1-31-2019

Examining the Roles of Army Reserve Component Forces in Military Cyberspace Operations

Jeffrey L. Caton

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH ~ WISDOM

EXAMINING THE ROLES OF ARMY RESERVE COMPONENT FORCES IN MILITARY CYBERSPACE OPERATIONS

Jeffrey L. Caton

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

EXAMINING THE ROLES OF ARMY RESERVE COMPONENT FORCES IN MILITARY CYBERSPACE OPERATIONS

Jeffrey L. Caton

January 2019

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5238.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *http://ssi.armywarcollege.edu/*, at the Opportunities tab.

*****

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a quarterly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at the following address: *http://ssi.armywarcollege.edu/newsletter/*.

ISBN 1-58487-799-5

FOREWORD

Cyberspace operations have become pervasive in the United States, and they enable many aspects of modern life for the average citizen, such as entertainment, communication, education, transportation, banking, and voting. The continuing development of Army and Department of Defense (DoD) Reserve component cyberspace units can leverage the capabilities and experience of industry and academia to help protect critical information infrastructure and enhance national security. What opportunities and challenges surround the integration of these forces into a still-evolving joint cyberspace force?

In this monograph, Mr. Jeffrey Caton argues that current efforts to integrate Reserve cyber components appear to be sufficient for certain specific applications, but the Nation has yet to benefit from the potential synergy offered by an optimized blend of these capabilities. He admits that some issues identified in his monograph may be common to other applications of Reserve component forces, but emphasizes that the negative impacts may be more significant for cyber units due to the ethereal nature of cyberspace operations that are far less intuitive than those occurring in the physical world.

Mr. Caton offers recommendations for policymakers and senior leaders toward improving the integration

and utilization of Army Reserve component cyberspace forces for both state and federal applications.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

JEFFREY L. CATON is president of Kepler Strategies LLC, Carlisle, PA, a veteran-owned small business specializing in national security, cyberspace theory, and aerospace technology. He is also an intermittent professor of program management with Defense Acquisition University. From 2007 to 2012, Mr. Caton served on the U.S. Army War College (USAWC) faculty, including as an associate professor of cyberspace operations and defense transformation chair. Over the past 9 years, he has presented lectures on cyberspace and space issues related to international security in the United States, Sweden, the United Kingdom, Estonia, Kazakhstan, and the Czech Republic, supporting programs such as the Partnership for Peace Consortium and the North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence. His current work includes research examining the recent elevation of U.S. Cyber Command (USCYBERCOM) to be a unified command as well as the evolving role of the U.S. Army with nuclear operations as part of the External Research Associates Program of the Strategic Studies Institute (SSI). Mr. Caton is also a member of the editorial board for *Parameters* magazine. He served 28 years in the U.S. Air Force working in engineering, space operations, joint operations, and foreign military sales, including command at the squadron and group level. Mr. Caton holds a bachelor's degree in chemical engineering from the University of Virginia, a master's degree in aeronautical engineering from the Air Force Institute of Technology, and a master's degree in strategic studies from the Air War College.

SUMMARY

The legacy of the Citizen Soldier concept in the United States predates the U.S. Constitution. Today, those serving in the oldest form of service to our Nation are called upon to address one of the newest manifestations of warfare in the realm of military cyberspace operations. What capabilities can Reserve component forces bring to Department of Defense (DoD) cyberspace forces? What opportunities and challenges surround the integration of these forces into a still-evolving joint cyberspace force? What are the expectations for cyber forces that serve in a militia capacity?

This monograph explores these questions in four major sections. The first section provides a concise review of basic information on the laws and policies governing the use of Reserve component forces. The second section explores the uses of Reserve component cyber forces from a DoD perspective, focusing on the current strength and organization of Army National Guard (ARNG) and Reserve cyber forces and their use as part of the Cyber Mission Forces (CMF). It also addresses responsibilities for defense support to civil authorities and related operational issues, training and exercise opportunities, and total force challenges. The third section examines the use of ARNG cyber forces from the perspective of a state government, emphasizing the expectations of governors for state incident response and cybersecurity support. This section also addresses military-private partnerships, state-sponsored cyber ranges and exercises, and international partnerships. In the final section, the author offers recommendations to policymakers and leaders toward improving the integration and utilization of Army Reserve component cyberspace forces.

This monograph was written to serve as a primer for senior policymakers, decision-makers, and military leaders at the federal and state levels on the current status of the integration of Army Reserve component forces into U.S. military cyberspace operations. The contents herein are limited to the presentation of unclassified and open source information available before November 2017. The monograph includes recommendations related to the planning and exercising of cyber incident response activities, the cataloging and prioritizing of Reserve component cyberspace capabilities, and the development and support of cyber training ranges.

EXAMINING THE ROLES OF ARMY RESERVE COMPONENT FORCES IN MILITARY CYBERSPACE OPERATIONS

The legacy of the Citizen Soldier concept in the United States predates the U.S. Constitution. Today, those serving in the oldest form of service to our Nation are called upon to address one of the newest manifestations of warfare in the realm of military cyberspace operations. What capabilities can Reserve component forces bring to Department of Defense (DoD) cyberspace forces? What opportunities and challenges surround the integration of these forces into a still-evolving joint cyberspace force? What are the expectations for cyber forces that serve in a militia capacity?

This monograph explores these questions in four major sections. The first section provides a concise review of basic information on the laws and policies governing the use of Reserve component forces. The second section explores the uses of Reserve component cyber forces from a DoD perspective, focusing on the current strength and organization of Army National Guard (ARNG) and Reserve cyber forces and their use as part of the Cyber Mission Forces (CMF). It also addresses responsibilities for defense support to civil authorities and related operational issues, training and exercise opportunities, and total force challenges. The third section examines the use of ARNG cyber forces from the perspective of a state government, emphasizing the expectations of governors for state incident response and cybersecurity support. This section also addresses military-private partnerships, state-sponsored cyber ranges and exercises, and international partnerships. In the final section, the author offers recommendations to policymakers and

leaders toward improving the integration and utilization of Army Reserve component cyberspace forces.

This monograph was written to serve as a primer for senior policymakers, decision-makers, and military leaders at the federal and state levels on the current status of the integration of Army Reserve component forces into U.S. military cyberspace operations. The contents herein are limited to the presentation of unclassified and open source information, therefore any classified discussion must occur at another venue.

RESERVE COMPONENT BASICS

On any given day, the total force of Active Duty, Reserve, and National Guard members perform cyberspace operations in locations throughout the world. This section provides a brief description of the Army Reserve components as a foundation for the examination of their role in the broad range of military cyberspace activities. Military Reserve components are governed by Title 10 and Title 32, United States Code, which defines their purpose as:

> The purpose of the reserve components is to provide trained units and qualified persons available for active duty in the armed forces, in time of war or national emergency and at such other times as the national security requires, to fill the needs of the armed forces whenever, during, and after the period needed to procure and train additional units and qualified persons to achieve the planned mobilization, more units and persons are needed than are in the regular components.[1]

The Army Reserve component consists of the ARNG and Army Reserve (USAR). The ARNG is a force of about 343,000 Soldiers, with units in 50 states, 3 territories, and the District of Columbia. ARNG members provide almost 39 percent of Army operational

forces.[2] The USAR has an authorized strength of 199,000 Soldiers and 11,000 civilians, with units in 50 states, 5 territories, and 30 countries.[3]

	State Active Duty	Title 32, U.S. Code	Title 10, U.S. Code
Command & Control	State Governor	State Governor	President
Who Performs Duty	The Militia	The Federally-recognized militia (i.e. National Guard)	Active Component, Reserve Component, and National Guard
Where Duty is Performed	Continental United States in accordance with State Law	Continental United States	Worldwide
Pay Source	In Accordance with State Law	Federal Pay & Allowances	Federal Pay & Allowances

Table 1. Different Status Possibilities for National Guard Members[4]

Depending on the situation, ARNG forces may operate in any of three different statuses (as summarized in table 1): state Active Duty, full-time National Guard (Title 32), and Active Duty (Title 10). Governors can activate ARNG to state Active Duty status in response to emergencies based on state law and policy. In state Active Duty status, the limitations of the Posse Comitatus Act do not apply, and thus Guardsmen may act in a law enforcement capacity. Governors can also activate ARNG forces to Title 32 status with the approval of the President or the Secretary of Defense to conduct various Homeland Defense activities. Title 32 forces may still act in a law enforcement capacity if their chain of command remains in the state. The President may activate ARNG forces to Title 10

status for a variety of purposes, but the restriction of posse comitatus applies, and they cannot perform law enforcement duties unless specifically authorized by the President in response to insurrection.[5] In certain complex situations, the President and Governor may agree to establish a dual-status commander to lead a force composed of personnel under different activation statuses.[6]

DOD RESERVE COMPONENT CYBERSPACE APPLICATIONS

The 2015 *DoD Cyber Strategy* considers the Reserve component as an integral part of DoD military cyber operations, noting that it:

> offers a unique capability for supporting each of DoD's missions, including for engaging the defense industrial base and the commercial sector. It represents DoD's critical surge capacity for cyber responders.[7]

One of the strategy's objectives focuses on improving how Reserve component cyber forces can support broader national security needs: "Define and refine the National Guard's role in supporting law enforcement, Homeland Defense, and Defense Support of Civil Authorities missions."[8] This section examines the progress that ARNG and USAR cyber forces are making toward meeting the needs of DoD cyber operations.

Cyber Mission Force (CMF) Responsibilities

U.S. Cyber Command (USCYBERCOM) is the primary organization for planning and conducting DoD military cyberspace operations.[9] These operations are conducted by the CMF, a group of over 5,000

individuals in 133 teams that collectively reached their initial operating capability in October 2016. The CMF is projected to grow to almost 6,200 personnel when it reaches full operational capability in 2018. There are five different types of operational units in the CMF: National Mission Team, National Support Team, Combat Mission Team, Combat Support Team, and Cyber Protection Teams (CPT).[10] In his May 2017 Senate testimony, Admiral Michael Rogers, Commander, USCYBERCOM, tied the contribution of Reserve components to the CMF:

> We [USCYBERCOM] will posture the CMF to deliver effects across all phases of operations; to improve operational outcomes by increasing resilience, speed, agility, and precision; to generate operational outcomes that support DoD strategy and priorities; to create a model for successful Reserve and National Guard integration in cyberspace operations; and finally to strengthen partnerships across the government, with our allies, and with the private sector.[11]

Army Cyber Command (ARCYBER) is the Army service component command for cyberspace operations. As such, ARCYBER is responsible for providing 41 teams for the CMF: 4 National Mission Teams, 3 National Support Teams, 8 Combat Mission Teams, 6 Combat Support Teams, and 20 CPTs. Additionally, ARCYBER is designated as the Joint Force Headquarters (JFHQ)-Cyber to support U.S. Central Command, U.S. Africa Command, and U.S. Northern Command.[12] Army Reserve components also have obligations to support the USCYBERCOM CMF, which we will now examine.

National Guard CMF Contributions

In a memorandum of agreement signed on June 5, 2014, by Lieutenant General Edward C. Cardon, commanding general, ARCYBER and Second Army, and Major General Judd H. Lyons, acting director, Army National Guard, the ARNG committed to fielding 11 CPTs by the end of Fiscal Year (FY) 2018 to enhance Army cyber enabling capabilities. Further, the agreement stipulated that "the ARNG will provide one cyber protection team, or CPT, in an active duty, Title 10 status, in support of ARCYBER and Second Army."[13] Even before the memorandum of agreement signing, the first ARNG CPT had already formed in October 2013 at Fort Meade, MD, and was designated the 1636th CPT as an homage to the National Guard's year of origin. On October 7, 2014, Cardon presided over the ceremony that fulfilled the memorandum of agreement provision, stating, "Today this cyber protection team represents another first—the first Army National Guard/active duty cyber protection team."[14]

The other 10 ARNG CPTs are planned to be formed by the states shown in table 2. Each CPT is designed to have 39 members organized into 5 squads with a headquarters element. The Mission Protection squad (Blue Team) provides cyber risk mitigation and response from a perspective inside the network looking outward. The Discovery and Counter-Cyber Infiltration squad (Hunt Team) seeks out and eliminates threat activity on friendly networks. The Cyber Threat Emulation squad (Red Team) adopts the perspective outside the network and emulates potential threats to help identify vulnerabilities in cyber defenses. The Inspection Forces/Cyber Readiness squad (White Team) evaluates the CPT for DoD compliance and

operational readiness and effectiveness. Finally, the Cyber Support squad (Green Team) provides the necessary technical assistance to facilitate CPT operations and mitigate gaps in training.[15] A typical headquarters element has the CPT chief (usually a major), an operations officer (usually a Department of Army civilian), and a cyber warfare planner (usually a chief warrant officer).[16]

Year	States	Team Number
FY 2016	Georgia	CPT 170
	California	CPT 171
	Michigan/Indiana/Ohio	CPT 172
FY 2017	New York/New Jersey	CPT 173
	Colorado/North Dakota/South Dakota/Utah	CPT 174
	Alabama/Kentucky/Tennessee	CPT 175
	Illinois/Wisconsin	CPT 176
FY 2018	Minnesota	CPT 177
	Texas/Louisiana/Mississippi	CPT 178
	Nebraska/Missouri/Arkansas	CPT 179
Note: A typical CPT consists of 39 members: 7 officers; 16 warrant officers; and 16 enlisted personnel.		

Table 2. Army National Guard Cyber Protection Teams[17]

The ARNG national training center has stepped up to support some of the training and certification requirements for ARNG cyber teams. Located at Camp Robinson, AR, the Lavern E. Weber Professional Education Center (PEC) includes the Information Technology Training Center (ITTC), which has courses that

cover topic areas such as network engineering, server administration, network security, and database administration, and also operates the ARNG Cyber Operations Range.[18] In July 2015, the PEC worked with the U.S. Army Training and Doctrine Command's Cyber Center of Excellence (CoE) at Fort Gordon, GA, to deliver a pilot Cyber Common Technical Core (CCTC) course at the Camp Robinson campus. The initial class of this CCTC course at the PEC included members of the 1636th CPT and Army Reserve as well as Active Duty Army and Navy personnel. The goal is to refine and validate the CCTC to the point where the PEC is certified by USCYBERCOM and U.S. Army Training and Doctrine Command to serve as a satellite campus of the Cyber CoE.[19]

ARNG cyber forces also provide critical support to joint operations. In August 2017, ARCYBER activated Task Force Echo at Fort Meade, MD. Comprised of 138 ARNG members from 7 states, this new unit was the largest mobilization of Reserve component cyber forces to date in support of USCYBERCOM operations.[20] One month later marked the activation of the 91st Cyber Brigade as part of the Virginia National Guard. This first ARNG cyber brigade includes two cyber battalions in Virginia and it also serves as higher headquarters for cyber battalions in South Carolina and Massachusetts. Also, the 91st Cyber Brigade has responsibility for training and validating the 10 National Guard CPTs.[21]

Army Reserve CMF Contributions

In his March 2016 Senate testimony, Lieutenant General Jeffrey W. Talley, Commanding General, U.S. Army Reserve Command, summed up the posture of cyber forces in his command as follows:

> Today, the Army Reserve is committed to building 10 cyber protection teams, an Army Reserve Cyber Training Element with advanced research and opposing force teams, and to providing highly skilled cyber warriors to the 1st Information Operations Command, the Defense Information Systems Agency, and the United States Army Cyber Command headquarters—a commitment of more than 800 Citizen Soldiers in support of cyberspace operations. This force structure effort is budget neutral, which benefits both the Army and the Nation.[22]

At the center of the USAR cyber force is the Army Reserve Cyber Operations Group (ARCOG) assigned under the 335th Signal Command (Theater). The ARCOG was established at Adelphi, MD, in October 2016 as a cyber brigade with the following mission:

> The ARCOG provides trained and ready Cyber forces under the Cyber Protection Team construct to conduct Defensive Cyberspace Operations and Cyber support to Army, CCMD, DoD, DSCA [Defense Support of Civil Authorities], and other government agencies against an evolving threat.[23]

The ARCOG replaced the former Army Reserve Information Operations Command (ARIOC), which had been organized into five information operations centers (IOCs). Each IOC included "an operations section, a computer emergency response team (CERT) support group, a technical research team, and an information infrastructure defense assistance team"

trained using programs developed by the Software Engineering Institute at Carnegie Mellon University.[24]

Currently, the ARCOG is an organization that includes 469 Soldiers and is responsible for 10 CPTs assigned to 1 to 5 Cyber Protections Centers (CPCs) as depicted in table 3.[25] ARCOG support activities are not limited to the continental United States. For example, in August 2017, a team from the Western CPC deployed to Asia in support of Ulchi Freedom Guardian:

> an annual computer simulated defensive exercise conducted with the Republic of Korea and the United States Combined Forces Command, designed to enhance readiness, protect the region and maintain stability on the Korean peninsula.[26]

The integration of USAR cyber support extends to current operations of organizations such as the Defense Intelligence Agency, the Defense Innovation Unit (Experimental), and the Army Research Laboratory.[27]

Training is a critical portion of operating the USAR cyber teams, and significant progress has been made to integrate USAR members into mainstream Army cyber training. In May 2017, five members of National Capital Region CPC graduated from the CCTC course taught by the first-ever Mobile Training Team of the Army Cyber CoE.[28] In July 2017, the first five Army Reserve members graduated from the Cyber Operations Officer Course at the Cyber CoE, Fort Gordon, GA.[29]

Cyber Protection Center Region	Location	Team Number
North East	Fort Devens, MA	CPT 180
		CPT 181
National Capitol Region	Adelphi, MD	CPT 182
		CPT 183
South West	San Antonio, TX	CPT 184
		CPT 185
North Central	Coraopolis, PA	CPT 186
		CPT 187
Western	Camp Parks, CA	CPT 188
		CPT 189
Note: A typical CPT consists of 39 members: 7 officers; 16 warrant officers; and, 16 enlisted personnel. The first two CPTs are projected to reach initial operating capability in FY 2018.		

Table 3. Army Reserve Planned Cyber Protection Teams[30]

Defense Support of Civil Authorities

Army Reserve components may be called upon to support emergencies and disasters that are coordinated at the state or national level, sometimes as part of a broader DoD support effort. Such activities are myriad and they fall into the category of Defense Support of Civil Authorities (DSCA).[31] This section examines the continuing evolution of potential DSCA support to cyberspace-related incidents. Foundational guidance provided in *Chairman of the Joint Chiefs of Staff Manual* (CJCSM) 6510.01B (July 10, 2012), *Cyber Incident Handling Program*, assigns USCYBERCOM the responsibility for cyber incident response efforts, which includes coordination with the Department of Homeland Security (DHS) and other federal agencies.

Further, CJCSM 6510.01B explicitly addresses such coordination for any situation that involves DSCA.[32]

Cyber incidents that require a national response are only part of a larger portfolio of incidents that are entrusted to the DHS's Federal Emergency Management Agency (FEMA) and administered using the National Response Framework (NRF). Simply put, the NRF provides guidance and structure to determine who does what in the face of national disasters and emergencies. It provides operational concepts focused on the priorities "to save lives, protect property and the environment, stabilize the incident, and provide for basic human needs."[33] The NRF identifies several principles for successful national response operations: "engaged partnership; tiered response; scalable, flexible, and adaptable operational capabilities; unity of effort through unified command; and readiness to act."[34]

Army and DoD doctrine largely defer to the NRF for DSCA related to cyberspace incidents. The DoD's *Strategy for Homeland Defense and Defense Support of Civil Authorities* addresses potential cyberspace-related threats, but provides no actionable details regarding DSCA-related response.[35] Joint Publication (JP) 3-28, *Defense Support of Civil Authorities*, only addresses cyberspace support related to securing critical information and telecommunication systems; it defers to JP 3-12(R), *Cyberspace Operations*, additional information.[36] In turn, JP 3-12(R) merely points to DHS and the NRF with regard to cyberspace-related DSCA; it provides no amplifying information for joint forces.[37] Army doctrine follows this trend in Army Doctrine Reference Publication (ADRP) 3-28, *Defense Support of Civil Authorities*, with cyberspace activities mentioned only in the context of possible threats and in regard

to communications support.[38] Army Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, does not address DSCA activities.[39] Given the dearth of detailed information in DoD regarding cyber incident related DSCA, let us examine what the NRF and related documents expect from DoD.

The evolution of national response guidance for cyber incidents, including the relevant DSCA responsibilities, is far from complete. In May 2013, DHS released the second edition of the NRF which included a separate cyber incident annex.[40] Oddly, the only NRF *Cyber Incident Annex* provided on the FEMA website is dated December 2004, despite being listed as updated in March 2012.[41] This version of the annex was written before the establishment of USCYBERCOM, and thus it still refers to the defunct Joint Task Force-Global Network Operations as the coordinator for DoD actions.[42]

In July 2016, President Barack Obama issued Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, to provide executive guidance for handling whole-of-government cyber incident response.[43] Only a month before, DHS released the NRF third edition that incorporated many of the tenets of PPD-41, but this new edition removed the response-related annexes (including the *Cyber Incident Annex*), stating that they were moved to the DHS Response Federal Interagency Operational Plan (FIOP).[44] However, the FIOP second edition, released in August 2016, does not have any reference to such a cyber incident annex.[45] In fact, the only DHS Response FIOP annex listed on the FEMA website is one for nuclear/radiological incidents.[46]

Regardless of this disconnect, DHS released the National Cyber Incident Response Plan (NCIRP) in December 2016, which was developed to implement the requirements of PPD-41.[47] Despite the significant progress made in 2016 following PPD-41, details of national response to cyber incidents remain somewhat convoluted and should be studied in greater detail than the scope of this monograph allows. For now, let us explore how cyberspace-related DSCA is portrayed in the current NCIRP.

The stated NCIRP scope reflects a whole-of-nation approach to cyber incidents, describing itself as "the strategic framework for operational coordination among federal and SLTT [state, local, tribal, and territorial] governments, the private sector, and international partners."[48] The document is built upon five guiding principles derived from PPD-41: shared responsibility, risk-based response, respecting affected entities, unity of government effort, and enabling restoration and recovery.[49] To enable a common operational context, the NCIRP uses the PPD-41 definitions for "cyber incident" and "significant cyber incident" and provides a methodology for differentiating the two.[50] Also, the NCIRP implements the Cyber Unified Coordination Group (UCG) concept from PPD-41 to provide an appropriate and consistent forum for national-level cyber incident coordination.[51] National policy and strategy coordination is charged to the DHS-led Cyber Response Group (CRG).[52] Depending on the circumstances, DoD may be a participant in both CRG and Cyber UCG.

How do DoD and Army Reserve components support the cyber DSCA efforts of the NCIRP? There are at least six different areas where such support may occur (which are summarized in table 4). First, the

NCIRP acknowledges DoD's responsibility for protecting its own cyberspace network assets as well as its ability to support civil authorities as authorized by law or directed by the President.[53] It also recognizes the various roles that National Guard cyber forces may perform to support cybersecurity activities at the state or federal level (to include DSCA), depending on their duty status.[54] Second, myriad Army Active and Reserve component units provide intelligence support through routine threat and situational awareness operations and may provide technical assistance as part of DSCA activities.[55] Third, DoD and Army total force cyber units operate three of the seven federal cybersecurity centers identified in the NCIRP "to execute operational missions, enhance information sharing, maintain situational awareness of cyber incidents, and serve as conduits between public- and private-sector stakeholder entities."[56] Fourth, national cyber incident response efforts can leverage the existing liaison relationship between contacts in the 10 FEMA regions and Army Active, Reserve, and National Guard units.[57] Fifth, DoD and Army cyberspace forces may provide support as determined by a Cyber UCG to the DHS for asset response efforts, the Department of Justice (DOJ) for threat response efforts, and the Office of the Director of National Intelligence (ODNI) for intelligence support efforts.[58] Finally, a sixth area of DoD and Army total force support to national cyber incident response is the general support of 14 core capabilities—such as cybersecurity, forensics, planning, and situational awareness—identified in the NCIRP as "activities that generally must be accomplished in cyber incident response, regardless of which levels of government are involved."[59]

Area of National Cyber Incident Support	Circumstances
Network protection	Ongoing operations and DSCA
Intelligence support	Ongoing operations and DSCA
Cybersecurity center operation: • USCYBERCOM Joint Operations Center (JOC) • NSA Cybersecurity Threat Operations Center (NCTOC) • DoD Cyber Crime Center (DC3)	Ongoing operations and DSCA
Liaison with FEMA regions	Ongoing operations and DSCA
Cyber UCG support: • DHS (asset response lead agency) • DOJ (threat response lead agency) • ODNI (intelligence support lead agency)	DSCA
NCIRP core capability support	DSCA
Note: DSCA efforts are requested by civil authorities and authorized by law or directed by the President.	

Table 4. Areas of DoD Support to National Cyber Incidents

A significant challenge for effective cyber incident response is the diversity of state, local, tribal, and territorial government organizations that coordinate FEMA, DoD, and National Guard activities. The NCIRP notes, "While many state, local, tribal, and territorial governments are developing and utilizing operational coordination structures for cyber incident response, they have not all adopted a standard approach."[60] What other challenges are present in cyber DSCA operations?

Operational Issues

The U.S. Government Accountability Office (GAO) published three studies in the last 2 years that address issues on how to fully and properly implement DoD cyber forces—especially Reserve components—into DSCA actions related to cyber incidents. The June 2015 GAO report "DOD Is Taking Action to Strengthen Support of Civil Authorities," noted that DoD had not implemented a 2012 GAO recommendation to update DoD DSCA guidance "to ensure that it was consistent with national plans and preparations for domestic cyber incidents."[61] Based on the preceding discussion in this monograph, the GAO finding remains valid.

The April 2016 GAO report, "DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents," built upon the 2015 GAO report and concluded that, while DoD had improved its DSCA guidance in many areas, the support for cyber incident response remained insufficient:

> Whether DOD updates DSCA guidance or issues additional guidance on a separate cyber-technical assistance framework, without clarifying guidance on DOD roles and responsibilities in a cyber incident, DOD cannot reasonably ensure that the department will be able to most effectively employ its capabilities to support civil authorities in a cyber incident.[62]

To support this conclusion, the report had three key findings that identify significant operational gaps and seams with regard to how DoD supports civil authorities during or after a cyber incident. First, the existing DoD guidance for DSCA does not explicitly address roles and responsibilities for cyber forces. Second, for cyber incidents in the continental United

States, it is unclear whether the supported command with primary responsibility for cyber DSCA is U.S. Northern Command or USCYBERCOM. Interestingly, the study noted that U.S. Northern Command had yet to receive a cyber DSCA request from DoD. Third, current DSCA guidance does not address the role of a dual-status commander for cyber DSCA.[63] The report noted that ARNG forces normally respond to emergencies in state status.[64]

Independent Cyber Mission Analysis reports to Congress in 2014 by DoD and the National Guard Bureau (NGB) acknowledge the need for clarity in the organization and command structures noted by the GAO. With respect to total force opportunities, both reports found that "cyber reserve components can offer load sharing and surge capacity and [NGB] supports DOD's plan to integrate reserve personnel into cyberspace forces."[65]

The September 2016 GAO report, "DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises," examined three areas of cyber capabilities found in ARNG units: communications directorates, computer network defense teams, and cyber operations units.[66] The GAO investigation included nongeneralizable interviews with state officials of the Georgia, Nevada, and Washington National Guard. One of the key findings was that DoD had still not acted upon earlier GAO recommendations to issue implementation guidance for the use of dual-status commanders in cyber incidents.[67] However, the most significant study finding was that DoD does not have adequate visibility of all ARNG cyber capabilities available for DSCA activities. Although the NGB uses the Defense Readiness Reporting System and Joint Information Exchanges Environment,

"officials acknowledged that neither of these systems fully or quickly identified National Guard cyber capabilities that could be used to support civil authorities in a cyber incident."[68]

As solutions are developed to address these operational challenges identified by the GAO, it is prudent that they be tested in a controlled environment before being implemented in real DSCA events. Large-scale cyber exercises can provide valuable opportunities to practice and refine new DSCA constructs for cyber incidents involving Active and Reserve component forces.

Cyber Exercises

Army Reserve component units participate in two major annual cyber exercises. Cyber Guard is co-hosted with USCYBERCOM at the Top Secret level to explore interagency responses to cyberattacks on U.S. critical infrastructure. Cyber Shield is an unclassified exercise that focuses "on the defense of Guard Net and state-directed coordination actions."[69] The upcoming section of this monograph on state cyberspace applications addresses further details of Cyber Shield exercises.

Cyber Guard was first conducted in 2012 with a goal "to foster coordinated cyberspace incident responses between the federal and state governments, exploring the Army National Guard (ARNG) potential as an enabler and 'force multiplier' in the cyberspace domain."[70] With the intent to practice a whole-of-nation response to cyberattacks, the exercise has expanded each year to incorporate participants from DHS, the Federal Bureau of Investigation (FBI), and the Federal Aviation Administration, as well as allies, private industry partners, and academia. Cyber

Shield also works to integrate the activities of multiple federal and state operations centers and information fusion centers.[71] Cyber Guard 17 was held in July 2017, with over 40 participants from 22 different countries, and included a "Multinational Day" for the second consecutive year.[72] Of particular interest to the Army is the Cyber Guard objective to support the development of a Persistent Cyberspace Training Environment across DoD, an effort for which the Army has been designated as acquisition lead.[73]

In its 2016 report on ARNG cyber exercises, the GAO noted three specific challenges in the way DoD runs these exercises: limited access of some team members because of classified exercise environments; limited inclusion of other federal agencies and critical infrastructure owners; and inadequate incorporation of scenarios with joint physical-cyber effects. Further, a key finding of the report was that the DoD "needs to conduct a tier 1 exercise to explore a disaster with physical and cyber effects."[74]

The Cyber Guard 17 preparation material included a USCYBERCOM presentation on Cyber DSCA command and control that appeared to offer some progress in the area of defining command relationships. The presentation provided detailed organization wiring diagrams for three scenarios: DSCA in a multi-domain operation; DSCA in a cyber-only operation with ARNG forces in state Active Duty status; and DSCA in cyber-only operations with some ARNG forces activated to Title 10 status. A prominent feature of each diagram was a dual-status commander with clearly defined lines of command, coordination, and support, including a Title 10 deputy and ARNG deputy.[75]

Total Force Issues

In 2014, the Reserve Forces Policy Board published the report, *Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force*, which advocated for the inclusion of Reserve components into the emerging CMF structure.[76] While the current 133 CMF teams are all Active Duty units, the report's intent to integrate cyber Reserve components is coming to fruition. In his 2016 USAR posture report to Congress, Talley clearly connected his command, the Army Total Force, and the CMF:

> As the Army continues to develop its cyber needs, the Army Reserve will continue to grow its cyber force through the Total Army Analysis process. We will also continue to collaborate with all Cyber Mission Force [CMF] partners to develop new and innovative training strategies, to include public and private partnerships with academia, industry and government, to lessen the length of time needed for training future cyber warriors by leveraging civilian-acquired education and work experience.[77]

While the tenets offered by Talley sound reasonable, it may take several years to amass enough operational data to assess properly and refine the Total Force balance required for cyberspace operations. The 2016 book published by Air University, *The Human Side of Cyber Conflict*, offers a critical analysis and some earlier insights of this integration process that resonate with the challenges facing Army Reserve component cyber operations:

> However, the rapid growth of RC [Reserve component] cyber units, coupled with the recent (2010) stand-up of USCYBERCOM, means that the roles and missions of both the Guard and Reserve are only now being understood.

> Cost savings alone is an invalid reason to stand up more RC cyber units. Solid requirements must drive force presentation, and policy makers and military planners alike must have access to accurate cost calculations. Using the civilian expertise of RC cyber warriors is an attractive selling point for RC cyber units, but people in civilian cyber first-responder jobs or in damage-mitigation roles cannot be counted on to choose between their civilian careers and activation.[78]

Cyberspace Reserve Components of Other Service

Other military Service cyber component commands are also integrating Reserve component personnel into their force structure. The Navy's Fleet Cyber Command is adding 298 cyber Reserve billets individually aligned to augment the cyber defense capabilities for their CPT and JFHQ-Cyber.[79] Many operational units within the Air Force Cyber Command are augmented by members of the 960th Cyberspace Operations Group that includes five squadrons that can conduct various forms of defensive cyber operations.[80]

The Air National Guard is of particular interest since these forces may be closely aligned with the ARNG in the same state. The Air National Guard designates its CPT-qualified units as cyber operations squadrons and the current plan is to have 12 Air National Guard CPT-capable units that will field 2 full time CPTs on a rotational basis (see table 5).[81] The typical cyber operations squadron structure consists of 35 members organized in the same manner as ARNG CPTs, with a leadership element that directs 5 teams: cyber threat emulation, mission protection, defensive cyber infiltration, cyber readiness, and a cyber support.[82]

State	Air National Guard CPT
Idaho	224th Cyber Operations Squadron
Iowa	168th Cyber Operations Squadron
Kansas	127th Cyber Operations Squadron
Maryland	275th Cyber Operations Squadron
	276th Cyber Operations Squadron
Michigan	272d Cyber Operations Squadron
New Jersey	140th Cyber Operations Squadron
Pennsylvania	112th Cyber Operations Squadron
Texas	273d Cyber Operations Squadron
Virginia	185th Cyber Operations Squadron
Washington	143d Cyber Operations Squadron
California	261st Cyber Operations Squadron

Table 5. Air National Guard Cyber Protection Teams

Recruitment and Retention

Recognizing the opportunities for highly skilled cyberspace technicians employed in the private sector to serve their country, the USAR established the Cyber Private Public Partnership (Cyber P3) initiative as "a cost-effective, innovative way to integrate public and private industry partnerships to recruit, train, educate, develop, and retain critical cyber skills."[83] The program started in 2015 with 6 university and 12 employer partners, including companies such as Microsoft, Verizon, and T-Mobile. The program is designed both to recruit potential qualified Reserve members and to help transition Active Duty Soldiers to Reserve positions while providing continuing education and acquiring employment in the cyber-related job market.[84]

In 2017, the RAND Corporation published *Cyber Power Potential of the Army's Reserve Component* that examined the current cyber skills, roles, and missions that exist in the Army Reserve component as well as assessed the recruitment, training, and assignment of cyber personnel. Their findings confirmed the extremely competitive environment for recruiting cyber talent and found that the skills required for many roles in the CMF could be acquired using civilian-based training. Further, the RAND team found that experience in civilian cyber jobs was usually frequent and relevant enough for individuals to stay "cyber-sharp" for military applications. The study results also indicated that the DoD and the Army need improved insight into the inventory of their cyber personnel and noted that there exists a significant number of personnel already in the Reserve components that have untapped cyber skills. Finally, the study members advocated the use of a standard cyber aptitude assessment tool for evaluating prospective recruits.[85] Such an asset would be a valuable tool to support a program under DoD consideration to establish direct commissioning for cyber officers in a similar manner to programs already in place for medical doctors, lawyers, and chaplains.[86]

In reality, it may be too soon to discuss the question of total cyber force balance as there is not sufficient data with regard to what actual forces are available, what mission these forces accomplish, and what broad requirements they should fulfill. It appears that the great competition for cyber resources may be encouraging the Army and the DoD to create and fill billets as fast as possible without scrutinizing the true needs and resources already available.

STATE CYBERSPACE APPLICATIONS

The previous section viewed the roles of Army Reserve component cyber units primarily through the lens of DoD operations performed under Title 10 authorities. This section adopts the perspective of U.S. state governments and the relevant state Active Duty and Title 32 authorities. The scope of discussion is not intended to be comprehensive; rather, this section provides illustrative examples of specific state implementation of Reserve component cyber competencies. Due to the unique capabilities to operate in multiple activation statuses, the discussions herein emphasize the role of ARNG units.

Expectations of State Governors

The National Governors Association (NGA) website includes a "Governor's Guide to Cybersecurity" page dedicated to the question: "Why is the National Guard integral to state cybersecurity?"[87] The ensuing discussion highlights the capabilities that ARNG units can provide not only to address major cyber incident responses but also to "assist routine, steady-state cybersecurity activities to defend state and local computer systems."[88] In pursuing these tasks, the ARNG offers governors the flexibility to lever members' experience and relationships with technology companies and academia as well as to provide access to DoD cyberspace resources, if requested.

Incident Response Responsibilities

The ARNG has established Defensive Cyberspace Operations Elements in all 54 states, territories, and the District of Columbia "to provide the first line of defense for our military networks."[89] The elements were formed in 1999 to address Y2K issues and, until 2017, were known as Computer Network Defense Teams. Current Defensive Cyberspace Operations Elements are small teams (8-10 members) organized at the state level. In January 2013, Computer Network Defense Team members from seven states came together for the first joint Computer Network Defense Team operation to support cybersecurity measures for the 57th Presidential Inauguration. The team of 27 Airmen and Soldiers provided "defense capabilities [that] were applied to various voice, video, and data communication systems that supported tactical operations."[90] The NGB has a goal to grow the number of these teams to 2,800 personnel collectively by 2019.[91]

An October 2014 paper by the NGA Center for Best Practices identified Delaware, Maryland, Michigan, Rhode Island, Utah, and Wisconsin as among the first states to leverage the capabilities of these ARNG cyber defense teams to address state cyber incidents.[92] The number of states incorporating ARNG forces in their state processes continues to grow. The South Carolina ARNG invested $1 million in Computer Network Defense Team training and certification to develop a 16-member team that is "ready to respond to any incident that occurs on the cyber scale . . . from a simple phishing attempt to a large-scale cyber attack causing destruction to a physical structure."[93] In February 2016, the Florida ARNG Computer Network Defense Team supported exercises with state agencies that

included "mock incursions from hacktivist groups, terrorist organizations and nation-states."[94]

In February 2017, the NGA released a policy statement on cybersecurity which provides five principles to describe its vision for how federal and state governments should work together in the response and recovery actions following a cyberattack. One principle emphasizes the need for unity of effort with national efforts defined in the NCIRP:

> Processes should be established and tested to ensure coordination and communications between federal and state authorities during cyber incidents are effective and consistent. Alignment of state cybersecurity plans with the National Cyber Incident Response Plan will facilitate an efficient and coordinated government response to serious cyber incidents.[95]

The National Guard Cyber Threat Working Group supports this principle as "a process to create a unified strategic message from NGB staffs to the States, Territories and District of Columbia, to ensure the . . . [National Guard] responds appropriately to cyber threats."[96] This process allows the Cyber Coordination Cell within the National Guard Coordination Center to convene the National Guard Cyber Threat Working Group to address cyber events.[97]

With the emphasis on cybersecurity and cyber incident response promulgated by the NGA, one might assume that ARNG cyber capabilities are explicitly cited in official state emergency response and recovery plans. But a survey of some of these plans indicates otherwise. Table 6 is a summary of the review of 15 emergency response plans taken from the official public websites of 11 states and the District of Columbia. Only 6 of these 15 plans provided

actionable details for responses to cyber incidents, and only the Florida Emergency Management Plan explicitly included specific ARNG cyber capabilities (albeit in the plan's Terrorism annex).[98] It is particularly surprising that states with a strong military cyberspace presence—such as Maryland (USCYBERCOM and Fleet Cyber Command headquarters), Georgia (ARCYBER headquarters), Texas (Air Force Cyber Command/24th Air Force headquarters), and Virginia (ARCYBER headquarters elements)—have no mention of ARNG or other military cyberspace capabilities in the state's primary emergency response plans. Further investigation of the reasons behind these gaps in operational planning documents is beyond the scope of this monograph, but the implications do not bode well for the unity of effort between federal and state authorities to leverage military cyberspace capabilities effectively in emergency situations.

State Plan	*Cyber Incident Details Addressed?	National Guard Cyber Capabilities Included?
Arizona: *Arizona State Emergency Response and Recovery Plan* (February 2017)	Yes (Annex)	No
California: *State of California Emergency Plan* (October 2017)	Yes	No
Colorado: *Colorado Hazard and Incident Response and Recovery Plan* (November 2016)	Yes (Appendix & Annex)	No

Table 6. Incorporation of Cyber Incident Response in State Emergency Plans[99]

State Plan	*Cyber Incident Details Addressed?	National Guard Cyber Capabilities Included?
District of Columbia: *District Response Plan* (September 2014)	No	No
Florida: *The State of Florida 2016 Comprehensive Emergency Management Plan* (2016)	Yes	Yes
Georgia: *Georgia Emergency Operations Plan* (January 2015)	No	No
Georgia: *Georgia Emergency Operations Plan 2015: Department of Defense Annex, Defense Support* (2015)	No	No
Maryland: *State of Maryland Response Operations Plan* (SROP) (March 2015)	No	No
Maryland: *State of Maryland Consequence Management Operations Plan* (September 2017)	No	No
Michigan: *Michigan Emergency Management Plan* (July 2016)	Yes	No
Pennsylvania: *Commonwealth Emergency Operations Plan* (June 2017)	No	No
Pennsylvania: *Pennsylvania 2013 Standard State All-Hazard Mitigation Plan* (2013)	No	No

Table 6. Incorporation of Cyber Incident Response in State Emergency Plans (cont.)

State Plan	*Cyber Incident Details Addressed?	National Guard Cyber Capabilities Included?
Texas: *State Of Texas Emergency Management Plan* (February 2015)	No	No
Virginia: *Commonwealth of Virginia Emergency Operations Plan* (March 2015)	No	No
Washington: *Comprehensive Emergency Management Plan* (June 2016)	Yes (Annex-March 2015)	No
*Note: For a "Yes" in this column, the plan must have an explicit section that addresses how the state uses specific resources to address cyber incident responses. The mere mention of "cyber" or "cybersecurity" is not sufficient.		

Table 6. Incorporation of Cyber Incident Response in State Emergency Plans (cont.)

It is interesting to note that some of the plans that were void of ARNG cyber capability references included significant details on ARNG chemical, biological, radiological, nuclear, and explosives response capabilities, such as civil support teams. Concepts for cyber support teams have been proposed twice in Congress, but not yet adopted. The Cyber Warrior Bill of 2013 called for the development of ARNG Cyber and Computer Network Incident Response Teams in all states; no action beyond its initial introduction has occurred since March 2013.[100] Similar legislation was proposed in September 2017—the Major General Tim Lowenberg National Guard Cyber Defenders Act—to establish Reserve component cyber civil support teams.[101] A more radical piece of legislation is the

Cyber Defense National Guard Act, a 2015 proposal to explore the feasibility of creating a separate Cyber Defense National Guard. It too has not progressed in Congress since its introduction.[102]

Support to State Cybersecurity

The NGA Governor's Guide to Cybersecurity advocates four areas of ARNG cyber support to help improve the defense of state and local computer systems: risk assessment, network design, training, and cyber response exercises.[103] In fact, there are examples of such ongoing ARNG cyber support in each of these areas. In Michigan, the ARNG is part of a "red team" that can conduct penetration testing on state networks to expose cybersecurity vulnerabilities. With this information, the team can help improve network design and "inform the allocation of additional resources and mitigation measures."[104] Similar ARNG support provided risk assessments and network design improvement efforts to South Carolina's state tax agency as well as California's and Maryland's state agency networks.[105] To provide training to key state officials, the Missouri ARNG cyber defense team initiated "table-top exercises with the state government and the owners of critical infrastructure."[106] Also, Washington includes ARNG cyber personnel as part of its Joint Forces Defense Assessment Team that conducts risk assessment and cyber emergency planning.[107] In November 2016, cyber defense teams in the Ohio and Maryland ARNG were called upon to help protect state computer systems that supported elections, such as voter registration databases.[108]

State Initiatives and Opportunities

Another question asked in the NGA Governor's Guide to Cybersecurity is: "What Can Governors do to Enhance the National Guard's Role in Cybersecurity?" The proffered answer covers four general areas: map National Guard cyber unit capabilities; determine how ARNG cyber units can be used in nonemergency scenarios; push for clarifications in DoD guidance in cyber DSCA; and, identify dual-purpose ARNG cyber training exercises that achieve federal objectives while fulfilling state cybersecurity objectives.[109] The preceding sections discussed how ARNG cyber units can be utilized in cyber response actions and nonemergency state support. This section will explore how private sector partnerships, cyber ranges, and cyber exercises may enhance both ARNG cyber unit effectiveness and state cybersecurity.

Military-Private Sector Partnerships

The USAR Cyber Private Public Partnership initiative has five lines of effort that facilitate mutually beneficial partnerships not only with employers and universities as discussed earlier, but also with community outreach, research and training infrastructure, and strategic communication.[110] The initial six Cyber Private Public Partnership partner universities were dispersed across the Nation: Drexel University (Pennsylvania); University of Washington (Washington); George Mason University (Virginia); the University of Texas at San Antonio (Texas); Norwich University (Vermont); and, the University of Colorado (Colorado).[111]

But partnerships with state universities are not limited to the Cyber Private Public Partnership program. For example, the Georgia ARNG teamed with the

Georgia Tech Research Institute during Cyber Shield 2017. During the exercise, Georgia Tech Research Institute provided support in the areas of network infrastructure, information technology administration, and malware analysis. The official Georgia Tech Research Institute article summarizing these efforts noted: "This inaugural collaborative cyber effort between Georgia Tech Research Institute and the Guard will, it is hoped, lead to a long-term, strategic relationship, supporting various state of Georgia and DoD activities."[112] Another partnership example is the Louisiana ARNG work with the Louisiana State University Stephenson Disaster Management Institute during the Vigilant Guard 2016 exercise. Facilities at the institute allowed the ARNG team to simulate a series of cyber-attacks and "to train alongside other government entities such as the FBI, the Department of Homeland Security and the Louisiana State Analytical and Fusion Exchange."[113]

In the future, ARNG cyber units may have the opportunity to deal with unique state organizations with complementary cyber capabilities like those of the Michigan Cyber Civilian Corps, a group of volunteer cybersecurity experts with stringent membership requirements. The Michigan Cyber Civilian Corps mission is "to work with government, education, private sector organizations, and volunteers to create and implement a rapid response team to be activated under a Governor declared Cyber State of Emergency."[114]

Cyber Ranges

As a key part of its cyber training program, the PEC ITTC also hosts and operates the ARNG Cyber Operations Range.[115] In addition to this ARNG facility,

several states are developing cyber ranges with capabilities that ARNG cyber units could leverage for training and certification. Table 7 provides some examples of state-sponsored cyber ranges that could accommodate ARNG training as well as provide a collaborative environment for addressing state cybersecurity challenges among government, military, academic, and private sector participants. Other states have programs underway that include the development of cyber ranges with ARNG supporters. In February 2017, the Ohio Adjutant General's Department announced the establishment of the Ohio Cyber Collaboration Committee, a group of more than 30 government, military, academic, and private sector organizations. The Ohio Cyber Collaboration Committee was formed at the request of Governor John Kasich, and one of its goals is "to create a cyber range—a virtual environment used for cybersecurity training and technology development."[116] In January 2017, Georgia Governor Nathan Deal announced plans to establish the Georgia Cyber Innovation and Training Center in Augusta. This $50 million state-funded initiative will include a state-owned cyber range used "to establish cybersecurity standards across state and local agencies to develop and practice protocols for responding to cyber threats."[117] The proposed cyber range will be designed with military users like the Georgia ARNG and ARCYBER in mind, and it will have the unique feature among state cyber ranges of being able to operate as a sensitive compartmented information facility.[118] These ranges are still on the drawing board, so let us look at the Michigan Cyber Range as an established example of what a cyber range can provide.

State	Cyber Range Description
Florida	The Florida Cyber Range provides advanced training and testing solutions for academic, government, military and industry organizations through cybersecurity exercises, competitions, conferences, operations and research. The Florida Cyber Range will support education, training and research for emerging needs, including ethical hacking and penetration testing, computer and network security, critical infrastructure and industrial control systems security, Internet of Things security, defensive cyberspace operations and cyber war gaming.[119]
Maryland	Baltimore Cyber Range (opened August 2017). Leveraging the Cyberbit Range platform, the BCR facility allows cybersecurity practitioners the opportunity to experience the latest real-world cyber threats in a controlled and sequestered environment to improve their hands-on skills. The range, which can simulate large-scale virtual networks and attacks based on real-world incidents, can also pinpoint system vulnerabilities and help users develop countermeasures and improved protocols for dealing with cyber-attacks on critical network systems. As a result, cybersecurity practitioners benefit from receiving real-time training for threat detection, and the response process, enabling them to dramatically improve the performance of all security and SOC [security operations center] teams.[120]
Michigan	Established in 2012, the Michigan Cyber Range has trained more than 2,900 whole community partners through interactive, virtual training programs. Initially supported with $365,000 in Homeland Security Grant Program. (HSGP) funds, the Cyber Range is a public-private partnership offering in-person and online courses in 14 topics including digital forensics, incident handling, penetration testing, and information systems auditing.[121]
Virginia	Regent University Cyber Range training center. The Cyber Range will also serve as a training center for local businesses, government and military organizations, and features customizable capabilities to meet every industry's data protection needs. The world-class facility will provide hands-on cybersecurity training and simulation platforms with real-time attack scenarios and security breaches for Regent students seeking to fill the projected 6 million job openings in the cybersecurity field by 2019.[122]

Table 7. Examples of State-Sponsored Cyber Ranges

The Michigan Cyber Range was opened by Governor Rick Snyder in November 2012 as an initiative to pair "cybersecurity resources with hands-on training opportunities to enhance Michigan's protection of computer systems and sensitive data."[123] Initially hosted at Eastern Michigan University, the applications and audiences envisioned for the cyber range included infrastructure defense, homeland security, law enforcement, education, and private sector business.[124] Since then, the Michigan Cyber Range has grown by adding hubs at different university locations throughout the state, all connected by over 4,000 miles of fiber-optic cable. The range also added "Alphaville," a virtual city with a typical urban information city that can be used in cyber defense exercises.[125] In 2014, the fourth hub of the Michigan Cyber Range was opened at the 110th Airlift Wing on the Kellogg Air National Guard Base in Battle Creek. Since then, members of the Michigan Army and Air National Guard have utilized the Alphaville model for training as well as collaboration with organizations such as West Point and the California ARNG.[126]

Cyber Exercises

As mentioned earlier, Cyber Shield is an unclassified annual exercise that concentrates on defense of ARNG networks. Like the Cyber Guard series, Cyber Shield exercises have grown steadily each year in many areas, such as the number of participants, number of states and territories represented, and complexity of the scenario. "Cyber Shield prepares the citizen-soldiers to Defend the Network, but also participate in the planning and execution of national-level exercises such as Cyber Guard and Cyber Flag which

focus on the broader mission of Defend the Nation."[127] There are significant implications for this exercise that work to improve how the ARNG protects its networks:

> Each week the National Guard's 54 Cyber Network Defense Teams (CNDT) defend the Guard's cyber backbone, GUARDNet, from more than 100,000 cyber attacks. GUARDNet connects 3,000 armories in 11 different time zones across the continental U.S. along with Alaska, Hawaii, U.S. Virgin Islands, Guam and Puerto Rico. It provides a critical link for command and control of the National Guard and continuity of services in times of emergency.[128]

With the enactment of Cyber Shield 15, the exercise focus started to emphasize DSCA aspects that were facilitated with the Cyber City training tool developed by the SANS Institute, North Bethesda, MD, as "a real city with working infrastructure and power grids allowing for visual result of what the CND teams might be facing as a future mission in their state."[129] During Cyber Shield 16, the DSCA elements of the exercise were further refined with the addition of participants from industries such as water and electrical utility companies.[130]

Cyber Shield 2017 started in April 2017 with its purpose "to provide a collective training event to evaluate cyber operations and set the conditions for team validation."[131] The 2-week exercise was held in Camp W. G. Williams, UT, with the 75th Training Command (USAR) providing the exercise operations such as C2 and training analyses and assessments cells. ARNG and USAR from 44 states and territories worked together during Cyber Shield 2017 in an exercise environment that facilitated the ability "to share and collaborate in regards to tactics, techniques and

procedures" as well as "to test their skills in response to cyber-incidents in a multi-service environment."[132]

Other collaborative cyber training activities include Cyber Yankee, an annual exercise initiated in 2015 to bring Army and Air National Guard cyber defense and intelligence units together from the six New England states (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont). The initial exercise was developed with support from DHS, FEMA, the FBI, the MITRE Corporation, and the Massachusetts Institute of Technology's Lincoln Laboratories.[133] In 2017, Cyber Yankee included participation from government partners at the local, state, and federal level that engaged in "mock drills defending websites, databases, and computer programs against simulated cyber-attacks from hackers, criminal elements, and international non-state actors."[134] Also, the ARCOG and Carnegie Mellon University hosted the Cyber-X games in June 2017, a 5-day exercise involving almost 50 participants from Pennsylvania Army and Air National Guard units, Defense Information Systems Agency, and the Army Military Surface Deployment and Distribution Command.[135] The Cyber-X games provided advanced cybersecurity training and served as a prelude to the Cyber Endeavour conference held the following week at Carnegie Mellon University.

International Partnerships

The ARNG State Partnership Program (SPP) is a well-established vehicle initiated at the end of the Cold War "to build enduring mil-to-mil and civil-military relationships that improve long-term international security while building partnership capacity."[136]

Currently, there are 73 partnerships across all U.S. geographic combatant commands. During 2016, there were over 750 SPP events, including several related to cyberspace capability development.[137] Table 8 provides examples of cyber-related SPP events that have occurred within different combatant commands over the past 3 years.

State	SPP Partner Nation	Event
California	Ukraine	SMEE on cyber defense practices
Colorado	Jordan	SMEE on network defense and cyber intelligence
Hawaii	Indonesia	SMEE on cyber defense practices
Maryland	Estonia	Baltic Ghost exercise
Michigan	Latvia	Baltic Ghost exercise
Nebraska	Czech Republic	NATO cyber defense information sharing
New Hampshire	El Salvador	SMEE on cyber operation interoperability
New Jersey	Albania	SMEE on NATO cybersecurity interoperability
North Carolina	Moldova	SMEE on cyber defense practices
North Dakota	Ghana	Assessment of cybersecurity programs
Ohio	Serbia	Cyber Tesla 2017
Pennsylvania	Lithuania	Baltic Ghost exercise
Washington	Thailand	SMEE on improving cyber defenses
Note: SMEE = Subject Matter Expertise Exchange		

Table 8. Examples of Cyber-Related SPP Events[138]

With the increased concern for Russian military cyberspace activity, the SPP programs with the Baltic nations have grown in prominence. Baltic Ghost

started as a series of cyber defense workshops facilitated by U.S. European Command (USEUCOM) to build and sustain cyber partnerships amongst Estonia and the Maryland ARNG, Latvia and the Michigan ARNG, and Lithuania and the Pennsylvania ARNG.[139] Baltic Ghost transitioned to become a training exercise in September 2015—held simultaneously in the capitals of Tallinn (Estonia), Riga (Latvia), and Vilnius (Lithuania)—and focused on the coordination of responses to cyberattacks on critical infrastructure.[140] The exercise was most recently hosted by USEUCOM in June 2017, with participation by the ARNG state partners and assistance by the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. Baltic Ghost 2017 pursued an objective "to test cooperation between the three Baltic States and the United States in the event of an escalating cyber incident, the solution of which requires internationally coordinated joint action."[141] In August 2017, the Maryland ARNG also supported Estonia in the Baltic Jungle cyber exercise, which included opportunities to exchange experiences in the areas of cyber range development, education, and research.[142] In September 2017, members of the Ohio and Serbian armed forces worked together in the second annual Cyber Tesla exercise, which examined cyber incident preparation and responses processes.[143]

The ARNG also supports the education and training of partner nations at U.S. facilities. In July 2015, the ARNG PEC welcomed the first group on international military students for a 6-week integrated information technology training course. Four students from Bulgaria, Poland, and the Slovak Republic attended, with two Illinois Guardsmen training in the same class with their Polish state partner.[144]

RECOMMENDATIONS

This monograph provides a brief overview of how Army Reserve component cyber capabilities are being integrated into a variety of DoD and state operations. Steady and significant progress in this process has been made since the establishment of the USCYBERCOM and the CMF. This section offers recommendations to help identify and resolve issues that challenge the utility and effectiveness of future ARNG and USAR operations.

Recommendation 1

The Army and DoD need to establish and maintain a database of Reserve component cyberspace capabilities that is readily available for state or federal emergency responses.

This recommendation was also raised in a 2016 report—GAO-16-574—that calls for the Secretary of Defense to maintain such a database "to ensure that decision-makers have immediate visibility into all capabilities of the National Guard that could support civil authorities in a cyber incident."[145] However, for the Army, this must be a team effort that includes the Army G-3/5/7, the state adjutant generals, and chiefs of the NGB and USAR. While establishing the initial database is not trivial, it is probably the easiest part of the task. The real challenge will be to establish procedures for the regular review, update, and distribution of changes as well as methods for ensuring changes are incorporated into the myriad plans at the state, local, tribal, territorial, interagency, and federal levels. Once established, annual exercises such as Cyber Guard and Cyber Shield could offer opportunities to improve the accuracy of the database, especially if review of the database was included as an exercise objective.

Recommendation 2

DoD should work with DHS to clarify the currency and applicability of a cyber incident response annex to the NRF.

The current version of the NRF (3d Edition, June 2016) notifies readers that all response annexes (including the cyber incident annex) that appeared in the early version of the NRF have been moved to the FIOP. However, the current version of the FIOP (2d Edition, August 2016) does not include these annexes; in fact, it actually refers the matter of cyber incident response back to the NRF by stating, "For cyber incidents that have significant physical cascading effects, FEMA leads the physical consequence management effort in accordance with the National Response Framework."[146] Adding to the confusion of this vicious reference cycle, the current NCIRP (December 2016) states that the Secretary of DHS "shall regularly update, maintain, and exercise the Cyber Incident Annex to the NRF of the Department," another reference to an annex that no longer exists there.[147] Regardless of this procedural disconnect, the most current DHS *Cyber Incident Annex* available online is dated December 2004, and it could not incorporate the provisions of PPD-41. Finally, to help clarify operations between DHS and DoD, Army and joint doctrine should explicitly address DSCA for cyber incidents—at the very least pointing to key documents such as the NCIRP, even if they are currently flawed in their guidance on cyber incidents.

Recommendation 3

The Army should support DoD efforts to develop a Tier 1 cyber incident response exercise.

The 2016 report, GAO-16-574, contended that DoD does not have a Tier 1 exercise that fully addresses a complex DSCA cyber response scenario. The report also rebuffed DoD claims that the existing Cyber Guard exercises met the intentions of a Tier 1 exercise, with the GAO noting that these exercises are also used for the certification of military cyber teams, which limits the flexibility to address training requirements. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3500.01H, *Joint Training Policy for the Armed Forces of the United States*, notes that for Tier 1 events, "The desired end state in integrating a diverse audience in a joint training environment is to identify core competencies, procedural disconnects, and common ground to achieve U.S. unity of effort."[148] The Army should support the GAO's recommendation to improve the visibility of Army Reserve component forces in cyber incident response processes. The Army may also play a significant role in developing a Tier 1 cyber exercise through its role as Executive Agent for DoD Cyber Ranges as well as development and acquisition lead for the Persistent Cyberspace Training Environment.

Recommendation 4

The Army and DoD should develop a prioritization process to balance the contributions of Reserve component cyber units over the range of military operations.

Given the myriad responsibilities of USCYBERCOM and state governments, how will Reserve components prioritize their utilization of scarce military cyberspace resources if attacks occur simultaneously across multiple mission areas? Expectations for DoD missions alone include network defense, offensive cyber, Service and combatant command support, and DSCA. It is not in the best interests of national security that the assignment of Reserve component cyber force activity remains arbitrary and capricious, especially when one considers the speed at which cyberspace activities occur. The Army should work with the other Service cyberspace component commands and DoD to develop and optimize force balance solutions through existing large-scale exercises (such as Cyber Guard) that could be used as heuristics during crises.

Recommendation 5

The Army G-3/5/7 and the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) should catalog and leverage the resources of state and private cyber ranges with which ARNG units are developing partnerships.

In March 2016, the Secretary of the Army was officially designated as the DoD Executive Agent for Cyber Training Ranges, who in turn delegated the task to the Army Deputy Chief of Staff G-3/5/7.[149] Also, the Army's chief acquisition leader, the ASA(ALT), has ultimate responsibility to ensure the development of the DoD Persistent Cyberspace Training Environment. Both of these efforts may benefit by utilizing existing and planned state-sponsored cyber ranges discussed earlier in this monograph. Partnerships with these ranges could provide ready access to leading edge private sector technology at geographically diverse locations.

Recommendation 6

State emergency response plans should identify the National Guard capabilities available to address cyber incidents.

As presented in table 6, a sampling of emergency response plans from 11 states and the District of Columbia showed that only one plan contained any details on the ARNG cyber capabilities available to the governor and other state authorities. At the very least, these plans should list the location and skills of ARNG cyber units trained and certified in cyber defense operations; such an approach is consistent with guidance from the NGA.[150] To support this process, the NGB could develop and provide "boilerplate" information—such as the basic description of Defensive Cyberspace Operations Elements and cyber protection teams—to serve as the core input to the plans. It can be refined by the state adjutant general staff to highlight any unique aspects of a particular state's ARNG cyber force.

Recommendation 7

The NGB should conduct stakeholder management for the tasks and activities assigned to National Guard cyber units.

As discussed herein, there are myriad assignments that ARNG cyber units are able to fulfill for a diverse group of stakeholders—state governments, ARCYBER, USCYBERCOM, DHS, and private industry, to name a few. Each stakeholder has requirements, expectations, and interests that may conflict with those of other stakeholders. Collectively, these tacit obligations most likely exceed the capability and capacity of

the ARNG to deliver. The NGB should identify these stakeholders as well as their unique desires and determine how to achieve the best balance of utilization to meet the collective needs of all stakeholders. This process should include a robust communication forum amongst the stakeholders and methods to help the group determine not only what ARNG cyber units are capable of doing, but also what they should be doing to best leverage their unique potential.

CLOSING THOUGHTS

Cyberspace operations have become pervasive in all areas of modern life. The continuing development of Army and DoD Reserve component cyberspace units can leverage the capabilities and experience of industry and academia to help protect critical information infrastructure and enhance national security. Current efforts to integrate cyber Reserve components appear to be sufficient for certain specific applications, but the Nation has yet to benefit from the potential synergy offered by an optimized blend of these capabilities. Granted, some of the issues identified here may be common to other applications of Reserve component forces. However, the negative impacts may be more significant for cyber units due to the ethereal nature of cyberspace operations that are far less intuitive than those occurring in the physical world. In the end, it would be regrettable if well-qualified cyber forces were not brought to bear to help ameliorate a crisis simply because leaders and their staffs were ignorant of their existence.

ENDNOTES

1. "Title 10 and Title 32, United States Code," Washington, DC: U.S. Government Printing Office, August 10, 1956, pp. 10-11, available from *https//www.gpo.gov/fdsys/pkg/STATUTE-70/pdf/STATUTE-70A-Pg1.pdf*, accessed October 31, 2017. The following paragraphs are of interest to this monograph:

> **§ 263. Basic policy for order into Federal service**
>
> Whenever Congress determines that more units and organizations are needed for the national security than are in the regular components of the ground and air forces, the Army National Guard of the United States and the Air National Guard of the United States, or such parts of them as are needed, together with units of other reserve components necessary for a balanced force, shall be ordered to active duty and retained as long as so needed [emphasis in original]. (p. 11)
>
> **§ 265. Policies and regulations: participation of reserve officers in preparation and administration**
>
> Within such numbers and in such grades and assignments as the Secretary concerned may prescribe, each armed force shall have officers of its reserve components on active duty (other than for training) at the seat of government, and at headquarters responsible for reserve affairs, to participate in preparing and administering the policies and regulations affecting those reserve components. While so serving, such an officer is an additional number of any staff with which he is serving [emphasis in original]. (p. 11)

2. *2018 National Guard Bureau Posture Statement: Building a Force for the Future*, Washington, DC: National Guard Bureau, 2017, p. 10.

3. "About Us," U.S. Army Reserve website page, n.d., available from *http://www.usar.army.mil/About-Us/*, accessed November 16, 2017.

4. "Understanding the Guard's Duty Status," NGAUS [National Guard Association of the United States] Fact Sheet, n.d., available from *http://congfamilyreadiness.net/wp-content/*

uploads/2017/06/TAA-Guard-Statues.pdf, accessed November 19, 2018.

5. Ibid.

6. "Dual Status Commander," National Guard Fact Sheet, December 2017, available from *https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/Dual%20Status%20Commander%20Fact%20Sheet%20(Dec.%202017).pdf*, accessed December 17, 2018..

7. *The DoD Cyber Strategy*, Washington, DC: U.S. Department of Defense, April 2015, p. 18.

8. Ibid., p. 22.

9. "U.S. Cyber Command (USCYBERCOM)," factsheet, U.S. Strategic Command, available from *http://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf,* accessed September 3, 2017. The USCYBERCOM mission is:

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

10. "All Cyber Mission Force Teams Achieve Initial Operating Capability," news release, Fort Meade, MD: U.S. Cyber Command, October 24, 2016, available from *https://dod.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/*, accessed November 19, 2018.

11. Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command before the Senate Committee on Armed Services, U.S. Senate, 115th Cong., 1st sess., May 9, 2017, available from *https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf*, accessed November 17, 2017.

12. Statement by Lieutenant General Paul M. Nakasone, Commanding General, U.S. Army Cyber Command before the Subcommittee on Cybersecurity, Committee on Armed Services,

U.S. Senate, 115th Cong., 1st sess., May 23, 2017, pp. 2 and 7, available from *https://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf*, accessed August 15, 2017.

13. Mike Milord, "Army Cyber Command, Army Guard sign memorandum to integrate cyber protection team," U.S. Army News, June 5, 2014, available from *https://www.army.mil/article/127442/army_cyber_command_army_guard_sign_memorandum_to_integrate_cyber_protection_team*, accessed November 5, 2017. The article stated the responsibilities of the Active Duty ARNG CPT as:

> The 1636th CPT will conduct one or a combination of the following missions: defensive cyberspace operations, cyber command readiness inspections, vulnerability assessments, cyber operational forces support to emulate threats, critical infrastructure assessments, theater security cooperation and Federal Emergency Management Agency support.

14. Mike Milord, "Guard Activates First Cyber Protection Team, Issues New Shoulder Sleeve Insignia," U.S. Army News, October 20, 2014, available from *https://www.army.mil/article/136100/guard_activates_first_cyber_protection_team_issues_new_shoulder_sleeve_insignia*, accessed October 30, 2017.

15. Gary A. Ropers, "Cyber Warrior: The Role of the National Guard," Strategy Research Project, Carlisle, PA: U.S. Army War College, April 15, 2014, pp. 18-20, available from *http://publications.armywarcollege.edu/pubs/228.pdf*, accessed November 19, 2018.

16. Joe Marty, "A Year on a Cyber Protection Team," *Cyber: The Magazine of the Military Cyber Professionals Association*, Vol. 1, No. 2, Fall 2016, pp. 42-47, available from *http://magazine.milcyber.org/stories/ayearonacyberprotectionteam*, accessed November 19, 2018.

17. Emmett Lawrence, "The Army National Guard (ARNG) Cyber Protection Team (CPT) Benefit to Critical Infrastructure," webinar presentation, Manufacturing Summit 2016, Mississippi State University Franklin Furniture Institute, Starkville, MS, slides 7 and 12, available from *http://www.ffi.msstate.edu/webinars/summit_2016/lawrence.pdf,* accessed October 22, 2017.

18. "Information Technology Training Center (ITTC)," Professional Education Center website page, available from *http://www.pec.ng.mil/ITTC*, accessed November 16, 2017. Further details on ITTC courses can only be accessed through a portal that is restricted to authorized government users.

19. Aaron K. Gatzke, "Professional Education Center offers Cyber Common Technical Core training," *National Guard News*, July 17, 2015, available from *http://www.nationalguard.mil/News/Article-View/Article/610060/professional-education-center-offers-cyber-common-technical-core-training/*, accessed November 7, 2017. According to the posted article, the Cyber Common Technical Core (CCTC) provided training in the following areas:

> Designed to meet equivalency of current National Security Agency (NSA), Intermediate Cyber Core (ICC) training, CCTC will enhance individual skills giving them the background they need to properly defend against cyber-attacks safeguarding our nation's military communications networks.
>
> The training is designed for enlisted soldiers, warrant officers, and commissioned officers. When trained, Service Members will be ready to serve in various Cyber work roles within the CPTs and other formations the same way current Guard units do when needed. The long range goal for PEC is to open the CCTC to other DoD agencies, allowing all services to speak a common language and have similar skill sets.
>
> The CCTC course is scheduled to be an 8 week course with four phases. The first phase will cover the Windows operating system with phase two covering the Linux operating system and the differences between the two. Phase three will cover networking, and the fourth phase provides training on security concepts. Phase four will culminate with several scenario based, real-world situations to test the student's fundamental understanding of the curriculum.

20. Joe Lacdan, "Newly Activated Guard Unit to bolster Army Cyber Forces," Army News Service, August 18, 2017, available from *https://www.army.mil/article/192601/newly_activated_guard_unit_to_bolster_army_cyber_forces*, accessed August 15, 2018. The article describes Task Force Echo as:

> The Guard recruited Soldiers from California, Georgia, Michigan, Indiana, Utah, Ohio and Virginia for their skills and experience in systems and cybersecurity. The Soldiers were mobilized for 400 days and will fall under the 780th Military Intelligence Brigade during their active duty.
>
> The TF Echo Soldiers are drawn from a wide palette of civilian sector skillsets that include experience in government cybersecurity to expertise in information technology. The Soldiers range in rank from junior enlisted to warrant officers and field grade officers. TF Echo will provide critical support for U.S. Cyber Command to carry out cyberspace operations against adversaries.
>
> TF Echo takes over and dramatically expands the role originally pioneered by 169th Cyber Protection Team: to engineer, operate and maintain critical network infrastructure.

21. Cotton Puryear, "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade," Virginia National Guard Public Affairs Office, September 18, 2017, available from *https://http://www.dvidshub.net/news/248764/91st-cyber-brigade-activated-army-national-guards-first-cyber-brigade*, accessed August 15, 2018. The article provides further details on the cyber battalions:

> The 91st Cyber Brigade was reflagged from the 91st Troop Command, and the Fairfax-based 123rd Data Processing Unit was divided into the 123rd and 124th Cyber Protection Battalions. The brigade will also serve as the higher headquarters for 125th and 126th Cyber Battalions stationed in Columbia, South Carolina, and Hanscom Air Force Base in Bedford, Massachusetts, as well as an additional battalion that has not been stationed. The 10 previously approved Army Cyber Protection Teams stationed across the country will also align under the 91st Cyber Brigade for training and validation management.
>
> The 91st Cyber Brigade consists of approximately 950 traditional status Army National Guard officers, warrant officers and enlisted Soldiers across units in the 30 states, and the cyber battalion headquarters will each consist of approximately 25 personnel with each company consisting of about 35-40 personnel.

> Each cyber protection battalion will have four subordinate units, a cyber security company, a cyber warfare company, and two cyber protection teams. In Virginia, the 133rd Cyber Security Company and 143rd Cyber Warfare Company will fall under the 123rd Cyber Protection Battalion and 134th Cyber Security Company and 144th Cyber Warfare Company will fall under the 124th.

22. Jeffrey W. Talley, Lieutenant General, 32d Chief of Army Reserve and 7th Commanding General, U.S. Army Reserve Command, "The 2016 Posture of the United States Army Reserve, A Global Operational Reserve Force," Senate Appropriations Committee, 114th Cong., 2d sess., March 16, 2016, p. 14, available from *https://www.appropriations.senate.gov/imo/media/doc/031616%20-%20LTG%20Talley%20-%20Army%20Reserve%20-%20Testimony.pdf*, accessed October 30, 2017. Talley went on to say:

> As the Army continues to develop its cyber needs, the Army Reserve will continue to grow its cyber force through the Total Army Analysis process. We will also continue to collaborate with all Cyber Mission Force [CMF] partners to develop new and innovative training strategies, to include public and private partnerships with academia, industry and government, to lessen the length of time needed for training future cyber warriors by leveraging civilian-acquired education and work experience.

23. *The ARCOG Net*, Vol. 1, No. 1, Spring 2017, p. 5.

24. Travis Good, "Army Reserve Trains for Information Assurance," *Signal,* January 2004, available from *https://www.afcea.org/content/?q=army-reserve-trains-information-assurance*, accessed November 4, 2017. The details of the training provided by the Software Engineering Institute include:

> The SEI is a research and development organization federally funded by the U.S. Defense Department. Much of the institute's work relates to the security of information systems. For example, the SEI operates the CERT Coordination Center (CERT/CC) and other programs that help organizations develop the ability to protect their networked systems against current and emerging cyberthreats. The SEI is working closely with the office of the Army's chief information officer (CIO), which oversees the

> entire project to ensure that training for the ARIOC satisfies Army goals and requirements.
>
> The institute is assembling a suite of information assurance and security training activities developed especially for the ARIOC, including a highly technical course in advanced information assurance. The course is designed for soldiers with three to five years of experience in system or network administration and preferably one year of experience in security administration. Before enrolling in this advanced course, soldiers acquire a broad technical foundation by completing the Information Security for Technical Staff course, the SEI's introduction to information security.
>
> The advanced course builds on the concepts and exercises covered in the introductory course and contains 40 hours of substantive technical content, including lecture and laboratory exercises. Eighty percent of that time is devoted to hands-on technical tasks.

25. Talley, "The 2016 Posture of the United States Army Reserve," p. 19.

26. Erick Yates, "Fast Forward Year for Army Reserve Cyber Unit," *U.S. Army Reserve News*, October 18, 2017, available from *http://www.usar.army.mil/News/Article/1346415/fast-forward-year-for-army-reserve-cyber-unit/*, accessed October 30, 2017.

27. "Army Reserve Cyber Integration," Stand-To! The Official Focus of the U.S. Army, February 22, 2017, available from *https://www.army.mil/standto/2017-02-22*, accessed October 23, 2017.

28. Erick Yates, "New Army Reserve Cyber Course Provides Advanced Training Opportunity," *U.S. Army Reserve News*, May 16, 2017, available from *https://www.usar.army.mil/News/News-Display/Article/1184428/new-army-reserve-cyber-course-provides-advanced-training-opportunity/,* accessed November 19, 2018.

29. Brent Powell, "Reserve Officers Are First to Finish Cyber Operations Course," *Fort Gordon Globe,* August 4, 2017, available from *http://www.fortgordonglobe.com/news/2017-08-04/Front_Page/Reserve_officers_are_first_to_finish_Cyber_Operati.html*, accessed November 19, 2018.

30. "Command Notes," *The ARCOG Net*, Vol. 1, No. 1, Spring 2017, available from *https://static.dvidshub.net/media/pubs/pdf_32480.pdf*, accessed November 19, 2018. The correlation of specific CPTs to their assigned regional Cyber Protection Center for the table was taken from the unit logos that appear on the left border of pp. 1 and 5 of this newsletter.

31. *Department of Defense Directive 3025.18, Defense Support of Civil Authorities* (DSCA), Washington, DC: Under Secretary of Defense for Policy, change 1, September 21, 2012, p. 16. The definition of DSCA per DoDD 3025.18 is:

> Support provided by U.S. Federal military forces, DoD civilians, DoD contract personnel, DoD Component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in Title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. Also known as civil support.

32. *Chairman of the Joint Chiefs of Staff Manual* (CJCSM) *6510.01B, Cyber Incident Handling Program*, Washington, DC: Joint Chiefs of Staff, July 10, 2012, p. A-5. Enclosure A of this document includes the following responsibilities for USCYBERCOM:

> (c) Coordinate with the Department of Homeland Security (DHS) and other federal agencies for incidents related to cyberspace involving the Department of Defense. As appropriate, notify and/or coordinate with the United States Computer Emergency Readiness Team (US-CERT) on cyberspace incidents.
>
> (d) Coordinate with USNORTHCOM, National Guard Bureau, and USPACOM for cyber incidents that involve the DHS and other federal agencies where Defense Support of Civil Authorities is involved.

33. *National Response Framework*, 3d Ed., Washington, DC: Department of Homeland Security, June 2016, p. i., available from *http://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf*,

accessed November 8, 2017. The purpose and scope of the NRF are stated as follows:

> The National Response Framework is a guide to how the Nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities across the Nation. This Framework describes specific authorities and best practices for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters. The National Response Framework describes the principles, roles and responsibilities, and coordinating structures for delivering the core capabilities required to respond to an incident and further describes how response efforts integrate with those of the other mission areas. This Framework is always in effect and describes the doctrine under which the Nation responds to incidents. The structures, roles, and responsibilities described in this Framework can be partially or fully implemented in the context of a threat or hazard, in anticipation of a significant event, or in response to an incident. Selective implementation of National Response Framework structures and procedures allows for a scaled response, delivery of the specific resources and capabilities, and a level of coordination appropriate to each incident.

34. Ibid., pp. i, 5-7.

35. *Strategy for Homeland Defense and Defense Support of Civil Authorities*, Washington, DC: Department of Defense, February 2013, available from *http://www.dtic.mil/dtic/tr/fulltext/u2/a582464.pdf*, accessed November 19, 2018.

36. Joint Chiefs of Staff, Joint Publication (JP) 3-28, *Defense Support of Civil Authorities*, Washington, DC: Joint Chiefs of Staff, July 31, 2013. JP 3-28 contains only one paragraph regarding DSCA cyberspace support:

> 8. Cyberspace Support.
>
> During DSCA operations, DOD forces may be required to assist state and local networks to operate in a disrupted or degraded environment. The Services may be requested to support the remediation and creation of critical emergency

telecommunication networks. They may also be required to provide cyberspace support services to secure critical information infrastructure.

See Joint Chiefs of Staff, JP 3-12(R), *Cyberspace Operations*, Washington, DC: Joint Chiefs of Staff, February 5, 2013, p. V-14, for more information on military support in cyberspace.

37. Ibid., p. III-1. JP 3-12(R) defers to the NRF for cyberspace-related DSCA guidance:

> d. National Incident Response. In addition to DOD's responsibility to defend the Nation, DOD provides defense support of civil authorities (DSCA), as directed. DOD coordinates with DHS and other interagency partners, as described in the National Response Framework.

38. Headquarters, Department of the Army, Army Doctrine Reference Publication (ADRP) 3-28, *Defense Support of Civil Authorities*, Washington, DC: Headquarters, Department of the Army, June 14, 2013.

39. Headquarters, Department of the Army, Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, DC: Headquarters, Department of the Army, April 11, 2017, p. iv. The Preface of FM 3-12 states its applicability to the total force: "FM 3-12 applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated."

40. *National Response Framework*, Second Ed., Washington, DC: Department of Homeland Security, May 2013, pp. 37-38, available from *https://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf*, accessed November 8, 2017. This version of the NRF included the following Incident Annexes:

> NRF Incident Annexes describe coordinating structures, in addition to the ESFs [Emergency Support Functions], that may be used to deliver core capabilities and support response missions that are unique to a specific type of incident. Incident annexes also describe specialized response teams and resources, incident-specific roles and responsibilities,

and other scenario-specific considerations. NRF Incident Annexes address the following contingencies or hazards:

- Biological Incident
- Catastrophic Incident
- Cyber Incident
- Food and Agriculture Incident
- Mass Evacuation Incident
- Nuclear/Radiological Incident
- Terrorism Incident Law Enforcement and Investigation.

41. *Cyber Incident Annex, National Response Plan*, Washington, DC: Department of Homeland Security, December 2004, p. CYB-1, available from *https://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf*, accessed November 8, 2017. The reference to this annex currently of "Last Updated: March 7, 2012" can be found at the "Cyber Incident Annex" page of the FEMA website, available from *https://www.fema.gov/media-library/assets/documents/25556*, accessed November 9, 2017. The scope of the annex contents is described as:

> This annex describes the framework for Federal cyber incident response coordination among Federal departments and agencies and, upon request, State, local, tribal, and private-sector entities. The Cyber Incident Annex is built primarily upon the National Cyberspace Security Response System (NCSRS), described in the National Strategy to Secure Cyberspace. The NCSRS is a public-private architecture that provides mechanisms for rapid identification, information exchange, response, and remediation to mitigate the damage caused by malicious cyberspace activity.
>
> This framework may be utilized in any Incident of National Significance with cyber-related issues, including significant cyber threats and disruptions; crippling cyber attacks against the Internet or critical infrastructure information systems; technological emergencies; or Presidentially declared disasters.

42. Ibid., p. CYB-3. The cyberspace organization for DoD in this document reflects its state in December 2004 and not the current organization:

> Department of Defense (DOD): DOD operates a network of Computer Emergency Response Teams which are staffed 24/7. These teams are coordinated by the Joint Task Force—Global Network Operations (JTF-GNO) to identify, mitigate, and, if necessary, respond to cyber attacks. U.S. Strategic Command (USSTRATCOM) and JTF-GNO also provide continuous intelligence analysis of cyber threats. Finally, the Law Enforcement/Counter Intelligence Center, located at the JTF-GNO, brings together DOD's law enforcement and counterintelligence organizations in response to cyber incidents.

43. For contextual details surrounding PPD-41, see Jeffrey L. Caton, *Evaluation of the 2015 DoD Cyber Strategy: Mild Progress in a Complex and Dynamic Military Domain*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, November 2, 2017, pp. 44-46, available from *https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1372,* accessed November 19, 2018.

44. *National Response Framework*, 3d Ed., p. 2. The movement of the Cyber Incident Annex (and other similar annexes) was explained as: "Note that the incident annexes, which address response to specific risks and hazards, can now be found as annexes to the Response FIOP rather than as supplements to the NRF."

45. *Response Federal Interagency Operational Plan*, 2d Ed., Washington, DC: Department of Homeland Security, August 2016, available from *https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf*, accessed November 9, 2017.

46. "Federal Interagency Operational Plans," FEMA website, available from *https://www.fema.gov/federal-interagency-operational-plans*, accessed November 9, 2017.

47. *National Cyber Incident Response Plan*, Washington, DC: Department of Homeland Security, December 2016, p. 4, available from *https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf*, accessed November 8, 2017. The NCIRP makes clear its connection to PPD-41:

> The National Cyber Incident Response Plan (NCIRP or Plan) was developed according to the direction of PPD-41 and

leveraging doctrine from the National Preparedness System to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure. The NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations. Authored in close coordination with government and private sector partners, the NCIRP expounds upon the concurrent lines of effort, defined by PPD-41, for how the Federal Government will organize its activities to manage the effects of significant cyber incidents. The concurrent lines of effort are threat response, asset response, intelligence support, and the affected entity, which undertakes efforts to manage the effects of the incident on its operations, customers, and workforce.

48. Ibid., p. 6.

49. Ibid., pp. 7-8.

50. Ibid., pp. 8, 38-39. The NCIRP uses the following definitions derived from PPD-41:

> Cyber Incident. An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
>
> Significant Cyber Incident. A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. (p. 8)

51. Ibid., p. 26. The NCIRP outlines the importance of the Cyber UCG:

> While existing policies and coordinating structures can handle the vast majority of cyber incidents, significant cyber

incidents may require a unique approach to coordinating the whole-of-Nation response. Pursuant to PPD-41, the U.S. Government will establish a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident, as well as for integrating SLTT governments and private sector partners into incident response efforts as appropriate for the specific incident. Other coordinating structures should be prepared to integrate and interoperate with a Cyber UCG, if one is established.

52. Ibid., p. 28. The NCIRP describes the role of the CRG as:

> To coordinate policy at the National level, PPD-41 assigns the Assistant to the President for Homeland Security and Counterterrorism the responsibility to convene and chair the CRG to coordinate development and implementation of Federal Government policy and strategy with respect to significant cyber incidents affecting the Nation or its interests abroad. The CRG will coordinate the development and implementation of U.S. Government policy and strategy for responding to significant cyber incidents. Federal departments and agencies, including relevant cybersecurity centers, are invited to participate in the CRG, as appropriate, based on their respective roles, responsibilities, and expertise or in the circumstances of a given incident or grouping of incidents. Federal agencies, including SSAs [Sector Specific Agencies] that regularly participate in the CRG must establish and implement enhanced coordination procedures to manage significant cyber incidents that exceed their standing response capacities.

53. Ibid., pp. 14 and 19. DoD's primary roles in the NCIRP are summarized as:

> DoD is responsible for threat response to cyber incidents affecting DoD assets and the DoD Information Network (DoDIN). DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by the lead federal agency, and approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces. (p. 14)

54. Ibid., p. 17. Possible National Guard roles in the NCIRP are summarized as:

> The National Guard is a force with dual state and federal roles. National Guard forces have expertise in critical response functions and many also have expertise and capabilities in cyber activities. At the direction of a State Governor and Adjutant General, the National Guard may perform state missions, including supporting civil authorities in response to a cyber incident. In certain circumstances, as permitted by law, the National Guard may be requested to perform federal service or be ordered to active duty to perform DoD missions, which could include supporting a federal agency in response to a cyber incident.

55. Ibid., pp. 20-21.

> The DoD actively characterizes and assesses foreign cybersecurity threats and informs the relevant interagency partners of current and potential malicious cyber activity. Upon request, the DoD intelligence components may provide technical assistance to U.S. Government departments and agencies; other DoD elements may provide support to civil authorities in accordance with applicable law and policy. The IC may identify classified information, indicating a potential credible cyber threat to an SLTT, critical infrastructure owner/operator, or other private sector entity. In accordance with Section 4 of Executive Order 13636, DHS and/or the FBI provide appropriate notification to the targeted entity. Where available, declassified threat detection and mitigation information may also be provided. In circumstances where the source of threat identification, nature of the adversary, or other factors of national security concern exist, incident response processes and procedures adhere to all guidelines and directions for handling matters of national security.

56. Ibid., pp. 43-44. The four non-DoD cybersecurity centers identified in the NCIRP are: DHS: National Cybersecurity and Communications Integration Center (NCCIC); FBI: National Cyber Investigative Joint Task Force (NCIJTF); ODNI: Cyber Threat Intelligence Integration Center (CTIIC); and, Intelligence Community-Security Coordination Center (IC-SCC).

57. For details on the 10 FEMA regions, see "FEMA Regional Contacts," FEMA website, available from *https://www.fema.gov/fema-regional-contacts*, accessed November 10, 2017.

58. *National Cyber Incident Response Plan,* pp. 33-34.

59. Ibid., pp. 21-25. The 14 core capabilities of the NCIRP are: Access Control and Identity Verification; Cybersecurity; Forensics and Attribution; Infrastructure Systems; Intelligence and Information Sharing; Interdiction and Disruption; Logistics and Supply Chain Management; Operational Communications; Operational Coordination; Planning; Public Information and Warning; Screening, Search, and Detection; Situational Assessment; and, Threats and Hazards Identification.

60. Ibid., p. 28.

61. *DOD Is Taking Action to Strengthen Support of Civil Authorities*, Report GAO-15-686T, Washington, DC: U.S. Government Accountability Office, June 10, 2015, p. 6, available from *https://www.gao.gov/products/GAO-15-686T*, accessed October 28, 2017. The GAO noted the failure of DoD to update its DSCA guidance as recommended:

> DOD has agreed to take steps to align cyber-support roles and responsibilities. In October 2012 [report GAO-13-128], we found that DOD had not updated its DSCA guidance, such as joint doctrine, to ensure that it was consistent with national plans and preparations for domestic cyber incidents. We recommended that DOD align guidance on preparing for and responding to domestic cyber incidents with national-level guidance to include roles and responsibilities. DOD partially concurred with this recommendation. However, the department has not yet taken action that meets the intent of the recommendation.

62. *DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, Report GAO-16-332, Washington, DC: U.S. Government Accountability Office, April 4, 2016, p. 20, available from *https://www.gao.gov/products/GAO-16-332*, accessed October 27, 2017. Further details on the report conclusion are:

> DOD has developed a significant body of guidance on how the department is to effectively provide support to civil authorities in a broad range of circumstances. However, the absence of clarity in roles and responsibilities to address a cyber incident represents a clear gap in guidance. The gap, and the uncertainty that results, could hinder the timeliness or effectiveness of critical DOD support to civil authorities during cyber-related emergencies that DOD must be prepared to provide. In addition to the relevant DOD guidance—such as DOD directives or instructions—that are important for guiding DOD planning and processes, the comprehensive plan DOD is required by Congress to develop in 2016 would be another opportunity for DOD to address the gap that we identified.

63. Report GAO-16-332, pp. 12-20.

64. Ibid., p. 6. The report included the following assumption as footnote 27:

> The National Guard normally responds to domestic emergencies in a state active duty status. Under state active duty, the National Guard can be used for state purposes in accordance with the state constitution and statues, and the respective state is responsible for National Guard expenses.

65. Ibid., p. 9. See also *Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense*, Washington, DC: Department of Defense, August 21, 2014; and *National Guard Bureau Cyber Mission Analysis Assessment*, Washington, DC: Chief, National Guard Bureau, September 29, 2014. Both of these reports were published as For Official Use Only and as such will not be discussed further. The GAO report summarized the finding of these reports as:

> In response to a provision in the National Defense Authorization Act for Fiscal Year 2014, DOD issued a cyber mission analysis report on the department's efforts to conduct cyberspace operations using its total cyber forces including its active and reserve components—the Army National Guard of the United States, Army Reserve, Air Force Reserve, Air National Guard of the United States, Marine Corps Reserve, and Navy Reserve. In this analysis, DOD found advantages to using its reserve components for

> cyber missions such as load sharing and providing surge capabilities. The report recommends, among other things, that National Guard state active-duty policies and processes be clarified to ensure unity of effort between DOD and National Guard forces, and that the National Guard focus on support roles such as coordinate, train, advise, and assist with state or local agencies or private industry when directed by their respective governor or authorized by DOD. Additionally, section 933(e) of the National Defense Authorization Act for Fiscal Year 2014 mandated that the Chief of the National Guard Bureau assess DOD's description of the role of the National Guard in supporting DOD's cyber operations. In September 2014, the National Guard Bureau issued its report highlighting, among other things, that the bureau concurs with DOD's finding that the cyber reserve components can offer load sharing and surge capacity and supports DOD's plan to integrate reserve personnel into cyberspace forces.

66. *DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises*, Report GAO-16-574, Washington, DC: U.S. Government Accountability Office, September 6, 2016, available from *https://www.gao.gov/products/GAO-16-574*, accessed August 22, 2017.

67. Ibid., p. 2.

68. Ibid., p. 14.

69. "NG Cyber Defense Team," National Guard fact sheet, October 2014, available from *http://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/NG%20Cyber%20Defense%20Team%20Fact%20Sheet%20(Dec.%202017).pdf*, accessed November 19, 2018.

70. U.S. Cyber Command Public Affairs, "Cyber Guard 15 Fact Sheet," p. 3, available from *http://archive.defense.gov/home/features/2015/0415_cyber-strategy/cyber_guard_15_fact_sheet_010715_f.pdf*, accessed November 19, 2018. The fact sheet summarizes the evolution of Cyber Guard exercises:

> Cyber Guard 13-1 expanded in scope as a collaborative, tactical-level exercise focused on state and national defensive cyberspace operations and included Federal Bureau of Investigation and Department of Homeland Security

National Cybersecurity and Communications Integration Center (NCCIC) participation.

Cyber Guard 14-1 improved realism by requiring teams to report information to state and Federal cyber centers outside of the exercise network. Six state Joint Operations Centers (JOCs), the DHS NCCIC watch floor, and the FBI Cyber Task Force and National Cyber Intelligence Joint Task Force (NCIJTF) were actively engaged throughout the exercise.

Cyber Guard 15 is the fourth in this series, and its expanded scope reflects the growing requirement to improve preparedness across government and the private sector. The addition of private sector participation, coordinated with the DHS Office of Infrastructure Protection Sector Outreach & Programs Division, represents a shift from a whole-of-government to whole-of-nation approach to cybersecurity preparedness and response. Cyber Guard 15 also provided another opportunity for USCYBERCOM to assess proficiency and operational readiness of its CMF teams.

71. U.S. Cyber Command Public Affairs, "Cyber Guard 16 Fact Sheet," available from *https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Cyber-Guard-16-FactSheet-FINAL.pdf,* accessed November 19, 2018.

72. "Allies, Partners Observe Cyber Guard Exercise," U.S. Cyber Command News Release, July 5, 2017, available from *https://dod.defense.gov/News/Article/Article/1238082/allies-partners-observe-cyber-guard-exercise/,* accessed November 19, 2018.

73. "Cyber Guard 15 Fact Sheet," p. 1. The description of the Cyber Guard objective is:

Continue efforts to build a Persistent Training Environment for cyberspace forces across the Department of Defense. This Persistent Training Environment includes a closed exercise network, training event planning, management and assessment, a live expert opposing force and transport layer to enable distributed participation in the environment. This Persistent Training Environment will be accessible to other U.S. government departments, allies and other partners and will set the foundation for whole-of-nation, full-spectrum cyberspace operations training.

For details on the Army's role as Persistent Cyber Training Environment (PCTE) acquisition lead, see Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview: United States Department of Defense, Fiscal Year 2018 Budget Request*, Washington, DC: Department of Defense, May 2017, p. 3-9, available from *https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2018/fy2018_Budget_Request_Overview_Book.pdf*, accessed November 19, 2018.

74. Report GAO-16-574, p. 20.

75. United States Cyber Command, "Cyber Support to DSCA: Command and Control," briefing to support Exercise Cyber Guard 17, January 13, 2017.

76. Reserve Forces Policy Board, *Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force*, Report to the Secretary of Defense, RFPB Report FY14-03, Falls Church, VA: Reserve Force Policy Board, August 18, 2014, available from *http://cc.bingj.com/cache.aspx?q=Department+of+Defense+Cyber+Approach%3a+Use+of+the+National+Guard+and+Reserve+in+the+Cyber+Mission+Force&d=495727877837490&mkt=en-US&setlang=en-US&w=BWgH5OGrM0XOT0M74xBCx_stRP_LySYm,* Washington, DC: Office of the Secretary of Defense, 2014, p. 2, available from *https://rfpb.defense.gov/Portals/67/Documents/Reports/Annual%20Report/2015%20RFPB%20Annual%20Report%20Final.pdf*, accessed November 17, 2017. The annual report provides this summary of the study findings:

1. Include Reserve Components in Cyber Mission Force [CMF] requirements in order to leverage Reserve Component reduced cost, civilian/AC acquired skill/experience, continuity and longevity.
2. As part of a Total Force solution, re-evaluate the composition, size and force mix of the planned Cyber Mission Force [CMF] by FY 2017, and refine as needed based on changing threats, team effectiveness, capability, required capacity and cost.
3. The Department of Defense should study, and then assign executive responsibility to a single Service for the full range of joint cyber training.

4. Recruit highly skilled members via a professional accessions and retention program to fill both AC and Reserve Component requirements within the Cyber Mission Force [CMF].

77. Talley, "2016 Posture of the United States Army Reserve," p. 14.

78. Panayotis A. Yannakogeorgos and John P. Geis II, *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce*, Maxwell Air Force Base, AL: Air University Press, June 2016, p. 143, available from *http://www.dtic.mil/dtic/tr/fulltext/u2/1017510.pdf*, accessed November 5, 2017.

79. Statement by Vice Admiral Michael M. Gilday, Commander, U.S. Fleet Cyber Command, U.S. Tenth Fleet, before the Senate Armed Services Committee Subcommittee on Cybersecurity, Cyber Posture, U.S. Senate, 115th Cong., 1st sess., May 23, 2017, p. 7, available from *https://www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf*, accessed November 17, 2017.

80. "960th Operations Group Units," Official 960th Operations Group website, available from *http://www.960cyber.afrc.af.mil/Units/*, accessed November 17, 2017. For further information on the cyberspace capabilities of other Services, see Jeffrey L. Caton, *Implications of Service Cyberspace Component Commands for Army Cyberspace Operations,* Carlisle, PA: Strategic Studies Institute, U.S. Army War College, forthcoming. The reader may contact the author for an interim copy.

81. William Matthews, "None Too Soon," *National Guard*, Vol. 70, No. 10, October 2016, pp. 18-23.

82. Andria Allmond, "Pennsylvania Cyberspace Operations Squadron to Become Prime Force in Cyber Defense," *National Guard News*, January 26, 2017, available from *http://www.nationalguard.mil/News/Article/1060842/pennsylvania-cyberspace-operations-squadron-to-become-prime-force-in-cyber-defe/*, accessed November 8, 2017.

83. U.S. Army Training and Doctrine Command, "The Cyber Private Public Partnership," Stand-To! The Official Focus of the U.S. Army, September 21, 2015, available from *https://www.army.mil/standto/archive_2015-09-21/,* accessed December 18, 2018. The

article describes key aspects of the Cyber P3 initiative related to recruitment and retention:

> **What has the Army Reserve done?**
>
> The Army Reserve has partnered with six top-tier universities and 12 employers in a first-of-its-kind effort to create and build cyber development programs for citizen Soldiers and units. These university programs provide skills development and advancement opportunities through a range of cyber academic programs ranging from full-time traditional courseware to non-traditional (evening and weekend courses) and on-line course instruments. These efforts are mutually beneficial, serving Army Reserve Soldiers in their military and civilian careers while providing a critical capability to the Army and nation.
>
> **What continued efforts does the Army Reserve have planned for the future?**
>
> Cyber P3 is a force multiplier that demonstrates the potential that collaborative partnerships offer to Army Reserve Soldiers. Cyber P3 will continue to partner with organizations that enhance Army Reserve cyber individual, leader and unit readiness, create civilian career opportunities, and provide continuous education opportunities at top-tier regional schools. Cyber P3 built programs around academic cyber networks, employment networks, community outreach, collective cyber training and education, research, and strategic communications [emphasis in original].

84. Scott Nelson, "US Army Reserve Cyber Private Public Partnership Initiative (P3i) Overview," Federal Information Systems Security Educators' Association (FISSEA) 28th Annual Conference presentation, March 24, 2015, available from *https://csrc.nist.gov/CSRC/media/Presentations/FISSEA-2015-Conference-Army-Reserve-Cyber-Privat/images-media/fissea-2015-nelson.pdf*, accessed October 29, 2017.

85. Isaac R. Porche III et al., *Cyber Power Potential of the Army's Reserve Component*, Santa Monica, CA: The RAND Corporation, 2017, p. xiii-xv, available from *http://www.rand.org/pubs/research_reports/RR1490.html*, accessed August 24, 2017.

86. Corey Dickstein, "Army Looking at Direct Commissions for Civilian Cybersecurity Experts," *Stars and Stripes,* February 8, 2017, available from *http://www.stripes.com/news/army-looking-at-direct-commissions-for-civilian-cybersecurity-experts-1.453101#.WNPVbqIpCUk*, accessed October 23, 2017.

87. "NGA Governor's Guide to Cybersecurity: National Guard," National Governors Association, n.d., archived page available from *https://web.archive.org/web/20170714010436/https://www.mediaw.nga.org/media/resources/cybersecurity/national-guard.html*, accessed November 12, 2017. See also "About," National Governors Association, n.d., available from *https://www.nga.org/cms/about*, for background about the NGA, which includes the following:

> Mission
>
> The National Governors Association (NGA) is the bipartisan organization of the nation's governors. Through NGA, governors share best practices, speak with a collective voice on national policy and develop innovative solutions that improve state government and support the principles of federalism.
>
> Who We Are
>
> Founded in 1908, the National Governors Association (NGA) is the collective voice of the nation's governors and one of Washington, DC's most respected public policy organizations. Its members are the governors of the 55 states, territories and commonwealths. NGA provides governors and their senior staff members with services that range from representing states on Capitol Hill and before the Administration on key federal issues to developing and implementing innovative solutions to public policy challenges through the NGA Center for Best Practices. NGA also provides management and technical assistance to both new and incumbent governors.

88. Ibid.

89. *2018 National Guard Bureau Posture Statement*, p. 18.

90. Jennifer Hotte and Ian Caple, "National Guard Computer Defense Teams Supported Inauguration," *National Guard News*, January 22, 2013, available from *http://www.nationalguard.mil/News/Article-View/Article/574226/national-guard-computer-defense-teams-supported-inauguration/*, accessed November 2, 2017. Details of the CND-T support for the inauguration include:

> The teams monitored network traffic that enters a mission specific stand-alone network established using the domestic operations Joint Incident Site Communication Capability (JISCC). Through doing this, they were able to identify and stop threats to the network.
>
> This joint operational mission integrated the Army and Air National Guard in a first of its kind effort. Cyber warriors from Rhode Island, North Carolina, Washington, Louisiana, Michigan, Oklahoma, New York, and Washington DC, came together to accomplish this real-world mission. These cyber warriors are able to defend their networks against threats.

91. Matt Leonard, "National Guard Expects Expanded Role in Cybersecurity," GCN website blog, January 6, 2017, available from *http://www.gcn.com/articles/2017/01/06/national-guard-cybersecurity.aspx*, accessed November 13, 2017. For additional details on the development and evolution of state-based cyber defense teams, see Murry McCullouch, "National Guard Forces in the Cyber Domain," Fort Leavenworth, KS: School of Advanced Military Studies, May 16, 2014, available from *http://www.dtic.mil/dtic/tr/fulltext/u2/1001702.pdf*, accessed November 2, 2017.

92. Laura Saporito, "The Cybersecurity Workforce: States' Needs and Opportunities," NGA Paper, Washington, DC: National Governors Association Center for Best Practices, October 27, 2014, p. 5, available from *https://classic.nga.org/files/live/sites/NGA/files/pdf/2014/1410TheCybersecurityWorkforce.pdf,* accessed November 19, 2018. The article explicitly ties National Guard forces to federal and state cyber incident response:

> In addition, the National Guard can play an important role in cyber incident response. Because of its unique role serving both governors and the President, the National Guard is well-positioned to support cyber incident response and recovery operations, to include assistance to law enforcement entities under state and federal law. States such as Delaware,

Maryland, Michigan, Rhode Island, Utah, and Wisconsin, as well as others, each have established units to support state responses to cyber attacks.

93. Brian Hare, "South Carolina National Guard Computer Network Defense Team Lends Expertise," *National Guard News*, June 4, 2015, available from *http://www.nationalguard.mil/News/Article-View/Article/590636/south-carolina-national-guard-computer-network-defense-team-lends-expertise/*, accessed November 2, 2017.

94. Derrol Fulghum, "Computer Network Defense Team Trains to Safeguard Florida," U.S. Army News, February 3, 2016, available from *https://www.army.mil/article/161805/computer_network_defense_team_trains_to_safeguard_florida*, accessed November 2, 2017.

95. "Cybersecurity," National Governors Association website page, available from *https://www.nga.org/policy-positions/cybersecurity/,* accessed November 19, 2018.

96. "National Guard Cyber Threat Working Group," *Chief National Guard Bureau (CNGB) Notice 3301*, June 7, 2016, p. 1, available from *https://web.archive.org/web/20161020104236/http://www.ngbpdc.ngb.army.mil/pubs/CNGBI/CNGBN_3301_20160607.pdf,* accessed November 2, 2017. The reason for creating the CTWG is summarized as:

> 4. Background. Cyber events frequently cross geographic and organizational boundaries. This necessitates a cross-functional team to evaluate events in order to effectively assess and communicate event details. The cross-functional team is formally defined as the CTWG. The CTWG established a process to create a unified strategic message from NGB staffs to the States, Territories and District of Columbia, to ensure the . . . [National Guard] responds appropriately to cyber threats.

97. CNGB Notice 3301, "National Guard Cyber Threat Working Group," p. 2. Excerpts from this CNGB address why and when the CTWG may be formed:

> d. Convene the CTWG. If the CCC [Cyber Coordination Cell] determines a cyber event exists, the CCC will convene the CTWG at the action officer level. Any CTWG member

may convene the group based on the initial assessment of a cyber event. When this occurs, the convening member will immediately share the information with the NGCC [National Guard Coordination Center]. The CTWG may expand its membership, as required, to include additional action officers or 06 level members based on areas of impact and event severity to ensure all stakeholders are advised of the situation.

f. Operational/Strategic Communication. The CCC and CTWG will identify events crossing multiple staffs, as well as events that require additional communications for purposes such as response, mitigation, or strategic messaging by NGB. For these events, the CTWG will identify and gather representation from all affected NGB staff elements, State, Territory and District of Columbia staffs, and when needed, mission partners. This group of stakeholders will develop recommended actions for NGB and identify a lead element to represent equities and ensure unified strategic messaging.

98. *The State of Florida 2016 Comprehensive Emergency Management Plan*, 2016 Draft Revision, Tallahassee, FL: Florida Division of Emergency Management, 2016 Terrorism Annex, p. 2-7. The only specific mention of National Guard cyber capabilities in the reference document is:

Florida National Guard Computer Emergency Response Team

The FLNG Emergency Response Team is a team of specialized National Guard personnel available for activation to any location in the state when authorized by an Executive Order of the Governor. The team provides support to the Incident Commander at the scene with highly specialized technical services that may be needed for the response to a known or suspected terrorist incident involving a cyber terrorism incident [emphasis in original].

99. Table 6 was developed by reviewing the named emergency response plans that were available to the general public on the respective states' emergency management websites on November 12-14, 2017. The reader may contact the author with any specific questions regarding the review of these plans. Arizona: see *Arizona State Emergency Response and Recovery Plan*, Phoenix, AZ: Arizona Department of Emergency and Military Affairs, September

1, 2016, available from *https://www.dema.az.gov/sites/default/files/publications/EM-PLN_State_Emergency_Response_and_Recovery_Plan-Basic_Plan_SERRP_2016FINAL_Oct7.pdf*; California: see *State of California Emergency Plan*, Mather, CA: California Governor's Office of Emergency Services, October 1, 2017, available from *http://www.caloes.ca.gov/PlanningPreparednessSite/Documents/California_State_Emergency_Plan_2017.pdf*; Colorado: see *Colorado Hazard and Incident Response and Recovery Plan*, Centennial, CO: Department of Public Safety, Colorado Division of Homeland Security and Emergency Management, November 2016, available from *https://www.colorado.gov/pacific/dhsem/atom/60606*; District of Columbia: see *District Response Plan*, Washington, DC: Homeland Security and Emergency Management Agency, September 2015, available from *https://www.hsema.dc.gov/sites/default/files/dc/sites/hsema/page_content/attachments/District%20Response%20Plan%202015.pdf*; Florida: see *State of Florida Comprehensive Emergency Management Plan*, Tallahassee, FL: Florida Division of Emergency Management, 2016; Georgia (2): see *Georgia Emergency Operations Plan*, Atlanta, GA: Emergency Management Agency and Homeland Security, State of Georgia, January 2013 (updated January 2015), available from *http://www.gema.ga.gov/Plan%20Library/GEOP%20-%20Base%20Plan%20(2015).pdf*, and *Georgia Emergency Operations Plan 2015: Department of Defense Annex, Defense Support*, Atlanta, GA: Emergency Management Agency and Homeland Security, State of Georgia, 2015; Maryland (2): see *State of Maryland Response Operations Plan*, Reisterstown, MD: Maryland Emergency Response Management Agency, March 2015, available from *http://www.mema.maryland.gov/Documents/SROP_V3_03_MAR-15.pdf*, and *State of Maryland Consequence Management Operations Plan*, Reisterstown, MD: Maryland Emergency Response Management Agency, September 2017, available from *https://mema.maryland.gov/Documents/Maryland_Consequence_Management_Operations_Plan%20_9.5.17.1_Public_Version.pdf*; Michigan: see *Michigan Emergency Management Plan*, Dimondale, MI: Emergency Management and Homeland Security Division, Michigan State Police, July 2016, available from *https://www.michigan.gov/documents/msp/MEMP_portfolio_for_web_383520_7.pdf*; Pennsylvania (2): see *Commonwealth of Pennsylvania Emergency Operations Plan*, Harrisburg, PA: Pennsylvania Emergency Management Agency, June 2017, available from *http://www.pema.pa.gov/Documents/CEOP%20JUNE%202017.pdf*, and *Pennsylvania 2013 Standard State All-Hazard Mitigation Plan*, Harrisburg, PA: Pennsylvania Emergency

Management Agency, 2013, available from *http://www.pema.pa.gov/responseandrecovery/Disaster-Assistance/Documents/General%20Mitigation%20Forms%20and%20Information/Pennsylvania%20State%20Hazard%20Mitigation%20Plan%20-%20Oct%2031%202013.pdf*; Texas: see *State of Texas Emergency Management Plan*, Chg. 2, Austin, TX: Texas Division of Emergency Management, February 17, 2015, available from *https://www.preparingtexas.org/Resources/documents/State%20and%20Fed%20Plans/2015_02_17_Basic_Plan_with_Appendices_za.pdf*; Virginia: see *Commonwealth of Virginia Emergency Operations Plan*, Richmond, VA: Virginia Department of Emergency Management, 2012 (updated March 2015), available from *http://www.vaemergency.gov/wp-content/uploads/drupal/2012COVEOPPlan2015March.pdf*; Washington: see *Washington State Comprehensive Emergency Management Plan: Basic Plan*, Camp Murray, WA: Emergency Management Division, Washington Military Department, June 2016, available from *http://www.mil.wa.gov/uploads/pdf/PLANS/final-wacemp-basic-plan-june2016-signed.pdf*.

100. "S.658—Cyber Warrior Act of 2013," 113th Congress (2013-2014), available from *https://www.congress.gov/bill/113th-congress/senate-bill/658*, accessed November 13, 2017.

101. "H.R.3712—Major General Tim Lowenberg National Guard Cyber Defenders Act," 115th Congress (2017-2018), available from *https://www.congress.gov/bill/115th-congress/house-bill/3712*, accessed November 15, 2017.

102. "H.R.60—Cyber Defense National Guard Act," 114th Congress (2015-2016), available from *https://www.congress.gov/bill/114th-congress/house-bill/60*, accessed November 15, 2017.

103. "NGA Governor's Guide to Cybersecurity: National Guard." The website include this list of tasks that National Guard cyber forces could support:

> The Guard can assist routine, steady-state cybersecurity activities to defend state and local computer systems by: Conducting risk assessments for state information systems; Designing secure network configurations for state agencies; Planning and leading cyber response simulations, exercises and drills; and, Training local government officials.

104. Saporito, "The Cybersecurity Workforce: States' Needs and Opportunities," p. 5.

105. William Matthews, "Cyber Uncertainty," *National Guard*, Vol. 68, No. 7, July 2014, p. 25, available from *http://nationalguard-magazine.com/article/Cyber_Uncertainty/1764536/218066/article.html*, accessed November 19, 2018.

106. Ibid.

107. Ibid.

108. Rene Marsh, "Ohio Taps National Guard to Defend Election System from Hackers," CNN online, November 1, 2016, available from *https://www.cnn.com/2016/11/01/politics/election-hacking-cyberattack/index.html*, accessed November 2, 2017.

109. "NGA Governor's Guide to Cybersecurity: National Guard."

110. Nelson, "Cyber Private Public Partnership Initiative (P3i) Overview," slide 7.

111. "Drexel Cybersecurity Institute and U.S. Army Reserve to Train Next Generation of 'Cyber Soldiers'," Drexel Now website, February 10, 2015, available from *https://www.drexel.edu/now/archive/2015/February/USAR-cybersecurity/*, accessed October 29, 2017.

112. "Georgia National Guard Collaborates with GTRI on Cyber Defense," Georgia Tech Research Institute, May 15, 2014, available from *https://www.gtri.gatech.edu/newsroom/georgia-national-guard-collaborates-gtri-cyber-defense*, accessed October 22, 2017.

113. Tarell J. Bilbo, "La. Guard's Cyber Defense Gets Tested," Louisiana National Guard, April 13, 2016, available from *https://geauxguard.la.gov/la-guards-cyber-defense-gets-tested/*, accessed November 19, 2018.

114. "Michigan Cyber Civilian Corps," Michigan state government website, available from *https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html,* accessed October

22, 2017. The qualifications for being a member of the Michigan Cyber Civilian Corps are:

> The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer to provide expert assistance to enhance the State's ability to rapidly resolve cyber incidents when activated under a Governor declared State of Emergency.
>
> Membership is open to information security professionals who are residents of the state of Michigan. Applicants should have at least 2 years of direct involvement with information security, preferably security operations, incident response and/or digital or network forensics. Applicants must also have a basic security certification (ANSI-certified/DOD 8570 compliant certifications such as Security+, C|EH, CISSP, or GIAC certifications are strongly preferred). Applicants will also be required to pass a series of tests to demonstrate basic knowledge of networking and security concepts, as well as basic IR and forensics skills. Because of the time commitment (up to 10 days/year for training and exercises), applicants must provide evidence of employer support. Successful applicants will also be subject to background screening and sign a confidential disclosure agreement.

115. "Information Technology Training Center (ITTC)," National Guard Professional Education Center website, available from *https://www.pec.ng.mil/ITTC*, accessed November 7, 2017.

116. Ohio Adjutant General's Department, "Ohio Takes Innovative Approach to Cybersecurity," News Release Log #17-10, February 27, 2017, available from *http://www.ong.ohio.gov/information/press_releases/2017/170227-Log10.pdf*, accessed November 14, 2017.

117. "Deal Announces New Georgia Cyber Innovation and Training Center," press release, Georgia Office of the Governor, Governor Nathan Deal, January 11, 2017, available from *https://gov.georgia.gov/press-releases/2017-01-11/deal-announces-new-georgia-cyber-innovation-and-training-center,* accessed December 18, 2018.

118. "Georgia Cyber Innovation and Training Center," Georgia state government website, January 11, 2017, pp. 3 and

6, available from *http://www.gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia%20Cyber%20Innovation%20and%20Training%20Center.pdf*, accessed October 22, 2017. This proposal clearly anticipates participation by Army Active and Reserve component forces, as indicated by these passages:

> **How will the Center be unique?**
>
> State-owned cyber ranges are extremely rare. Michigan, Virginia, Rhode Island, and Arizona have state-owned cyber ranges. Texas, California, and Minnesota are looking into the potential of having cyber ranges. The Georgia Cyber Innovation and Training Center will be one of a few state-owned cyber ranges and will offer the ability to leverage state resources like research, infrastructure, and training with private industry to advance cybersecurity efforts. The facility will be unique by offering sensitive compartmented information facility (SCIF) space for sensitive information, training and education, and incubator space for Georgia's start-ups. (p. 3)
>
> **Why Augusta?**
>
> Augusta is home to the United States Army's Cyber Command (Fort Gordon), the US Army Cyber Center of Excellence and the National Security Agency (NSA) (representing all branches), making Augusta the destination for cyber professionals in any stage of their career. The US Department of Defense plans to invest $2.1 billion on the construction of the new Cyber Command Headquarters. Centrally located to enhance partnerships across the University System of Georgia (USG) and TCSG, Augusta offers the opportunity to foster collaborative efforts given the scope of professionals required which include computer scientists, computer engineers, electrical engineers, journalists, linguists, business, and health, etc. Augusta University (AU) is a Center of Academic Excellence in Cyber Defense Education as recognized by NSA and the Department of Homeland Security (DHS) and most recently, AU entered into an articulation agreement affording NSA language professionals the opportunity to attain a bachelor's degree while here in Georgia. Additionally, Georgia is already home to one of the ten cyber protection teams with the Army National Guard. (p. 6)

119. "Florida Cyber Range," Florida Cyber Range website about page, available from *http://www.floridacyberrange.org/about/florida-cyber-range/*, accessed November 13, 2017.

120. "Baltimore Cyber Range and Cyberbit Open New Cybersecurity Training and Simulation Center," Cyberbit, August 3, 2017, available from *https://www.cyberbit.com/company/news/baltimore-cyber-range-cyberbit-open-new-cybersecurity-training-simulation-center/*, accessed November 14, 2017. Details of the cyber range include:

> The Baltimore Cyber Range is located in the SPARK building at the Power Plant Live square in downtown Baltimore. The facility is part of the new Intrusion Countermeasures Education and Training (ICE-T) Consortium, formed by Electronic Technology Associates, LLC of Baltimore to provide Maryland residents the skills and training required to obtain an initial IT position and or significantly enhance the skill set of the existing Maryland IT / Cyber workforce. The consortium includes nine private and three public companies. Centrally located in Baltimore—close to the federal government's cyber-related activities in Washington, DC, at Fort Meade, Md., and at Aberdeen Proving Ground, Md.—the Baltimore Cyber Range offers cybersecurity professionals the convenience of training with the most current cyber warfare strategies, close to home. To learn more about the facility, please visit: *http://baltimorecyberrange.com/*.

121. David Behen, "Michigan Cyber Initiatives," Lansing, MI: Michigan Department of Technology, Management, and Budget (DTMB), May 16, 2016, available from *http://www.fema.gov/media-library-data/1464352944315-cf04893ed1815b71bb85e1e1c4ff60a2/MI_CyberInnoPract_Clean_20160517-2.pdf*, accessed November 8, 2017.

122. Brett Wilson Tubbs, "Regent University Launches State-of-the-Art Cyber Range Training Center with Cyberbit," Virginia Beach, VA: Regent University, October 3, 2017, available from *https://www.regentalumni.org/s/832/social.aspx?sid=832&gid=1&pgid=252&cid=6723&ecid=6723&ciid=18903&crid=0*, accessed November 13, 2017.

123. "Governor Launches Cutting-Edge Cybersecurity Training Program," Michigan Governor Rick Synder official website, November 9, 2012, available from *https://www.michigan.gov/som/0,4669,7-192-29701-289758--,00.html,* accessed November 15, 2017.

124. Ibid. The article lists the initial supporters of the cyber range as:

> Michigan Cyber Range partners include Merit Network, U.S. Department of Homeland Security, U.S. Department of Energy, National Institute of Standards and Technology, DTE Energy, Consumers Energy, Plante and Moran PLLC, Juniper Networks, Eastern Michigan University, Michigan State Police, Michigan Department of Military and Veterans Affairs, Michigan Economic Development Corp. and the Michigan Department of Technology, Management and Budget.
>
> Merit Network, a nonprofit corporation governed by Michigan's public universities, owns and operates America's longest running regional research and education network and supports the high-performance networking needs of Michigan's universities, colleges, K-12 schools, libraries, state government, health care and other nonprofit organizations.

125. "The Michigan Cyber Range," Merit website, available from *https://www.merit.edu/cyberrange/*, accessed November 15, 2017. See also the webpage Alphaville & Griffinville, available from *http://www.merit.edu/cyberrange/alphaville/*.

126. Theresa Ghiloni, "Cyber Range Training Center Added to 110th Airlift Wing at Battle Creek National Guard Base," MLive Media Group, March 25, 2014, available from *https://www.mlive.com/news/kalamazoo/index.ssf/2014/03/cyber_range_training_center_ad.html*, accessed November 15, 2017.

127. "Cyber Shield '14," Stand-To! The Official Focus of the U.S. Army, June 18, 2014, available from *https://www.army.mil/standto/archive_2014-06-18*, accessed November 7, 2017.

128. Kelvin M. Green and Kyle Key, "Cyber Warriors Flex Digital Muscle at 2014 Cyber Shield Exercise," *National Guard News*, May 20, 2014, available from *http://www.nationalguard.mil/*

News/Article-View/Article/575680/cyber-warriors-flex-digital-muscle-at-2014-cyber-shield-exercise/, accessed November 7, 2017. The article noted that cyber defense teams may be slightly different in each state:

> The Computer Network Defense Teams consist of eight highly trained and proficient network defenders who have varying skill sets. Each state and territory has similarities but is also individually unique due to their state guidelines and restrictions. The state of California has a unique model in which they are directly engaged with state agencies, conduct vulnerability scans, and provide recommendations on how they can improve their overall security. Ken Foster, a CNDT analyst with the California Army National Guard, said many interagency partners are largely unaware of their vulnerability.

129. Jessica Cates, "Cyber Shield Concluded in Admiration," Atterbury-Muscatatuck Public Affairs, March 27, 2015, available from *https://www.atterburymuscatatuck.in.ng.mil/NewsMedia/LatestNews/TabId/582/artmid/4756/articleid/25/Cyber-Shield-Concluded-in-Admiration.aspx*, accessed November 7, 2017. For further details on the Cyber City tool, see also Jessica Cates, "Cyber City Trains Warriors," Atterbury-Muscatatuck Public Affairs, March 19, 2015, available from *https://www.atterburymuscatatuck.in.ng.mil/NewsMedia/LatestNews/TabId/582/ArtMID/4756/ArticleID/24/Cyber-City-Trains-Warriors.aspx*, accessed November 7, 2017.

130. Brad Staggs, "Indiana National Guard participates in Cyber Shield 2016," Atterbury-Muscatatuck Public Affairs, May 10, 2016, available from *https://www.atterburymuscatatuck.in.ng.mil/NewsMedia/LatestNews/TabId/582/ArtMID/4756/ArticleID/125/Indiana-National-Guard-participates-in-Cyber-Shield-2016.aspx*, accessed November 8, 2017.

131. Ray McCulloch, "Exercise Cyber Shield 2017 Gets Underway," U.S. Army News, April 26, 2017, available from *https://www.army.mil/article/186702/exercise_cyber_shield_2017_gets_underway*, accessed November 6, 2017. The article contains more details on the purpose of the exercise:

> Cyber Shield is designed to train National Guard members from across the United States on cyber protection, network defense, forensic analysis, tactics, techniques and procedures defense against cyber attacks, hackers, or other malign actors. The exercise is a culminating training event that supports the National Guard's defensive cyberspace operations missions to defend Department of Defense assets by conducting cyber command readiness inspections and critical infrastructure vulnerability assessments.

132. Stephanie Ramirez, "Guard and Reserve Soldiers Team Up for Cyber Defense," U.S. Army Reserve News, May 5, 2017, available from *https://www.usar.army.mil/News/News-Display/Article/1174708/guard-and-reserve-soldiers-team-up-for-cyber-defense/*, accessed November 19, 2018.

133. Kyleen Kelleher, "Cyber Training Unites New England," Massachusetts National Guard official website, May 7, 2015, available from *https://www.massnationalguard.org/cyber-training-unites-new-england.html*, accessed November 19, 2018.

134. "Mass. Guard Hosts Cyber Defense Exercise 'Cyber Yankee'," Massachusetts National Guard—The Nation's First facebook page, June 23 2017, available from *https://www.facebook.com/media/set/?set=a.10154813116982865.1073742336.195131757864&type=3*, accessed November 14, 2017.

135. Erick Yates, "Pennsylvania Guard Members Participating in Advance Cyber Challenge," National Guard News, June 20, 2017, available from *http://www.nationalguard.mil/News/Article-View/Article/1219511/advanced-cyber-challenge-underway-at-carnegie-mellon-university/*, accessed November 4, 2017. Details of the Cyber X-Games include:

> Attendees at Cyber X-Games 2017 will be challenged in areas of cyber detection, response and recovery. A competitive environment will be created with live red/blue teaming, evaluation by facilitators during strategy briefings and cyber mission exercise scenarios. Quizzes and status updates for each team are also part of the five-day challenge, according to coordinators of the event.

136. "State Partnership Program," National Guard fact sheet, August 2014, available from *https://www.nationalguard.mil/*

Leadership/Joint-Staff/J-5/International-Affairs-Division/State-Partnership-Program/, accessed December 18, 2018.

137. *2018 National Guard Bureau Posture Statement*, pp. 20-21.

138. *The State Partnership Program FY 2015 Annual Report to Congress*, Washington, DC: Department of Defense, 2016, pp. 13-62, available from *https://securityassistance.org/content/state-partnership-program-annual-report-congress,* accessed December 18, 2018. Several of the examples of cyber-related SPP events in table 8 were derived from the report's annexes B through G.

139. Shaun Cavanaugh, "Baltic Ghost: Regional Cyber Defense Cooperation between the Baltic States, EUCOM and the SPP," US European Command Blog, June 11, 2013, available from *http://www.eucom.mil/media-library/blogpost/25209/baltic-ghost-regional-cyber-defense-cooperation-between-the-baltic-states-eucom-and-the-spp*, accessed November 7, 2017. The purpose of Baltic Ghost workshops include:

> Issues being worked on at the [Baltic Ghost] workshops include: defining what the cyber critical infrastructure within the region is, what authorities are available when it comes to defining civil and military cyber organizations supporting one another during times of a cyber crisis, building public private partnerships, and defining what the most likely threat scenarios are within the region.

140. "Cyber Security Training Baltic Ghost Practises Ensuring Electricity Supply in the Case of Cyber-Attacks," Elerging Blog, September 21, 2016, available from *https://www.elering.ee/en/cyber-security-training-baltic-ghost-practises-ensuring-electricity-supply-case-cyber-attacks*, accessed November 7, 2017. Per its website, Elerging is an independent electricity and gas operator in Estonia. This blog includes the two main objectives of the Baltic Ghost exercise:

> The main focus of the Baltic Ghost training is testing the exchange of information between institutions in the event of a cyber incident, as well as practising the procedures for involving external support (e.g. the Cyber Unit of the Estonian Defence League).

> The secondary objective is to test cooperation between the three Baltic States in the event of an escalating cyber incident, the solution of which requires internationally coordinated joint action.

141. "USEUCOM Hosts Cyber Exercise with Baltic Allies," US European Command Press Release, July 5, 2017, available from *http://www.eucom.mil/media-library/pressrelease/35877/useucom-hosts-cyber-exercise-with-baltic-allies*, accessed November 7, 2017.

142. "Estonian, Maryland National Guard cyber exercise begins at Ämari," August 8, 2017, ERR News, available from *https://news.err.ee/611741/estonian-maryland-national-guard-cyber-exercise-begins-at-amari*, accessed October 22, 2017.

143. Bill Pierce, "Ohio National Guard works with Serbian Partners during Cyber Tesla 2017 exercise," U.S. Army News, October 13, 2017, available from *http://www.army.mil/article/195296/ohio_national_guard_works_with_serbian_partners_during_cyber_tesla_2017_exercise*, accessed October 22, 2017.

144. "Welcome the First International Military Students to PEC!" National Guard Professional Education Center facebook post, July 16, 2017, available from *https://www.facebook.com/media/set/?set=a.991450077572737.1073741858.379287698788981&type=3*, accessed November 7, 2017.

145. Report GAO-16-574, p. 21. One of the key findings of the report was:

> The National Guard has cyber capabilities that could be used—if requested and approved—to support civil authorities in a cyber incident. During an emergency, it is necessary for decision makers to have visibility into the full capabilities that National Guard units possess to support civil authorities. Unless DOD develops or specifies a database to provide full and quick identification of all National Guard units' cyber capabilities, DOD may not have timely visibility and access for needed capabilities when requested by civil authorities during a cyber incident.

146. *Response Federal Interagency Operational Plan,* 2d Ed., p. E-17.

147. *National Cyber Incident Response Plan*, p. 9.

148. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3500.01H, *Joint Training Policy for the Armed Forces of the United States*, Washington, DC: Joint Chiefs of Staff, April 25, 2014, p. B-6. CJCSI 3500.01H defines Tier 1 training as:

> Tier 1: National Level and CCMD training—Joint training designed to prepare national level organizations and CCDR and staffs at the strategic and operational levels of war to integrate interagency, non-governmental, and multinational partners in highly complex environments. The desired end state in integrating a diverse audience in a joint training environment is to identify core competencies, procedural disconnects, and common ground to achieve U.S. unity of effort.

149. Eric K. Fanning, Memorandum for Deputy Chief of Staff, G-3/5/7, Subject: Delegation of Authority for Department of Defense Executive Agency Responsibility for Cyber Training Ranges, Washington, DC: Secretary of the Army, August 25, 2016.

150. "NGA Governor's Guide to Cybersecurity: National Guard." This guide offers the following advice for governors with regard to the development of cyber response plans:

> Incorporate procedures for using Guard cyber capabilities into cyber response plans. Assemble a team including the TAG, CIO, CISO, Homeland Security Advisory and chief cyber advisor (if not already listed) to integrate National Guard cyber units into statewide cyber emergency response procedures. The TAG should coordinate with the Chief of the National Guard Bureau to clarify and document procedures for requesting and accessing Title 32 funding for response activities.

U.S. ARMY WAR COLLEGE

Major General John S. Kem
Commandant

*****

STRATEGIC STUDIES INSTITUTE
AND
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Author
Jeffrey L. Caton

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
https://www.armywarcollege.edu/

ISBN 1-58487-799-5
9 781584 877998
90000 >

This Publication

SSI Website

USAWC Website