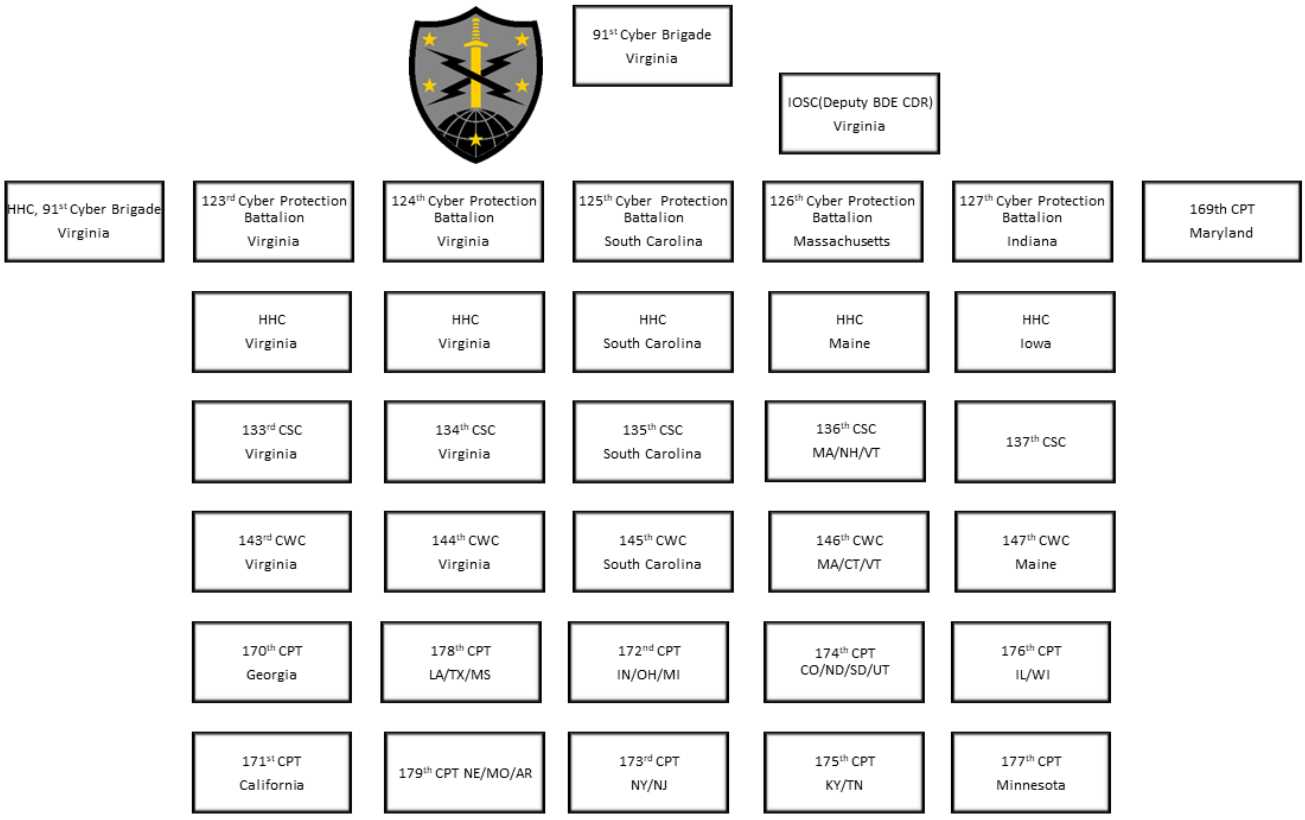

Figure 8. ARNG 91st Cyber Brigade Organizational Chart (Source: (91st Cyber Brigade)

---

69 CPT units in the ARNG exist as CPTs only when in Title 10 duty status.

70 Alex Ebrahimi, et al., *National Guard Cyber Protection teams as a Response to Cybersecurity Threats*, June 2020.

b. Defensive Cyber Operating Elements (~540 billets of which 380 are filled)[71]

The ARNG has 54 DCOEs (each DCOE has 10 personnel)—one in each U.S. state and territory and one in the District of Columbia. DCOEs conduct DCO–Internal Defensive Measures (DCO-IDM) to secure their state's portion of GuardNet—the ARNG contribution to the Department of Defense Information Network–Army (DODIN-A).[72] DCOEs can be tasked to protect critical state infrastructure and respond to state or territorial cyberspace emergencies as directed by the Adjutant General (TAG) or by the governor. DCOEs do not mobilize for Title-10 missions nor conduct Offensive Cyberspace Operations (OCO). Along with the ARNG CPTs, the DCOEs are among the first ARNG units called to support off-DoDIN actions.[73]

c. Examples of ARNG Cyber Task Forces

Task Force Echo (TFE) is an ARNG Task Force mobilized annually to engineer, install, operate, maintain, and defend critical network infrastructure and conduct cyberspace operations in support of U.S. Cyber Command and the Cyber National Mission Force (CNMF).[74] TFE Rotations last for more than a year and each of the more than 60 TFE work roles have a unique training pipeline to prepare them for their mission requirements.[75]

Figure 9. Task Force Echo Soldiers 2018
(Steven Stover, DVIDS)

The **Kodiak Cyber Operations Team** (KCOT) is another task organized ARNG activity supporting ARCYBER that actually predates the 2010 establishment of ARCYBER. Its unclassified mission is to support combatant commanders and joint task forces global

---

[71] DCOEs are not included as part of the cyber operations force. There are 17 authorized billets for each state, territory, and the District of Columbia (54 units total); however, as of this writing, only 380 were filled and a smaller portion of that number are fully qualified in their military occupation specialty.

[72] According to JP 3-12, Defensive Cyberspace Operations—Internal Defensive Measures (DCO-IDM) is a form of DCO where authorized defense actions occur within the defended network. Most DCO missions are DCO-IDM which include pro-active and aggressive internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses used to eliminate these threats and mitigate their effects.

[73] Official website of the Colorado National Guard.

[74] This mission is concluding after TFE 7, which starts September 2022. ARNG continues to work with ARCYBER to define the next mission.

[75] "Task Force Echo—America's Citizen Cyber Warriors," Steven Stover, U.S. Army website, 1 December 2021.

requirements by conducting information operations, electronic warfare and offensive capabilities and supporting the fielding and operationalization of new capabilities, in an immediate and timely operational response.[76]

2. Air National Guard Cyber Force (~2,400 personnel of which 1,200 are part of the cyber operations force)

a. Cyber Operations Squadrons (~1200 personnel)

A significant portion of the ANG cyber force lies in the 15 COSs (~70 personnel per COS) located in 12 different states. The COSs are an important part of the Air Force's (USAF) contribution to USCYBERCOM's CMF. Twelve of the COSs serve six-month activations in Title 10 status on a rotating basis to provide two continuous full-time USAF CPTs. When activated as a CPT, the COS defends priority DoD networks and systems against significant cyber threats. Three other COSs, each containing two sets of cyber operations that, on the same six-month rotation basis, fill the cyber operations component of one USAF National Mission Team for USCYBERCOM. This defends the U.S. and its interests against cyber attacks and malicious cyber activity of significant consequence.[77]

b. Other Cyber Units (~1200 personnel)

The remaining half of the ANG cyber force is distributed across wing and group headquarters elements, mission support units and units associated with intelligence, surveillance and reconnaissance. Among the missions performed by these other units are active cyber defense of USAF networks, training, test and evaluation, and threat emulation. This grouping also includes mission defense teams who provide cybersecurity defense of USAF weapons systems. These teams are under the authority of local wing commanders and are considered as Service-retained assets outside of the DoD Cyber Operations Force (COF) structure.

---

[76] Volant, "Army National Guard–Cyber Brigade," AFCEA Industry Day presentation, slides 22–26.

[77] Guthrie, et al. *The Air National Guard Cyber Force*, 2-1, Appendix A.

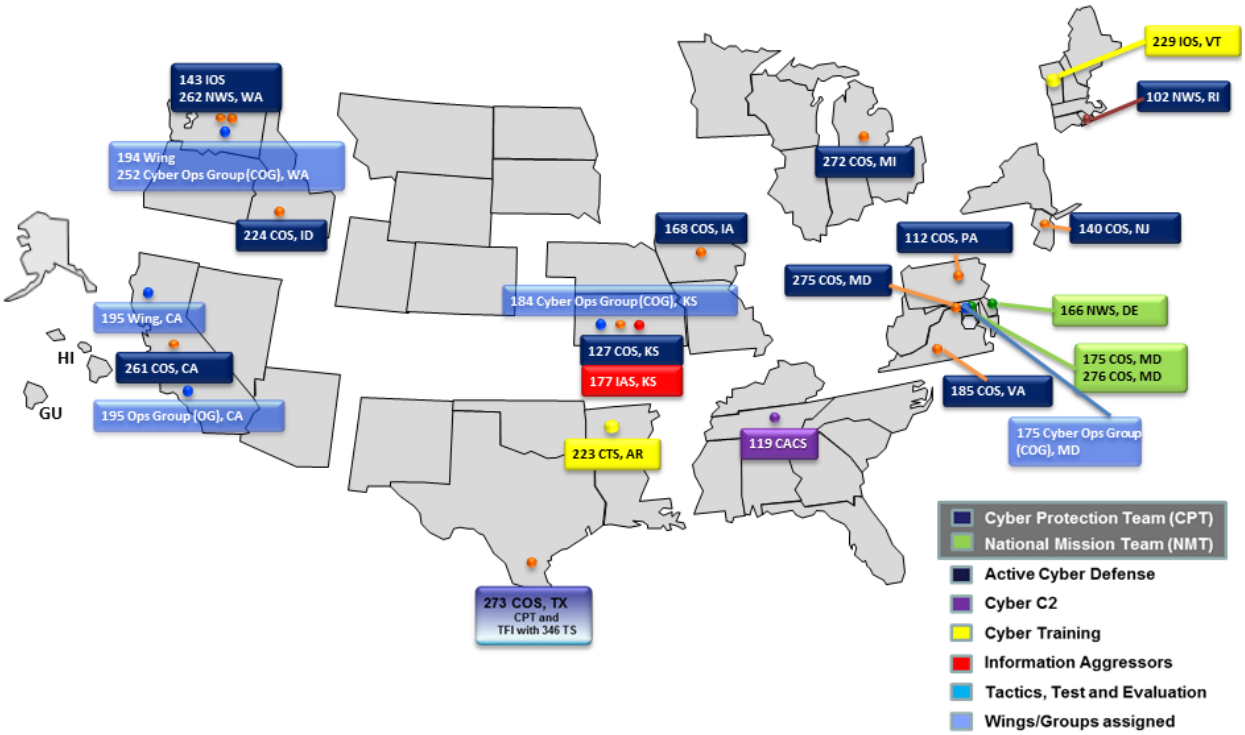

Figure 10. Distribution of ANG Cyber Forces

3. USCYBERCOM Cyber Mission Force

The CMF is the portion of the COF that, when activated in the case of National Guard cyber forces, are under the command of USCYBERCOM and are tasked with executing DoD's Title 10 missions in cyberspace. Comprised of active, reserve and ANG personnel, the CMF is principally oriented on defending federal assets and conducting offensive operations. There are no ARNG cyber units assigned to the CMF. It consists of the following three elements and associated entities:

- **Cyber National Mission Force** conducts cyberspace operations to defeat cyberspace threats to the DoDIN and, when ordered, to defeat significant cyberspace threats to the nation. The CNMF includes mission teams and support teams. There are 13 National Mission Teams (NMTs) in the CNMF. The ANG maintains three Cyber Operations Squadron (COS) of ~70 persons each in order to fulfill standing six-month long rotations of a portion one of the NMTs (~40 percent of a total NMT).
- .**Cyber Protection Force** conducts CO for internal protection of the DoDIN or other blue cyberspace when ordered. The CPF includes six DoDIN CPTs and the ANG maintains 12 COS that fulfill standing 6-month rotations of two of the CPTs. The ARNG has established 11 CPTs that could contribute to the CPF mission.
- **Cyber Combat Mission Force** conducts CO to support the missions, plans, and priorities of the geographic and functional combatant commanders. No National Non-CMF Aligned National Guard Forces

4. Non-CMF Aligned National Guard Forces

The ARNG and the ANG maintain COF units that are not aligned with the CMF, meaning their missions do not directly support USCYBERCOM. The ANG forces include various cyber mission support units and intelligence, surveillance and reconnaissance (ISR) units. These are Service-aligned entities who perform duties including training and testing and threat emulation. The ISR units conduct cryptologic and signals intelligence activities in support of cyber operations. There are ~1,180 Air Guard members assigned to these units.

The ARNG's entire force structure is not aligned with the CMF; however, the ARNG includes 11 CPTs that could contribute to CMF taskings despite not being aligned. The ARNG also includes the DCOE described previously in this chapter.

5. Non-COF National Guard Forces

The ANG maintains Mission Defense Teams (MDTs) that provide cybersecurity defense of USAF weapons systems. These teams are under the authority of local wing commanders and are considered as Service-retained assets outside of the DoD COF structure.

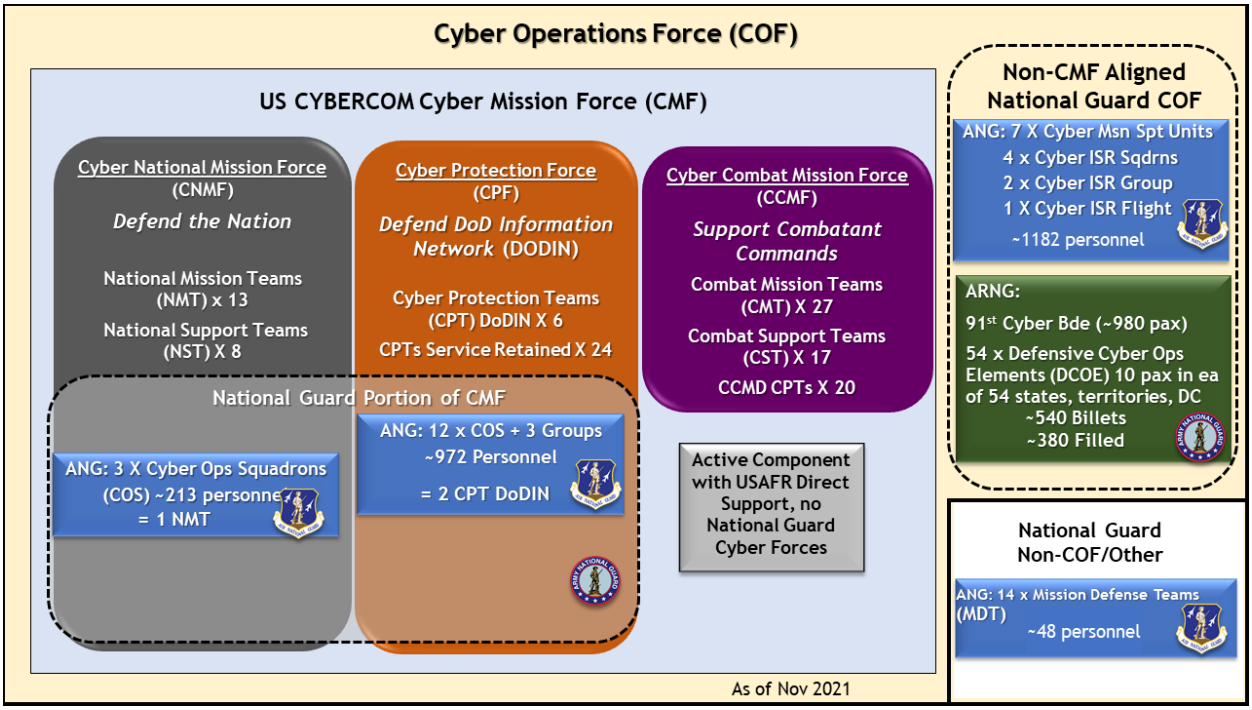

Figure 11. Alignment of National Guard Cyber Forces[78]

[78] Guthrie, et al. *The Air National Guard Cyber Force*, 2-1, Appendix A.

B. Unique Attributes and Cyber Skills of the National Guard

As indicated by the structure of the National Guard Cyber Operations Forces and beyond, the inherent strength of the National Guard is its dual state and federal missions and statuses. In addition to the ability to support both federal and non-federal missions, Guardsmen have a unique set of cyber skills that bridge their civilian and military responsibilities—also termed the "hybrid benefits" of the National Guard in a 2019 article by cyber security experts—that are foundational to National Guard cyber professionals (Figure 12).[79]

Figure 12. Unique Aspects of National Guard Cyber Personnel

Pairing civilian skills such as industry certifications, with military skills like security clearances and knowledge of adversarial tactics, techniques, and procedures, combined with hybrid understanding of operating system environments, make Guardsmen uniquely positioned to respond in both DoD and non-DoD-owned cyberspace. These skills are crucially combined with relationships Guardsmen establish with public and private partners by being members of the communities they serve. In turn, these relationships build the trust critical to information sharing and an effective cyber response. Through interviews, Guardsmen repeatedly indicated these relationships were a key contribution that National Guard cyber professionals add to the national cyber response, particularly to Title 32 missions that bridge the public-private gap.

---

[79] Monica M. Ruiz and David Forcey. "The Hybrid Benefits of the National Guard," *Lawfare* (23 June 2019).

Figure 13. Partial List of Public and Private Civilian Employers of Washington Air Guard Cyber Personnel[80]

While multiple interviewees expressed no difficulty retaining cyber talent once in the National Guard, both the elite industry/military skills and these relationships take years to build and train, and the ability to recruit and train these skills is uneven across the 54 states and territories due to clusters of talent in certain parts of the country.

Throughout our interviews and research, the IDA team attempted to understand whether the historically limited usage of the National Guard in Title 32 status was a result of the difficulty applying existing authorities to the cyber domain, differences in interpretation of these authorities, the scope of the authorities, the nature of cyber incidents, or a combination of some or all of the above. As we dove into specific examples of National Guard cyber activities on non-DoD-owned cyberspace, we began to understand the limitations on Title 32 usage based on existing statute and the increasing off-DoDIN demand for National Guard cyber support (see Chapter 3).

When putting together a team for a mission on non-DoD-owned cyberspace, preparedness varies on a state-by-state basis. Many commanders have a short list of individuals with special skills applicable to cyberspace missions, and their relationships with network owners and operators as applicable. They will call these individuals and inquire about their availability for the mission, which typically occurs during two to three days and comprises initial incident assessment, triage, and reporting. This is almost always done in SAD status.

---

[80] Washington Air National Guard, 252nd Cyberspace Operations Group

Should the mission take longer, the commander will often rotate Guardsmen because staffing is on a volunteer basis; the commander can sustain this for ~2–3 weeks maximum. Longer missions are rare due to resource constraints.

While there is little difficulty in retaining cyber talent, and often cyber teams are perceived as high-performing contributors to critical missions, recruiting for specific missions can be challenging. Because most rapid response missions occur in SAD due to increased flexibility and the need for faster response times, the limited duration use of SAD and lower pay and benefits relative to federal missions makes SAD cyber missions more challenging to execute depending on the timing of the mission. If a state does not have a large budget for such missions, the breadth and depth of the National Guard's ability to mitigate and help entities recover from a cyber incident are limited. If an incident follows others earlier in the year, this also hampers recruiting. The same day jobs that give the National Guard the unique skillsets and relationships that are so crucial to effective cyber response are the jobs Soldiers and Airmen are being asked to leave, sometimes taking a pay cut. The discrepancies in pay, access, and benefits to National Guard of operating in SAD rather than Title 32 could damage recruiting and retention in the long term if a balance cannot be struck between support to federal and non-federal missions. (A previous IDA study cited manpower logistics and continuity challenges of maintaining an activity over an extended timeframe with manpower available only on a part-time basis.[81])

No clear path forward yet exists to employ the Guard's unique skills and capabilities to respond to off-DoDIN cyber incidents to the benefit of federal government, state governments and entities, and individual Service members.

C. National Guard support off-DoDIN

When considering the Guard's off-DoDIN cyber activities, there is an immediate need to avoid competing with private entities that provide goods and services for cyber security and defense as well the tendency for local National Guard cyber experts to become the go-to responders to cyber incidents for state, local, tribal and territorial governments (see Chapter 2). This has limited authorizing Title 32 support in the past and will continue to drive DoD's views on the matter.

The following is a list of what National Guard cyber support could look like, and can be broken down into the five functions of NIST's Cybersecurity Framework (Figure 14).

[81] Strickland et al. *Cyber Models for the National Guard*.

Figure 14. Five Functions of the NIST Cybersecurity Framework[82]

- **Identify**—"assist in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities"[83]
  - Vulnerability Assessments
  - Threat identification
  - Risk management strategies
  - Coordinated actions planning
- **Protect**—"outlines appropriate safeguards to ensure delivery of critical infrastructure services [and] supports the ability to limit or contain the impact of a potential cybersecurity event"[84]**Detect**—"activities to identify the occurrence of a cybersecurity event. Enables timely discovery of cybersecurity events."[85]
  - Detect anomalies and events
  - Continuous security monitoring capabilities
  - Maintaining detection processes
  - Information sharing
- **Respond**—"actions taken regarding a detected cybersecurity incident."[86]
  - Ensuring response planning processes are executed during and after an incident
  - Communications planning (with stakeholders, law enforcement, State CIOs, DHS CISA)

---

[82] Graphic from National Institute of Standards and Technology, The Five Functions.
[83] National Institute of Standards and Technology, The Five Functions.
[84] National Institute of Standards and Technology, The Five Functions.
[85] National Institute of Standards and Technology, The Five Functions.
[86] National Institute of Standards and Technology, The Five Functions.

- Analysis to ensure effective response and support recovery activities including forensic analysis and determining the impacts of the incident
- Mitigation activities to prevent expansion of an event and resolve the incident

- **Recover**—"identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity"[87]
  - Implementation of improvements based on lessons learned from current and previous detection and response activities
  - Advise on best processes and procedures to speed recovery

A notional set of characteristics for a National Guard cyber incident response could include:

- **Few people—**Cyber incident response does not always require a large number of personnel like those required for other domestic operations, such as natural disaster response. These are small teams that deploy with specialized equipment and knowledge.
- **Doing exquisite things**—These are the exquisite skills and knowledge that are the hybrid of military training and civilian work experience and certifications. Notably, these abilities may come in the form of "shoulder surfing" and in an advisory capacity that does not involve direct interactions with non-DoD systems.
- **Ad hoc**—Given the nature and severity of cyber incidents, such as ransomware, the responses are ad hoc and tailored to each incident.
- **Limited duration**—Responses are usually measured in hours and days and are not long-term commitments for NG personnel and resources.
- **Low cost, but precedent setting**—While the one-time incident response may be low cost, it is the cumulative effects of the demand for personnel time (away from their civilian and military duties) and the expectation that the NG will be available in the future and more frequently that may set a precedent.

D. Other Considerations

The first thing to consider in the scope and extent for future Title 32 National Guard support off-DoDIN is the nature of coordinating Guard activities. The National Guard Bureau coordinates policy but doesn't control forces. It is the channel of communication to the Air Force and Army on all matters relating to the National Guard. The Chief of the National Guard Bureau is a member of the Joint Chiefs of Staff. DoD owns the Title 10 missions and trains and equips National Guard personnel to support those missions. Title 32 authorizations

[87] National Institute of Standards and Technology, The Five Functions.

and reimbursements must come through DoD (OSD), as in the case of Chapter 9 homeland defense activities as previously discussed. However, the personnel themselves fall under a governor's control unless they are federalized (i.e., in a Title 10 duty status).

The capabilities that National Guard cyber professionals gain as part of their cyber mission occupational specialty training are available for non-federal use in the states. The IDA team found that while much of the cyber activity support to the states is reported back to the Bureau to capture as metrics, increased or unreported demand and use of Guard cyber personnel may go unreported and unmeasured, thus it is difficult to accurately portray supply and demand for off-DoDIN support.

There are also alternatives to or complications to the Guard's capacity to support these activities. IDA heard through interviews that some states, such as Virginia with its Virginia Defense Force, can also use their state militias for cyber incident responses. A more widespread adoption of this model could ease the burden of response during heightened demand, such as elections and ransomware incidents in multiple locations. However, all stakeholders—DoD active duty forces, the National Guard, state militias, state/local governments and private network operators—compete for the same pool of cyber talent.

In addition, states with access to cyber talent through the Cyber Protection Teams may not always have them available for cyber responses. The requirements of their training and deployment cycles may mean that they are out-of-state (or just mobilized in place and not available) in support of national missions when a major cyber incident impacts their home state. In that case, states would have to look to existing signed agreements for support from neighboring states—known as Emergency Management Assistance Compacts[88]—to assist with the response.

E. Implications for National Guard Title 32 activity on non-DoD-owned cyberspace

The National Guard still faces numerous challenges to employing its unique skills to address the growing demand for cyber support across the country. The National Guard cyber force is organized, trained and equipped to support Title 10 missions, but the inherent strength of the National Guard is its dual state and federal missions. Not only are National Guard cyber units limited in their ability to respond to non-federal missions in cyberspace, but states and localities will be the main drivers of future demand. Given these limited capacities, there is no consensus on how to employ National Guard skills to simultaneously benefit federal, state, and local governments.

[88] For more information see www.emacweb.org/index.php/training-education/learn-about-emac-your-discipline/national-guard.

IDA has outlined the subset of skills that are relevant to the cyber activities that National Guard units are called up to do in non-DoD-owned cyberspace. It takes years to train to these skills, and the ability to recruit, train, and retain is uneven across the 54 states and territories. Overuse of these limited resources off-DoDIN could impact their availability for Title 10 missions and could imperil the retention and recruiting largely done at the unit level.

5. Opportunities for National Guard to contribute to Defense of non-DoD–owned Cyberspace

A. Framework for off-DoDIN Actions by National Guard Cyber Force

National Guard actions in non-DoD owned cyberspace are bound by authorities and policies and can be arranged by duty status, event consequence, and time to prepare or respond. Figure 15 compares the relative use of authorities for Off-DoDIN actions by National Guard cyber forces.

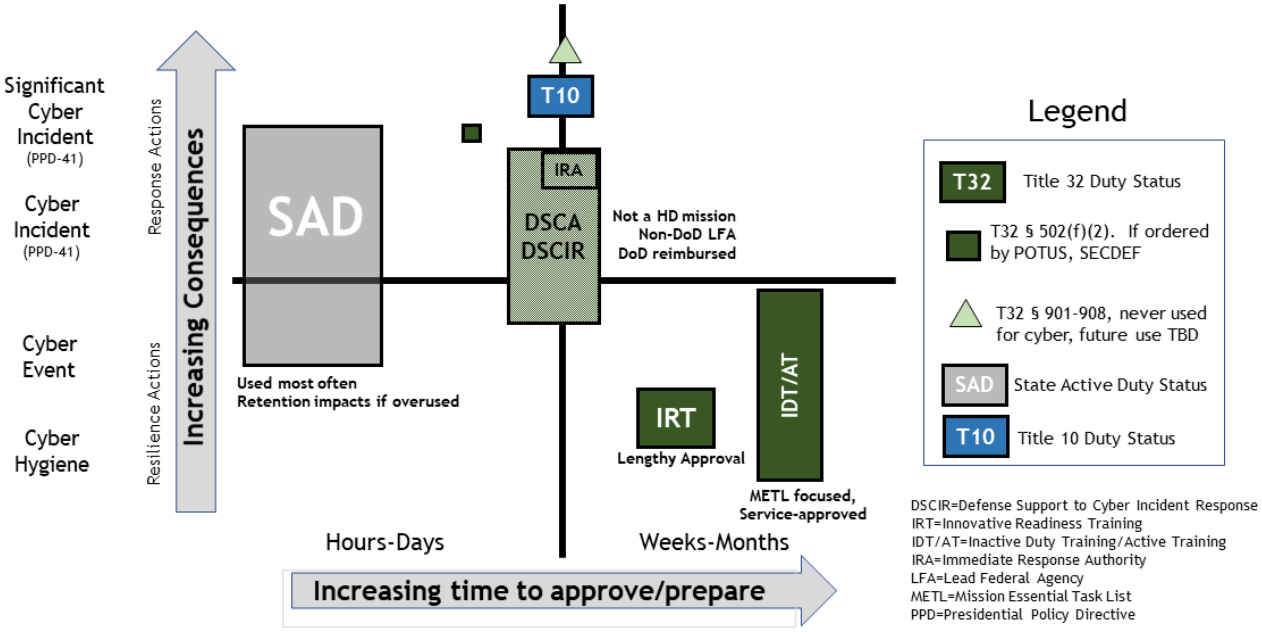

Figure 15. Comparison of Relative Use of National Guard Authorities when Conducting Off-DoDIN Cyber Actions

The horizontal axis is the time to approve a request for National Guard support off-DoDIN and the time for a tasked unit to respond once approval is received. The vertical axis is the possible consequence of the event arrayed form low consequence preventative activities (cyber hygiene) to devastating significant cyber incidents as defined in Presidential Policy Directive 41.

Within each quadrant are the duty statuses and authorities the National Guard uses when acting off-DoDIN. The size of the boxes within the quadrants reflects the relative off-DoDIN use of this particular duty status or authority. For example, SAD is used the

most and is often done for higher consequence events and seldom, if ever, used for cyber hygiene support off-DoDIN. This is because the State Governors control the use of the Guard under SAD and thus own the decision for employing the Guard under SAD.

The positioning and sizing of the quadrant contents is relative, not absolute. While there are exceptions, this figure reflects the responses IDA received from stakeholders interviewed for this project.

The National Guard must have both proper fiscal authority and the mission authority to conduct cyberspace actions while in Title 32. The fiscal authority is derived from Congressional funding of the National Guard's training for their federal mission. Thus, any off-DoDIN training in Title 32 status must build skills and certifications needed to execute the National Guard's federal mission. Training for the federal mission is conducted under Title 32 U.S.C. §502(a) within an existing and published training plan.[89]

Commanders are not limited to computer-based training or exercises on their own systems. Several unit commanders interviewed remarked that the best cyber training range is someone else's network, implying there are limits to the fidelity and outcomes of training on synthetic cyber ranges. Title 32 training authorities can be leveraged to provide support to civil authorities and other statutorily eligible off-DoDIN entities.[90] Units that seek off-DoDIN training events included as part of their Service-level training must plan far in advance in order to secure the required Service-level approval for that training.

Innovative Readiness Training (IRT) is a limited but possible path for off-DoDIN cyber activities. IRT must be approved in advance, the approval process can be lengthy, and the uses of IRT are narrow with many caveats. IRT is authorized only when the military training activities meet the following conditions.[91]

- Meets valid training requirements for the Active, Guard, or Reserve components of the Military Departments; either individual training requirements to achieve and sustain an occupational specialty or collective training requirements to generate and sustain capabilities required by the Combatant Commanders and the Chairman of the Joint Chiefs of Staff.
- Occurs within the United States, its territories, and possessions

[89] Domestic Operations Law and Policy, National Guard Bureau Office of the Chief Counsel, 2nd Edition, 2019, 219.

[90] Domestic Operations Law and Policy, 219.

[91] Traditional IRT consists primarily of medical assistance, road and building construction activity.

- Results in incidental benefit, in the form of support and services to organizations or activities outside the DoD, while addressing a valid and appropriate civic and community need in the particular locale, state, or region, where assistance is to be provided, and does not duplicate other available public services.
- Expends DoD funds, regardless of funding source [92]

DSCA and DSCIR are depicted on the figure though these actions are not homeland defense activities; DoD does not fund them and thus fall outside this research. Immediate Response Authority (IRA) is a tool to fill the initial response gap between the flashpoint of an unforeseen circumstance and marshalling forces or capabilities through other mechanisms such as SAD.[93] IRA falls under DSCA guidance and is therefore outside this research.[94]

National Command Authorities can mobilize National Guard cyber forces in Title 10 status for off-DoDIN support, for example, during a national emergency, though this must be balanced with possible encroachment on *posse comitatus* restrictions governing Title 10 forces.[95] Title 10 Guardsmen can respond to IRA requests in a training status but cannot intentionally be placed in or extended for anyone on orders for the specific purpose of IRA.[96]

Homeland Defense Actions (HDA), 32 U.S.C. §§901–908, are depicted by the small green triangle. As Chapter 3 of this report detailed, there has not been an approved use of HDA for off-DoDIN cyber support. In interviews with various stakeholders, IDA determined an illustrative scenario to guide applicants seeking use of HDA does not exist. In many cases, the likely HDA scenario will approach a national emergency or conflict with an adversary where homeland cyber networks are under increased, debilitating attack. This scenario is just as likely to mobilize Guardsmen in Title 10 status. Nevertheless, IDA recommends that the National Guard continue to work with OSD to identify a plausible HDA scenario and then give that to the states and territories as a guide for future HDA submittals.

The small green square depicts the use of 32 U.S.C. § 502(f), Full Time National Guard Duty-Operational Support (FTNGD-OS). The purpose of FTNGD-OS is to provide the necessary skilled manpower to support existing or emerging requirements under Title 32. Training may occur incidental to performing FTNGD-OS. Guardsmen mobilized in this status may be used for DSCA if the Governor formally requests DSCA support.

---

92 DoDI 1100.24, Innovative Readiness Training (IRT) Support and Services for Eligible Organizations and Activities Outside DoD, 5 May 2020.

93 Domestic Operations Law and Policy, 17.

94 DoDD 3025.18 Defense Support of Civil Authorities (DSCA), 19 March 2018.

95 For a discussion of *posse comitatus,* see appendix D of Eric V. Larson and John E. Peters, *Preparing the U.S. Army for Homeland Security, Concepts, Issues and Options*, Rand Report MR1251, 2001.

96 Domestic Operations and Law Policy, 72.

The National Guard cyber force is most constrained when attempting to respond rapidly, in extremis, to a cyber incident. As the bottom right of Figure 16 depicts, the quadrant where the National Guard authorities best align for off-DoDIN support—when there is ample time to prepare, to integrate the action into a training plan. The bottom right quadrant is where partnership building, response planning actions and unit training occur. There is not an urgent need to act quickly. Actions here are more threat-agnostic, they respond to collective threats across cyberspace and are not focused on any one threat actor. Title 32 duty status is well-aligned for this quadrant. This quadrant is also well-aligned for the limited capacities of the National Guard force where the Guard can focus its scarce resources on those priority networks most important to DoD's mission assurance.

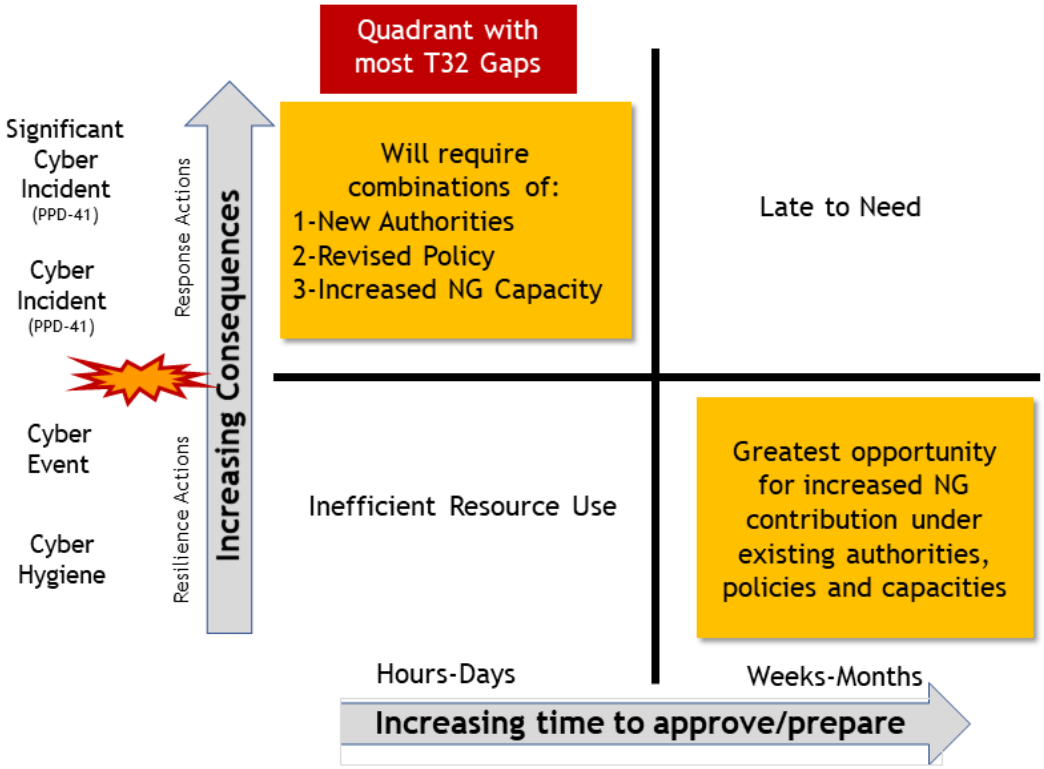

Figure 16. Opportunities and Limitations of National Guard Cyber Force to support Off-DoDIN requests in Title 32 Status

Given the threats and vulnerabilities accruing across national cyberspace, requests for the National Guard off-DoDIN support are likely to grow in the top left quadrant—this is where using DoD-funded Title 32 status is most limited. Expanding the Guard's contribution in this quadrant will require combining new authorities, new policy, and additional forces.

6. Findings and Recommendations

The complex operational environment of the homeland is more challenging in the context of cyberspace that operates according to different rules than the physical world. For example, the speed of cyber reduces concepts like distance. Threats can come from anywhere and from any actor. Cyberspace borders are also marked by routers, firewalls and other gateways—everyone's network is on the border in cyberspace.

Legal and policy frameworks are still maturing in cyberspace. Legal questions remain about balancing the right division of responsibility between governments and the private sector; the line between acceptable and unacceptable actions of governments, companies, and individuals; who maintains responsibility for addressing vulnerabilities and responding to incidents. On the policy front, the landscape is complicated by the fact that the vast majority of cyberspace in the United States is owned and operated by the private sector. Therefore, the U.S. Government does not exercise direct authority over much of domestic cyberspace, and as a result, U.S. Government strategies have focused on information sharing, advocating standards, and motivating the private sector to adopt best practices.

Crucial policies are developing that will help respond to cyber attacks. Given that cyberspace incidents can easily span the concept of homeland security and homeland defense, it is critical to establish roles and responsibilities. For example, a cyber attack can be executed from outside the United States, but its effects can be felt inside. In such a case, it must be determined whether DHS or DoD is responsible for either preventing or responding to such an attack. The findings included here account for the challenging context of cyberspace.

For a summary of the following findings and recommendations, see the matrix in Appendix B.

A. Finding: DoD's cyber focus is on Title 10 mission: military and national security issues in DoD cyberspace

The statutes and policies that enable and limit National Guard activities off-DoDIN are intended to preserve the National Guard's Title 10 ability to execute its Title 10 obligations. DoD's cyber directives, policies, and resources center on preparing for and executing its Title 10 cyberspace operational requirements. This limits the National Guards capability to plan for and execute cyber engagements in non-DoD cyberspace while in Title 32 status. DoD's homeland defense cyber activities and resources are aligned for defending and protecting the DoDIN, the Defense Industrial Base, and Defense Critical Infrastructure. IDA's interviews identified concerns that Guard cyber activities in Title 32

status that do not support a DoD mission or mission requirements could negatively impact the Guard's capability and readiness for its Title 10 missions. DoD funding for Guard activity undertaken in Title 32 duty status aligns with the intended statutory use of Title 32 for training for Title 10 missions. As such, funds have not been generally available for activities off DoD networks undertaken in Title 32 duty status.

DSCA is an important element of DoD's homeland defense mission. DSCA policies are not well suited to the cyber environment: they are not particularly agile or timely, and they structurally constrain cyber incident response in the non-DoD environment. The National Guard's ability to support timely cyber incident response in Title 32 status is further constrained policy and process.

Recommendation 1

Engage DHS/CISA to develop a National Guard Annex to the National Cyber Incident Response Plan and to Joint Publication 3-27, Homeland Defense. A National Guard Annex to the NCIP affords several opportunities: a forum for presenting Guard cyber capabilities and processes; a framework for identifying and developing Guard cyber responsibilities under each of its operational statuses Title 10—Title 32—SAD, and incorporating these into the national cyber framework.

Recommendation 2

The National Guard Bureau can develop and promulgate guidance coordinating and integrating Guard cyber protection and response activities with CISA regional and state-based cyber security advisors. CISA has established and staffed a senior cyber position at each FEMA Regional Headquarters and is working to position a CISA cybersecurity advisor in each state and territory. If the Bureau develops and issues guidance that offers a framework for establishing and sustaining working relationships between the Guard's cyber units and these CISA assets, it would benefit both organizations.

Recommendation 3

Fill critical billets such as the cyber liaison officer at the National Guard's USNORTHCOM office. IDA's interviews identified the National Guard's difficulty staffing critical cyber liaison positions with individuals possessing cyber subject matter expertise and experience. This limits the Guard's ability to fully and efficiently support and participate in some cyber initiatives and activities.

B. Finding: There are limits to the Guard's capacity to respond to cyber incidents

During this project, the study benefited from rapid developments in the level of activity and focus of adversarial cyber activity. During our interviews, the nation experienced

the SolarWinds event, a sophisticated supply-chain attack that affected more than 18,000 customers; the Microsoft Exchange Server Hafnium attack, an event threatened the very backbone of the world-wide email distribution infrastructure; an attack on a municipal water supply that was fortunately thwarted; and an attack on the Colonial pipeline, responsible for almost half of the transportation fuel supply for the East coast, that was not thwarted and resulted in lines at gas stations reminiscent of the oil shock events of the 1970s.

We list these events to reinforce the standard argument that cyber attacks are growing in number, sophistication, and interdependence across sectors. This trend is not lost on state-level government and National Guard leadership. The consensus was that demand for cyber response capability at the state level would continue to grow. This reality was reflected by several state initiatives to create or consider the creation of state cyber response capabilities, i.e., cyber militias, outside of the National Guard structure.

The movement to create state-controlled cyber response forces outside of the National Guard structure was partly driven by the view that the additional cyber capacity in the existing National Guard force structure available to the states was limited. States felt that calling on National Guard cyber forces more frequently to meet the growing demand would result in recruiting and retention problems as the increased operational tempo would create stress between the additional duty and the Guardsmen's employers. The states were clearly aware of the primacy of the Title 10 missions and their associated training and readiness requirements. While some flexibility might exist to leverage this training requirement to address a limited scope of cyber hygiene issues, the training requirement did not align with the reality of most cyber response events.

It is well known that the demand for trained and qualified cyber professionals exceeds the supply. The imbalance exists in public and private sectors and is evidenced by high salaries in the private sector and special hiring authorities in the public sector. A recent survey by (ISC)2 adds evidence of this imbalance showing a shortage of 359,000.[97] While the National Guard is not experiencing recruiting and retention issues, it must remain aware of the trained worker issues. Given its capacity constraints, expanding Guard efforts to meet state cyber demands would likely drive force structure and force allocation decisions within the National Guard and the DoD—adding the challenge of a shortage of qualified individuals necessary to support force structure/allocation changes.[98]

Recommendation 1

Focus National Guard off-DoDIN activities on cyber prevention and protection to maximize utilization efficiency. Given the limited capacity of the National Guard cyber

---

[97] "Cybersecurity Professionals Stand Up to a Pandemic," ISC^2 Cybersecurity Workforce Study, 2020.

[98] The National Guard could also expand its efforts to meet state demands under SAD authorities, but state budget limitations apply.

forces to perform missions outside of their Title 10 roles, it makes sense to efficiently use the existing force. Scheduled events associated with cyber protection and prevention activities allow National Guard units to leverage their planned training efforts while being aware of the demands such activities place on Guardsmen and their employers. Cyber incident response activities can provide valuable training experiences but are by definition unplanned events that present difficulties for the Guardsmen and their employers. Our recommendation includes conducting cyber protection and prevention activities on real-world networks rather than cyber ranges—such experiences provide superior training outcomes and also allow the Guardsmen to build relationships with the owners and operators of critical systems and infrastructure.

Recommendation 2

Work to synchronize cyber efforts with other state and federal resources. While Congress and the current administration have begun to realize that the available resources to address the cyber threat are likely inadequate, most of solutions focus on providing additional resources to CISA in DHS. While DHS and CISA have the lead for protecting critical infrastructure, the National Guard frequently has the relationships and the personnel on the ground to facilitate state-federal cooperation.

Recommendation 3

Improve data collection on National Guard cyber activities to better quantify and characterize state cyber demands to support future planning. As mentioned elsewhere in this report, data describing ongoing cyber efforts at the state level is hard to come by and almost always incomplete. Without better understanding what is going on and what may come, it is difficult to plan a future force appropriate for a response. It is important to better quantify and characterize state cyber demands to support future force planning.

C. Finding: Policy restrictions on employing the National Guard under Chapter 9 of Title 32 restrain off-DoDIN cyber response options

The National Guard's unique relationship with state and local authorities can enhance a state's response to cyber incidents, but past interpretation of Chapter 9 by the Office of the Under Secretary of Defense for Policy has constrained the National Guard's contributions. This research found that the inability to describe attribution or intent in cyber incidents hampers using Title 32 Chapter 9. In nearly all scenarios, fast and efficient coordination between private sector, law enforcement, and the military is key to an effective cyber responses, yet it typically takes time to ascertain an attacker's identity, intention, and the attack's potential impact. Furthermore, the Secretary of Defense's requirement to determine affected infrastructure or assets as "critical to national security" may be conditional, inconsistent, sensitive, or otherwise difficult to obtain.

The research team conducted interviews to better understand the circumstances related to previous Title 32 Chapter 9 requests. Interviewees suggested that state requests to OSD had to meet stringent criteria to qualify for approval: requests could not be a DSCA or DSCA-like activity in support of some other entity. Furthermore, the circumstances must involve an external threat, possibly only a nation-state action, that broadly targets the nation, not a single state. Lastly, there must be a "military-unique" activity to be "military protection." Notably, the IDA team did not identify a single instance of a Chapter 9 request that was approved; in fact, at least three requests for National Guard cyber support were denied.

To meet these challenges, the Guard must obtain clarity from OSD on its criteria governing the use of Chapter 9 if it is to create an approval process, or it must pursue other paths.

Recommendation 1

The National Guard should inform the states that Chapter 9 of Title 32 appears unlikely to be approved for cyber incident response without meeting the stringent approval criteria outlined in Appendix C under existing statute and policy**.** Given the myriad challenges of obtaining a more expansive interpretation under current law, Chapter 9 requests for employment of the National Guard are not a practical tool.

Recommendation 2

If the National Guard seeks to use Chapter 9 of Title 32 for cyber incident response, it should seek either a change in statute, a change in policy, or both. The existing policy sets a high bar for approval and is not conducive to cyber incidents that require timely responses.

Recommendation 3

Enhance the National Guard's communication and coordination with OSD and others. This will ensure that Guard capabilities can be fully utilized when they need to be.

D. Finding: The legislative branch has limited the expansion of DoD's footprint in non-DoD cyberspace.

Congress has limited the expansion of DoD's footprint in non-DoD cyberspace in a number of ways. Historically, Congress has shown little appetite, particularly in a fiscally constrained environment, to expand into non-core mission areas. This is demonstrated by the absence of dedicated funding for Homeland Defense Cybersecurity activities.

Expansion could be accomplished in a variety of ways: defining statutory terms more precisely, clarifying that some cyber activities qualify as "military protection," or expanding the required connection to "infrastructure or other assets…critical to national security" to include mission assurance.

Recommendation 1

The National Guard, in coordination with OSD, should work to enhance the understanding of its cyber capabilities among key Congressional stakeholders. Congressional buy-in on a national-level vision for the National Guard's future roles and responsibilities in cyberspace could help clarify existing statues and policy requirements.

Recommendation 2

The National Guard, in coordination with OSD, should develop a legislative engagement strategy to address the gaps in policy that inhibit its ability to meet present and future demands in cyberspace. This could include re-evaluating the directives and instructions implementing Chapter 9, and revising them as appropriate to address National Guard cyber homeland defense activities (required by §1729 of the FY2021 NDAA).

E. Finding: There is movement in Congress to refine roles and responsibilities in cyberspace.

The recent spate of cyber attacks on public and private sector infrastructure have severely impacted the nation. Those incidents could motivate Congress to act on the job of refining roles and responsibilities in the cyber realm. Consequently, the National Guard, in coordination with the Office of the Under Secretary of Defense for Legislative Affairs, should closely monitor legislative activity and position itself to shape and inform the debate over potential changes in law.

Recommendation 1

The National Guard should demonstrate value by doing the following: Create state-level plans for the Guard's engagement in accomplishing governors' cybersecurity goals; and Develop command and control constructs for responding to domestic cyber incidents.

Recommendation 2

Maintain and update the database of National Guard cyber capabilities. This recommendation is derived from the Government Accountability Office report, *DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises,* GAO-16-574, September 6, 2016.

Recommendation 3

Develop standard measures of effectiveness to show the National Guard's value in cyberspace. While these measures can be difficult to create, they will enhance the Guard's ability to showcase its progress and achievements in cyberspace.

Appendix A: Specified Tasks Cross Reference

This appendix contains the specific tasks the National Guard expected this report to address. It refers to where in this report the detailed response can be found and it includes a summary of that response.

Define the range of mission areas associated with protecting the homeland within the cyberspace domain (referred to hereafter as Homeland Defense cyber mission areas).

See Chapter 1, Section B of this report.

A homeland defense cyber mission area (HDCMA), as referenced in the project description, is not defined in statute, DoD issuances, or joint doctrine. So, in solidifying the focus of this project, IDA narrowed the purview to *National Guard Cyber Forces in Title 32 status, executing cyber actions in non-DoD-owned cyberspace with DoD providing funding for the employment of those forces.*

Joint Publication 3-12 defines cyberspace missions in a variety of ways, to include defensive cyber operations (DCO), offensive cyber operations (OCO), Internal Defense Measures (DCO-IDM), Response Actions (DCO-RA), among others. However, only DCO are permitted in Title 32 status, which narrowed the focus to DCO missions. Further, U.S. Code 32 § 901-908 defines a "homeland defense activity" (HDA) as activities which excludes DCO-RA from authorized missions under Title 32. Since not all HDCMAs are HDAs, the scope narrows further to DCO-IDM.

In exploring the authority structure further, not all cyber actions captured within DCO-IDM are allowed in Title 32 status. Critical to this distinction is the difference between homeland defense and homeland security—DoD is responsible for homeland defense, and is most likely to have to fund the employed forces. Homeland security is the responsibility of DHS, and within this study DSCA is exempt from homeland defense since DoD is reimbursed by the agency requesting DoD support. Within the bounds of DCO-IDM missions, defense cyber actions rarely take place in Title 32 status and are often post-cyber incident, while security cyber actions may fit the definition of Title 32-authorized activities, but are unlikely to be seen as a DoD responsibility. All these constraints combined, the National Guard is unlikely to secure approval for activity in defense of the DoD Information Network (DoDIN), but may be suited to filling the cybersecurity gap in defending the off-DoDIN cyberspace referred to in joint doctrine as DoD associated cyberspace. Thus, IDA oriented its research on National Guard Title 32 support to non-DoD-owned cyberspace, not National Guard expanded support to the DoDIN.

Within non-DoD-owned cyberspace, there exist critical DoD dependencies in "DoD associated cyberspace," the defense of which can be considered a DoD responsibility, and could require military-unique cyber capabilities post-incident, all of which would be a theoretical fit for Title 32 Chapter 9 authorization. This is the critical intersection the IDA research explores.

Specific to Title 32, review and index existing authorities, policies, and directives that apply to Homeland Defense cyber mission areas.

See Chapters 1, 2, and 3.

Identify existing and potential demands for National Guard Cyber Force capabilities in support to Governors or the Secretary of Defense through coordination with combatant commands (USNORTHCOM, USCYBERCOM, USINDOPACOM), the Department of Homeland Security, State and Territorial governments, and others as applicable.

See Chapters 2 and 4.

Demands for the National Guard to support non-DoD–owned cyberspace are symptomatic of cyber threats that are growing across sectors in the United States. IDA research revealed that demand exceeds current National Guard capacities, so the National Guard cyber force can contribute but cannot solve the broader gaps. Following a cyber incident, cyber network owner operators are the first line of cyber defense, but many have limited capabilities and capacities. Further, security standards applied across and within these different networks vary greatly.

When ordered, military cyberspace forces may defend any U.S. or other blue cyberspace. Activities span the range of prevention, detection, response and recovery, most of which happens off-keyboard. The support is generally provided to state and local governments, private enterprises, and critical infrastructure owners. The fact that this support occurs in SAD is critical to IDA's findings.

Identify the attributes and capabilities of the National Guard Cyber Force that are relevant to current and potential Homeland Defense cyber mission areas.

See Chapter 4.

Several key attributes of the Guard make it a unique actor in cyberspace:

- National Guard cyber units and personnel blend civilian and military cyber skills;
- The National Guard has unique relationships with network owners/operators in non-DoD-owned cyberspace;

- The National Guard can operate in Title 10, Title 32, and SAD status, which provides needed flexibility to decision-makers.

The National Guard has the capabilities, but limited capacity, to support future demand in non-DoD-owned cyberspace. The National Guard cyber force is small in number, and an even smaller set have both the skills and availability required to respond to a mission at any given time. Additionally, with few exceptions, Title 10 missions are the *raison d'etre* for the National Guard cyber force, making it difficult to secure approval for homeland defense cyber activities in Title 32 status. The state cyber units that IDA interviewed have a limited capacity for quick responses to cyber incidents due to their dependence on SAD status. This is exacerbated by the Guard's cyber force being unevenly spread across the 54, although EMACs help somewhat. Where any true elastic capacity exists is *before* a cyber incident, in planning, exercises, and relationship-building.

Identify potential gaps in the National Guard's ability to exercise authorities and capabilities in meeting present and projected Homeland Defense cyber mission areas

See Chapters 5 and 6.

Efforts to increase National Guard cyber homeland defense fall into two key areas: response actions to cyber events in the immediate aftermath, and preparatory resilience actions before an incident, including cyber hygiene and minor cyber event response.

It is unclear the extent to which short-term response to cyber incidents is DoD's responsibility, and this in part explains a lack of approval of Title 32 Chapter 9 state requests. Filling gaps in this key area will require combining new authorities, revised policy, and increased National Guard capacity.

The greatest opportunity for increasing the Guard's contribution under existing authorities, policies, and capacities is in resilience actions. This does not cover homeland defense activities as outlined in Chapter 9, but does include other Title 32 Duty Status authorities, including Inactive Duty Training/Annual Training and Innovative Readiness Training.

Identify and assess options for revisions to authorities and capabilities to better align the National Guard to support Homeland Defense cyber mission areas.

See Chapter 6.

Options for revisions to authorities include:

- For 502(f), securing DA/DAF approval for METL revisions that nest with activities in non-DoD-owned cyberspace;
- Work with OSD to define any use cases for Title 32 Chapter 9, and publish this information for the states; and
- Forge tighter links to mission assurance and DoD-affiliated cyberspace.

Options for revising capabilities and capacities include:

- Develop metrics and messaging to fully articulate capabilities and limits of existing capacities, such as
  - Consider developing cyber response handbooks to be shared across states[99]
  - Foster a more robust partnership with the Army Cyber Institute to broaden and deepen the Jack Voltaic exercise program
  - Maintain an inventory of National Guard cyber capabilities available to support non-DoD-owned cyberspace[100]
- Meet IOC/FOC requirements of all existing units, assess cyber force growth ceiling across the 54
- Fill critically-leveraged AGR billets, especially the cyber liaison inside the National Guard USNORTHCOM Office
- Continue to leverage State Partnership Programs to promote exchange of information regarding threats, indicators and warnings
- Examine the uneven gaps in capabilities-capacities across the 54, and develop collaborative structures to smooth those capability-capacity gaps. Perhaps consider assigning U.S. regions to high-capability National Guard units in states such as Washington and Virginia.

Provide a draft final report that enumerates and assesses a range of options the National Guard might pursue in improving the alignment of its authorities, policies, and directives with current and projected cyber capabilities.

This report is submitted in response to this tasking.

Provide information and materials to the National Guard Studies Program (NGSP) program office to assist in their oversight and support to this National Guard study.

IDA provided monthly status reports to the National Guard throughout this project.

Provide study Outbrief to NGB Senior Leaders, within 90 days after delivery of the final report.

IDA outbriefed various NGB leaders on 15 July 2021 and 27 September 2021. IDA outbriefed the NGB Cyber General Officer Advisory Council on 10 December 2021.

---

[99] Recommendation also found in Franklin D. Kramer and Robert J. Butler, "Cybersecurity: Changing the Model," *Atlantic Council*, April 2019.

[100] Kramer and Butler, "Cybersecurity:…"

Appendix B: Findings and Recommendations Matrix

Findings	Recommendations
A. DoD's focus is on T10 missions—military and national security issues in DoD cyberspace.	1. Engage with DHS/CISA to develop a National Guard Annex to the National Cyber Incident Response Plan (NCIRP). 2. NGB develop and promulgate guidance coordinating and integrating Guard cyber protection and response activities with CISA regional and state-based cybersecurity advisors. 3. Fill critical billets such as the cyber liaison officer at NG's NORTHCOM office.
B. Based on interviews conducted, there are limits on the National Guard's capacity to respond to cyber incidents on non-DoD-owned cyberspace.	1. Focus National Guard off-DoDIN activities cyber on prevention and make effective use of the National Guard's available cyber capacity. 2. Work with states to synchronize state cyber efforts with National Guard cyber force and other state and federal resources, including working with local critical infrastructure operators. 3. Better quantify and characterize state cyber demands.
C. Policy restrictions on employing the National Guard under Chapter 9 of Title 32 are too limiting for cyber incidents.	1. Inform the states that Chapter 9 of Title 32 appears unlikely to be approved for cyber incident response without a change in either statute or policy. 2. If the National Guard seeks to use Chapter 9 of Title 32 for cyber incident response, it should seek either a change in statute, a change in policy, or both. 3. Enhance Guard communication and coordination with OSD and others to ensure that NG capabilities can be fully utilized during a cyber incident.
D. The legislative branch has limited the expansion of DoD's footprint in non-DoD cyberspace.	1. Work, in coordination with OSD, to increase understanding of NG cyber capabilities with key stakeholders in Congress. 2. Develop, in coordination with OSD, a legislative engagement strategy to address the gaps in policy that inhibit its ability to meet current and projected demands in cyberspace.
E. Looking ahead, there is movement in Congress to further refine roles and responsibilities in cyberspace.	1. The National Guard can demonstrate value by creating state-level plans for accomplishing governors' cybersecurity goals; developing C2 constructs for responding to domestic cyber incidents; and expanding pilot programs to enhance NG domestic cyber protection efforts. 2. Maintain and update database of NG cyber capabilities (DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises, GAO-16-574, Sept. 6, 2016). 3. Develop standard measures of effectiveness to show National Guard's value in cyberspace.

Appendix C: Homeland Defense Activity Review Process, as Provided by DoD Directive 3160.01, "Homeland Defense Activities Conducted by the National Guard"[101]

Step 1: Governor's Request

- Governor submits written request for homeland defense activity funding prior to the anticipated date of a planned homeland defense activity, as defined by §901 of Title 32, U.S. Code.[102] The requests will include:
  - The specific intended homeland defense activities.
  - An explanation of why participation of National Guard units or members is necessary and appropriate.
  - A certification that the activities will be conducted at a time when the units or members to be involved are not in Federal service.

Step 2: DoD Executive Secretary Task Request

- Upon receipt, DoD Executive Secretary tasks Office of the Assistant Secretary of Defense (OASD) for Homeland Defense and Global Security (HD&GS), in coordination with specified offices of coordinating responsibility, to provide the Secretary of Defense with a recommended response.
- Normally, the Secretary of Defense approves the response and the ASD(HD&GS) signs the response.

Step 3: ASD(HD&GS) Review of Governor's Request

- **Step 3.a (Homeland Defense Activity)**: Consult with the Office of the Secretary of Defense Office of General Counsel (OGC) to determine if the request conforms to the statutory definition of a homeland defense activity in § 901 of Title 32, U.S.

---

101 Office of the Assistant Secretary of Defense for HD&GS

102 The term *homeland defense activity* means an activity undertaken for the military protection of the territory or domestic population of the United States, or of infrastructure or other assets of the United States determined by theSecretary of Defense as being critical to national security, from a threat or aggression against the United States.

Code. If no, recommend that the Secretary of Defense disapprove the request; if yes, proceed to Step 3.b.

- **Step 3.b (Threat):** Consult with the Office of the Under Secretary of Defense for Intelligence (OUSD-I) to determine whether there is an actual or credible homeland defense threat to the United States. If no, recommend that the Secretary of Defense disapprove the request; if yes, proceed to Step 3.c.
- **Step 3.c (Infrastructure or Assets):** Does the request involve the protection of infrastructure or assets? If no, proceed to Step 3.d; if yes:
  - Determine whether the Secretary of Defense has previously identified theinfrastructure or asset in question as critical to national security; or
  - Determine whether to recommend that the Secretary of Defense identify the infrastructure or asset in question as critical to national security.
- **Step 3.d (Compliance):** Consult with OGC to determine if the request complies with Federal laws and regulations. If no, recommend that the Secretary of Defense disapprove the request; if yes, proceed to Step 3.e.
- **Step 3.e (Necessary and Appropriate):** Consult with OGC, OUSD for Personnel and Readiness (P&R), the National Guard Bureau (NGB), and the applicable Combatant Commander (CCDR) to determine if the homeland defense activity is necessary and appropriate for National Guard participation. Also, consult with the applicable CCDR to determine the compatibility of the requested homeland defense activities with military operations ongoing within their respective areas of responsibility (AORs). If no, recommend that the Secretary of Defense disapprove; if yes, proceed to Step 3.f**.**
- **Step 3.f (Training and Readiness):** Consult with OUSD(P&R), the Joint Staff, the Army, and the Air Force to determine that performance of the requested homeland defense activity does not:
  - Adversely impact the training or readiness of a member or unit of the National Guard to perform the military functions of the member or unit.
  - Degrade the military skills of the members of the National Guard performing the activity.
  - Adversely impact the preparedness of the total National Guard force.

  If the requested homeland defense activity has any of these adverse impacts, recommend that the Secretary of Defense disapprove the request; if the requested homeland defense activity has none of these adverse impacts, recommend that the Secretary of Defense approve the request.

Step 4: ASD(HD&GS) Develop and Staff the Response

- Based on the results of the review in Step 3, ASD(HD&GS) develops and staffs the recommended response with OCRs required by DoD Executive Secretary.
- When staffing is completed, ASD(HD&GS), through USD(P), provides the recommended response to the Secretary of Defense. If an OCR has dissenting views, ASD(HD&GS) includes these views in the recommendation provided to the Secretary of Defense.

Step 5: Secretary of Defense Decision

- The Secretary of Defense considers the recommendation, including any dissenting views, and makes a decision.

Step 6: The Response

- Unless the Secretary of Defense has decided otherwise, ASD(HD&GS) signs the response and sends it to the requesting Governor (note: the Secretary of Defense has approved ASD(HD&GS) signature of the response for every request received to date).

Appendix D: Related Prior IDA Research

The research presented in this report builds on recent cyber-related research projects IDA has conducted for the National Guard, including the following.

Cyber Models for the National Guard, 2018–20

The objective of the study was to analyze potential models for the use of National Guard cyber capabilities under Title 32. It found that the National Guard is well-positioned to contribute to homeland defense missions under Title 32, but within the constraints of activities authorized by SECDEF for use of the National Guard in Title 32 status. Illustrative models and frameworks for National Guard cyber contributions under Title 32 include

- Defense Support of Civil Authorities—for cyber support to state, local, tribal and territorial (SLTT) governments and critical infrastructure
- Cyber Mission Assurance Team—dual-use domestic/DoD mission assurance;
- Cyber Civil Support Team—state-based reserve for state response;
- Weapons of mass destruction Civil Support Team—dedicated, full time National Guard cyber support to states;
- Counter-drug model—DoD funding for state-based programs;
- Federated intelligence model—reach-back support to combatant commands;
- DHS Protective Security Advisor—DHS funding to National Guard focused on counterterrorism and counter-improvised explosive device.

The report recommended leveraging the National Guard's unique positioning integrated between SLTT and national security infrastructures, and to augment homeland security capabilities and capacities by seeking more partnership with DHS. It also pointed out that national and DoD cyber strategies omit National Guard roles or DoD-resourced Title 32 for SLTT, a point that ties directly into the impetus for this study.[103]

[103] W. Thomas Strickland, et al., *Cyber Models for the National Guard,* (Alexandria, VA: Institute for Defense Analyses, 2019).

National Guard Critical Infrastructure Cyber Response, 2018–20

The study aimed to develop a model for assessing critical infrastructure vulnerabilities to cyber attacks. IDA hosted an information-sharing roundtable across federal, state, and private stakeholders; developed a conceptual framework for threat vulnerability and response assessments; and built a dynamic common operation picture for vulnerability and response analysis. It recommended establishing a governance body to oversee and maintain use of the common operation picture.[104]

The Air National Guard Cyber Force, 2016–17

This analytical product assessed the Guard's recruitment and use of cyber talent. It recommended National Guard units work closely with the states and territories on planning and executing state cyber objectives, and collaborate with federal and SLTT to develop needed constructs in cyber command and control. IDA suggested the Guard look for pilot projects that would allow it to demonstrate and enhance its cyber capabilities in an attempt to establish a baseline for those cyber command and control constructs. IDA also recommended the Guard develop measures of performance for cyber units in order to anticipate performance impacts, and develop plans for allocating scarce cyber personnel during a domestic cyber incident. Given the dynamic environment of cyberspace, IDA noted that policies and guidance will and should continue to evolve and shape National Guard roles and responsibilities in this space.[105]

---

[104] Laura A. Odell, Cameron D. DiLorenzo, and Alec C. Wahlman, *National Guard Bureau Critical Infrastructure Cyber Response Framework,* (Alexandria, VA: Institute for Defense Analyses, 2020).

[105] Priscilla E. Guthrie, et al., *The Air National Guard Cyber Force,* (Alexandria, VA: Institute for Defense Analyses, 20170.

Appendix E:References

Laws, Statutes, U.S. Code

Active Guard and Reserve Duty: Governor's Authority 32 U.S.C. § 328 (2006). Administration of Reserve Components 10 U.S.C. Chap 1007 §§10201-10219 (2014). Cybersecurity 6 U.S.C. Chap 6 §§ 1501-1533 (2018).

Analysis for Cyber Operations of Department of Defense. Pub. L. 113-66, 26. December 2013.

Cybersecurity Act of 2015. Division N of Consolidated Appropriations Act of 2016. Pub.L. 114-113, 18 Dec 2015; 129 Stat. 2242.

Defense Production Act of 1950, Pub. L. 81-774, 8 September 1950.

Economy Act of 1932, as amended, 31 U.S.C. § 1535, 48 C.F.R. § 17.502-2.

Homeland Defense Activities [of the National Guard] 32 U.S.C. Chap 9 §§ 901-908 (2018).

John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA 2019). Pub. L. 115-232, 13 August 2018.

- § 1084. Improvement of Database on Emergency Response Capabilities
- § 1651. Pilot Program on Regional Cybersecurity Training Center for the Army National Guard
- § 1653. Study and Report on Reserve Component Cyber Civil Support Teams National Cybersecurity Protection Act of 2014, Pub. L. 113-282, 18 December 2014. National Defense Authorization Act for Fiscal Year 2014 (NDAA 2014), § 933 Mission

National Defense Authorization Act for Fiscal Year 2017 (NDAA 2017), § 1651 Strategy to Incorporate Army Reserve Component Cyber Protection Teams into Department of Defense Cyber Mission Force. Pub. L. 114-328, 23 December 2016.

National Defense Authorization Act for Fiscal Year 2018 (NDAA 2018), § 1638 Exercise on Assessing Cybersecurity Support of Election Systems of States. Pub. L. 115-91, 12 December 2017, 131 Stat. 1332.

National Guard Bureau 10 U.S.C. Chap 1011 §§ 10501-10508 (2017)

Operations Relating to Defense against Weapons of Mass Destruction and Terrorist Acts 10 U.S.C. § 12310 (c)

Required Drills and Field Exercises 32 U.S.C. §§ 502(a), 502(f) (2006)

Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988, as amended, Pub. L. 100-107, 42 U.S.C. Chap 68, §§ 5121-5208.

Support and Services for Eligible Organizations and Activities Outside Department of Defense 10 U.S.C. § 2012 (1998)

Unified COCOM for Cyber Operations 10 U.S.C. § 167b (2017)

Use of Army and Air Force as Posse Comitatus 18 U.S.C. § 1385 (1994) Congressional Testimony

United States Congress. House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation Holds Hearing on State and Local Cybersecurity Challenges. 116th Cong. D753, 25 June 2019.

United States Congress. House Appropriations Subcommittee on Defense Holds Hearing on Reserve Components. 116th Cong. D297, 26 March 2019.

Presidential Documents

President of the United States. "Homeland Security Presidential Directive - 5 (HSPD-5). Management of Domestic Incidents." 28 February 2003.

President of the United States. National Cyber Strategy of the United States. September 2018.

President of the United States. National Strategy to Secure Cyberspace. February 2003. President of the United States. National Security Strategy of the United States of America. December 2017.

President of the United States. "National Security Presidential Memorandum - 13 (NSPM-13). Offensive Cyber Operations." 2018.

President of the United States. "Presidential Decision Directive—39 (PDD-39), U. S. Policy on Counterterrorism." 21 June 1995.

President of the United States. "Presidential Policy Directive - 8 (PPD-8). National Preparedness." 30 March 2011.

President of the United States. "Presidential Policy Directive-21 (PPD-21). Critical Infrastructure and Resilience." 12 February 2013.

President of the United States. "Presidential Policy Directive-41 (PPD-41). US Cyber Incident Coordination." 26 July 2016.

President of the United States. Unified Command Plan (UCP) 2017. Amended 24 May 2019.

Department of Defense Documents

"Business Case Analysis for a Washington Air National Guard Cyber-to-Physical Systems Center of Excellence." Undated.

Chairman of the Joint Chiefs of Staff. "Joint Publication 3-12 (JP 3-12) Cyberspace Operations." 8 June 2018.

Chairman of the Joint Chiefs of Staff. "Joint Publication 3-27 (JP 3-27) Homeland Defense." 10 April 2018

Chairman of the Joint Chiefs of Staff. "Joint Publication 3-28 (JP-3-28) Defense support of civil authorities." 29 October 2018.

Chief, National Guard Bureau Instruction 2000.01C. "National Guard Intelligence Activities." 14 August 2018.

Chief, National Guard Bureau Instruction 3000.04. "National Guard Bureau Domestic Operations." 24 January 2018.

Chief, National Guard Bureau Instruction 3100.01A. "National Guard Counterdrug Support." 22 June 2015.

Chief, National Guard Bureau Instruction 3501.00. "Weapons of Mass Destruction Civil Support Team Management." 8 July 2014.

Chief, National Guard Bureau Instruction 6001.00. "National Guard Bureau Cybersecurity Program." 28 February 2017.

Chief, National Guard Bureau. "National Guard Bureau Cyber Mission Analysis Assessment." 29 September 2014.

Collins, David L, National Guard -J52. "Cyber Policy Guidance: Coordinate, Train, Advise and Assist Memo." Briefing, United States National Guard Bureau, 3 August 2016.

Consequence Management Program and Integration Office. "Weapons of Mass Destruction Civil Support Teams (WMD CST) Doctrine Handbook." WMD CST Doctrine No. 1-2000. Undated.

Department of Defense. The DoD Cyber Strategy. April 2015.

Department of Defense. Summary: Department of Defense Cyber Strategy. 2018. Department of Defense Directive 1100.20, Support and Services for Eligible Organizations and Activities Outside the Department of Defense, 12 April 2004.
Department of Defense Directive 1322.18. Military Training, 13 January 2009 w. chg 1 23 February 2017.
Department of Defense Directive 3025.18. Defense Support of Civil Authorities (DSCA), 29 December 2010, w. chg 2 19 March 2018.
Department of Defense Directive 3020.40. Mission Assurance (MA), 29 November 2016.
Department of Defense Directive 3160.01. Homeland Defense Activities Conducted by the National Guard, 25 August 2008, w. chg 2 6 June 2017.
Department of Defense Directive 5105.77. National Guard Bureau (National Guard B), 30 October 2015, w. chg 1 10 October 2017.
Department of Defense Directive 5111.13, Assistant Secretary of Defense for Homeland Defense and Global Security (ASD(HD&GS)), 23 March 2018.
Department of Defense Instruction 1215.06. Uniform Reserve, Training, and Retirement Categories for the Reserve Components, 11 March 2014, w. chg 1, 19 May 2015.
Department of Defense Instruction 1322.28, Realistic Military Training (RMT) Off Federal Real Property, 18 March 2013, with chg 1, 13 May 2014.
Department of Defense Instruction 3025.22. The Use of the National Guard for Defense Support of Civil Authorities, 26 July 2013, w. chg 1, 15 May 2017.
Department of Defense Instruction 3300.05, Reserve Component Intelligence Enterprise (RCIE) Management, 17 July 2013.
Department of Defense Instruction 3325.11, Management of the Joint Reserve Intelligence Program (JRIP), 26 June 2015, with chg 1, 6 April 2018.
Department of Defense Instruction 8530.01. Cybersecurity Activities Support to DoD Information Network Operations, 7 March 2016, w. chg 1, 25 July 2017.
Department of Defense. Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense. 21 August 2014.
Deputy Secretary of Defense Memorandum. "Policy Memorandum 16-002, Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities." 24 May 2016.
Deputy Secretary of Defense Memorandum. "Directive-Type Memorandum (DTM) 17- 007 'Interim Policy and Guidance for Defense Support to Cyber Incident Response'." 21 June 2017, w. chg 1, 25 May 2018.
Deputy Secretary of Defense Memorandum. "Transition of Policy Memorandum 16-002, 'Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities'." 21 March 2019.
Deputy Secretary of Defense. Letter to the Honorable Mary Fallin, Governor of Oklahoma, and the Honorable Dan Malloy, Governor of Connecticut, Co-Chairs of the Council of Governors, 17 May 2018.
EXERCISE: Version 1.1. Working draft, 27 April 2016.
Hessling, Paul, National Guard B IC LNO. "National Guard Bureau: Federated Intelligence Program (FIP)." Briefing, 16 May 2019.
Kirschner, Timothy and Brian McGarry. "The Federated Intelligence Program at the State Level." *Military Intelligence Professional Bulletin*, vol. 41. no. 3, July- September 2015, 27- 29.
Macias, Vic. "Operation BALTIMORE RALLY Cyber Support to the State." Briefing, Maryland Air National Guard, undated.

McClellan, Wes. “CYBER YANKEE: Academics Brief.” United States National Guard Bureau, undated.
McHahon, Erin. “National Guard Cyber Operations in SAD and Title 32 Status.” Briefing, Office of the Chief Counsel, National Guard Bureau, 24 February 2016.
Pries, Tom. “Washington Military Department Cyber Operations.” Briefing, State of Washington Military Department J-36, 3 July 2016.
Reserve Forces Policy Board, Office of the Secretary of Defense. Report of the Reserve Forces Policy Board on Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force. 19 August 2014.
“Training National Guard Cyber Forces: Effectively Utilizing the National Guard under Title 32.” Information paper, undated.
United States National Guard Bureau. “National Guard Cyber Strategy.” 5 January 2018. United States National Guard Bureau. “National Guard Cyber Strategic Plan.” 9 July 2018.
United States Cyber Command Guard & Reserve Division (GRD). “Training National Guard Cyber Forces: Effectively Utilizing the National Guard Under Title 32.” Information paper dtd 26 April 2019.
United States Cyber Command Guard & Reserve Division (GRD). “Delivering Outcomes Through Cyberspace.” Briefing, undated.
United States National Guard. “Cyber Mission Assurance Team (CMAT) Table Top Exercise 28-29 November 2018 After Action Report.” Undated.
United States National Guard Bureau-J36. National Guard Cyber Domestic Operations Pilot Concept of Operations. Draft dated 2018.
United States National Guard Bureau, Office of the Chief Counsel. 2019 Domestic Operations Law and Policy, second edition, 28 November 2018.
United States National Guard Bureau. 2019 National Guard Bureau Posture Statement.2019.
United States National Guard Bureau. National Guard Cyber Capabilities Based Assessment (CBA) Final Report. 24 March 2016.
United States National Guard Bureau. Fact Sheet: Weapons of Mass Destruction (WMD) Civil Support Team (CST). Nationalguard.mil, current as of December 2017. Accessed 11 April 2020.
United States National Guard Bureau, Fact Sheet: National Guard Cyber Defense Team.
United States Army National Guard. Concept of Operations Army National Guard Computer Network Defense Team (CND-T). June 2015.
United States Air Force Policy Directive 36-21 (AFPD 36-21). “Utilization and Classification of Air Force Military Personnel.” 20 June 2017.
United States Air Force Instruction 90-1001 (AFI 90-1001). “Special Management: Planning Total Force Associations (TFAS). 9 January 2017.
United States Department of the Army. ADP 3-28: Defense Support of Civil Authorities. Headquarters, Department of the Army, February 2019.
United States Department of the Army. Operational and Organizational (O&O) Concept for United States Army Cyber Command (ARCYBER). 25 March 2019.
Unknown. CyberShield 2016: Legal Resource Guide for Domestic Cyber Operations.
Welsh, Gen, Thomas Muehleisen, Toby Ream. *Washington National Guard Concept of Operations (CONOPS) for Domestic Cyberspace Response*. 15 June 2012.

Department of Homeland Security Documents

Federal Emergency Management Agency. National Incident Management System (NIMS); Third Edition, October 2017. United States Department of Homeland Security, October 2017.

United States Department of Homeland Security. National Cyber Incident Response Plan. December 2016.
United States Department of Homeland Security. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. 2013.
United States Department of Homeland Security. National Preparedness System. November 2011.
United States Department of Homeland Security. National Response Framework (NRF). Third Edition, June 2016.
United States Department of Homeland Security. Response Federal Interagency Operational Plan. Second edition, August 2016.

Interagency and Other Government Documents

Commission on Enhancing National Cybersecurity. Report on Securing and Growing the Digital Economy. National Institute of Standards and Technology, Department of Commerce. 1 December 2016. Accessed 12 April 2020.
Council of Governors. "Joint Action Plan for State-Federal Unity of Effort on Cybersecurity." 2014.
Cyberspace Solarium Commission (2020): United States of America Cyberspace Solarium Commission (Executive Summary). Washington, DC. Available online at https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view, checked on 9/22/2020.
Cyberspace Solarium Commission (2020). United States of America Cyberspace Solarium Commission (Final Report). Washington, DC.
Department of Defense and Department of Homeland Security. "Memorandum of Agreement on Critical Infrastructure Mutual Cooperation and Support." 29 September 2017.
Department of Defense and Department of Homeland Security. "Report to Congress: Feasibility and Advisability of Establishing a Reserve Component Cyber Civil Support Team for Each State." Draft, undated.
Fallin, Mary and Dannel Malloy, co-chairs Council of Governors letter to Chairmen and Ranking Members of Senate and House Armed Services Committees, 10 July 2018.
Fallin, Mary and Dannel Malloy, co-chairs Council of Governors letter to Deputy Secretary of Defense, 22 May 2018.
Fallin, Mary and Dannel Malloy, co-chairs Council of Governors letter to Deputy Secretary of Defense and Chief, National Guard Bureau, 13 March 2018.
National Association of Chief Information Officers (NASCIO). "Securing Our Elections: A State and National Perspective." Briefing, 6 September 2018.
National Association of Chief Information Officers (NASCIO). Cyber Disruption Response Planning Guide. April 2016.
National Governor's Association. "State Cyber Disruption Response Plans Issue Brief." July 2019.
"Meet the Threat: States Confront the Cyber Challenge: 2016-2017 National Guard A Chair's Initiative; Memo on State Cybersecurity Response Plans." Undated.
National Guard Bureau, J3 Domestic Operations Vulnerability Assessments Initiatives, Department of Homeland Security National Protection and Programs Directorate, Office of Infrastructure Protection, Protective Security Coordination Division. "Statement of Work." 30 September 2017.

National Institute of Standards and Technology (NIST). "Positioning the National Guard and Civilian Organization to Augment the Cybersecurity Workforce." National Initiative for Cybersecurity Education (NICE) Webinar Series. United States Department of Commerce. 21 June 2017.

National Institute of Standards and Technology (NIST). "Framework for Improving Critical Infrastructure Cybersecurity." Version 1.1. United States Department of Commerce. 16 April 2018.

Robinson, Doug and Srini Subramanian. 2018 Deloitte-NASCIO Cybersecurity Study. National Association of State Chief Information Officers, Deloitte Development LLC, 2018.

United States Government Accountability Office. Report to the Committee On Armed Services, House of Representatives: DoD Training- U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. GAO- 19-362, March 2019.

United States Government Accountability Office. Report to Congressional Committees: Defense Civil Support: DoD Needs to Address Cyber Incident Training Requirements. GAO-18-47, November 2017.

United States Government Accountability Office. Report to Congressional Committees: Defense Civil Support: DoD Needs to Identify National Guard's Cyber Capability and Address Challenge in its Exercises. GAO-16-574, September 2016.

United States Government Accountability Office. Report to Congressional Committees: Civil Support: DoD Needs to Clarify its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents. GAO-16-332, April 2016.

Washington State Legislature, RCW Title 42, Section 42.56.420

Non-Government Documents

"Can the National Guard Help Solve States' Cyber Problems?" Fifth Domain, 22 January 2019. Accessed 23 January 2019.

Carr, Courtney. *Cyber Pre- Thru Post-Incident Working Group Strategic Plan*. Indiana Executive Council on Cybersecurity, September 2018.

Caton, Jeffrey L. *Examining the Roles of Army Reserve Component Forces in Military Cyberspace Operations*. U.S. Army War College Strategic Studies Institute, 2019.

Cimpanu, Catalin. "New US Bill Wants to Create National Guard Cyber Units." Bleepingcomputer, 22 May 2018. Accessed 13 August 2019.

Crowe, Greg. "National Guard Preparing to defend cyberspace for states." Federal News Network, 16 April 2018. Accessed 22 March 2019.

"Cybersecurity Professionals Stand Up to a Pandemic." ISC^2 Cybersecurity Workforce Study, *ISC^2,* 2020.

Davis, George. "'Cyber Warriors' selected to defend critical infrastructure." U.S. Army website, 23 April 2019. Accessed 6 May 2019.

Department of Defense Instruction 1100.24. Innovative Readiness Training (IRT): Support and Services for Eligible Organizations and Activities Outside DoD, 5 May 2020.

Diaz, Jaclyn (2020): U.S. Cyber Agency: SolarWinds Attack Hitting Local Governments. National Public Radio, 12/24/2020.

Duncan, Ian. "City Faced Cyberattacks Amid Chaos and Unrest on the Streets." The Baltimore Sun, 31 July 2015. Accessed 25 September 2019.

Freed, Benjamin. "Ransomware Threat Raises National Guard's Role in State Cybersecurity." StateScoop, 26 August 2019. Accessed 5 September 2019.

Guthrie, Priscilla E. et al. The Air National Guard Cyber Force. Institute for Defense Analyses Document D-8539, 15 September 2017. (Document is FOUO)

Guthrie, Priscilla E., Barth, Thomas H., Brown, Herbert R., Davis, Stanley O., Le Vine, Donald M., Nash, Michael S., Pipher, James W. and Warshafsky, Julia R. *The Air National Guard Cyber Force*. Institute for Defense Analyses, 2017.

Homeland Defense Activities 32 U.S.C. §§ 901-908.

Keply-Steward, Kristy. "National Guard now involved in school Ransomware attack investigation." *ABC13 News,* August 25, 2020.

Kramer, Franklin D. and Butler, Robert J. "Cybersecurity: Changing the Model." *Atlantic Council*, April 2019.

Liscka, Allan. "Early Findings: Review of State and Local Government Ransomware Attacks." Recorded Future, 10 May 2019.

———. "Update: New Findings in Ransomware Attacks on State and Local Government." Recorded Future. 8 October 2019.

Maucione, Scott. "Air National Guard Uses Crash Courses to Narrow Cyber Training Backlog." Federal News Network, 7 February 2017. Accessed 20 August 2020.

"National Guard Cyber Units Protect Country's Interests, Still Face Training Issues." Federal News Network, 18 January 2019. Accessed 30 June 2020.

Nakashima, Ellen. "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries." *The Washington Post*, 28 September 2018. Accessed at 13 August 2020.

National Guard Association of the United States (National Guard AUS). Fact Sheet: Understanding the Guard's Duty Status. Undated.

New York State Homeland Security and Emergency Services. "Cyber Support Element."

Odell, Laura A., DiLorenzo, Cameron D. and Wahlman, Alec C. *National Guard Bureau Critical Infrastructure Cyber Response Framework*. (Alexandria, VA: Institute for Defense Analyses, 2020).

Office of Governor Phil Scott. "Vermont Army National Guard Cyber Response Team to Support UVM Health Network In Response to Ongoing Information Technology System Disruption." *State of Vermont,* November 4, 2020.

Office of Secretary of the State Denise W. Merrill. "Secretary Merrill and General Evon Announce Partnership to Evaluate Election Cybersecurity in Each Connecticut Town." *State of Connecticut,* June 12, 2020.

Pomerleau, Mark. "The Army Wants to Know How to Deploy Cyber Teams During Peacetime." Fifth Domain, 28 March 2019. Accessed 13 August 2020.

Puryear, Cotton. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." army.mil, 29 September 2017. Accessed 22 March 2020.

Smith, Aaron. "National Guard Conducts Annual Nationwide Cybersecurity Exercise." Defense.gov, 14 May 2018. Accessed 13 August 2020.

Soucy, Jon. "Guard Cyber Units Evolve as Cyber Threats Continue." Ang.af.mil. 22 January 2019. Accessed 13 August 2019.

Special Operations Forces: Training with Friendly Foreign Forces 10 U.S.C. § 2011

Strickland, W. Thomas, Burton, J. Katharine, Caverly, Robert J., Nash, Michael S. and Warshafsky, Julia R. *Cyber Models for the National Guard*. (Alexandria, VA: Institute for Defense Analyses, 2019).

"The National Guard Decodes How to Beat Encrypted Attacks." Fifth Domain, 10 April 2019. Accessed 11 April 2020.

United States Government Accountability Office. Report to Congressional Committees: Defense Civil Support: DoD Needs to Identify National Guard's Cyber Capability and Address Challenge in its Exercises.GAO-16-574, September 2016.

Williams, Lauren. "National Guard May Help States Defend Against Ransomware." GCN, 29 August 2019. Accessed 18 September 2019.

Appendix F: Abbreviations

ASD	Assistant Secretary of Defense
CISA	Cybersecurity and Infrastructure Security Agency
CMF	Cyber Mission Force
CPT	Cyber Protection Team
DCO	Defensive Cyber Operations
DCOE	Defensive Cyber Operations Element
DCO-IDM	Defensive Cyber Operations–Internal Defense Measures
DCO-RA	Defensive Cyber Operations–Response Actions
DHS	Department of Homeland Security
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DSCA	Defense Support to Civil Authorities
DSCIR	Defense Support to Cyber Incident Response
EMAC	Emergency Management Assistance Compact
HAD	Homeland Defense Activity
HD&GS	Homeland Defense and Global Security
HDCMA	Homeland Defense Cyber Mission Areas
IDT/AT	Inactive Duty Training/Active Training
IRA	Immediate Response Authority
IRT	Innovative Readiness Training
LFA	Lead Federal Agency
METL	Mission Essential Task List
MOU	Memorandum of Understanding
NGB	National Guard Bureau
NMT	National Mission Team
OCO	Offensive Cyber Operations
OSD	Office of the Secretary of Defense
PPD	Presidential Policy Directive
SAD	State Active Duty
SPP	State Partnership Program
TAG	Adjutant General
U.S.C.	United States Code

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From – To)
09-11-2022	Study (Final)	

4. TITLE AND SUBTITLE	5a. CONTRACT NO.
Using National Guard Cyber Forces to support Homeland Cyber Defense activities in non–DoD-Owned Cyberspace	HQ0034-19-D-0001/20-F-0003
	5b. GRANT NO.
	5c. PROGRAM ELEMENT NO(S).

6. AUTHOR(S)	5d. PROJECT NO.
James R. Ayers, project lead; Thomas H. Barth; Robert J. Caverly, Jr.; Elizabeth N. Conrad; Claire R. Harrison; Terry C. Heuring; Jessica M. Huckabey; Michael S. Nash	5e. TASK NO. Project DZ-8-4706
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NO.
Joint Advanced Warfighting Division (JAWD) Institute for Defense Analyses (IDA) 4850 Mark Center Drive, Alexandria, VA 22311-1882	IDA Paper P-33082 Log no. H 2022-000183

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM(S)
NGB J36 Engagements Branch Chief 111 South George Mason Drive TARC2 Arlington, VA 22204-1373	NGB
	11. SPONSOR'S / MONITOR'S REPORT NO(S).

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Unclassified

14. ABSTRACT

The defense of public and private cyberspace within the Homeland is a growing priority. The National Guard cyber force is an important contributor to defending the DoD Information Network (DoDIN), and is also frequently tasked to defend non-DoDIN cyberspace. This research examined the use of the National Guard cyber force off-DoDIN when the elements of that force are in Title 32 duty status and when DoD funds the specific use of that force. The analysis included existing and potential demand for National Guard support off-DoDIN; authorities, policies, and directives that enable and limit the National Guard's off- DoDIN activities; and the Guard's capabilities and capacities to respond to off-DoDIN taskings. Findings and recommendations for using the Guard's limited capacities in off-DoDIN cyberspace close the final report.

15. SUBJECT TERMS

National Guard Cyber Force, DoDIN, off-DoDIN, Cyber Mission Force, Homeland Defense, Homeland Security, Title 32, Defense Support to Civil Authorities (DSCA)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NO. OF PAGES	19a. NAME OF RESPONSIBLE PERSON
			UU	80	James Ayers
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
U	U	U			703-845-6721

This page is intentionally blank.