AIR WAR COLLEGE

AIR UNIVERSITY

TOTAL ARMY CYBER MISSION FORCE:

RESERVE COMPONENT INTEGRATION

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

by

Joseph A. Papenfus, LTC, USA

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Panayotis A. Yannakogeorgos, PhD

16 February 2016

DISTRIBUTION A. Approved for public release: distribution unlimited.

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Biography

LTC Joseph Papenfus is a U.S. Army Signal Corps officer with an Information Systems Management (FA-53A) specialty. Having served in both Active and Reserve Component (USAR and ARNG) status, he currently serves the USAR in a Title-10 status.

LTC Papenfus has held Company to Battalion command level assignments. He has also lead in Signal and Computer Network Operations (CNO) assignments at all staff levels from Company to Army Service Component Command (ASCC). His most recent deployment includes serving as the Director COMMS-I Afghanistan and Deputy Brigade Commander for a Strategic Signal Brigade, Bagram Air Force Base, Afghanistan.

LTC Papenfus earned a Bachelor's of Science Degree from the University of Wisconsin - Milwaukee and a Master's Degree from Webster University in Business Administration (MBA). In additional to branch specific training, he has graduated from the FA-40A Course, FA-53A Course, Basic CNO Planners Course (BCNOPC), and the Reserve Component National Security Course (RCNSC). He earned JMPE Phase 1 from the Army Intermediate Level Education (ILE) and the Canadian Forces College Joint Command and Staff Program (JCSP). He is working towards a Master's of Strategic Studies Degree from the Air War College.

Air University–Maxwell AFB, AL

Abstract

As cyberspace continues to play an important role in projection of military power, in an environment where the mission of tomorrow is ill defined and budgets are becoming constrained, there is an increasing need for a Total Force (AC/RC) concept. The existing and emerging requirements for Army Cyber Mission Forces (CMF) are currently greater than the Army's active component has personnel available or trained to support USCYBERCOM and ARCYBER requirements. The Army's RC is uniquely postured to fill current, midterm and longer-term cyber gap requirements, but it requires planning and investment now in training, development, and integrations of the RC CMF.

Although moving cautiously, some of the distinct advantages many Reserve Component (USAR and ARNG) Soldiers have are their ties to the communities, full-time employment in the civilian information technology, and their dispersion across the country. Unlike centrally consolidated Title-10 (AC and USAR) organizations, with Homeland Defense and Defense Support to Civil Authorities requirements with limited authorities under the *Posse Comitatus Act*, the ARNG units can further assist local and state governmental agencies nationwide to defend critical infrastructure networks.

These aspects further make the RC uniquely postured to fill current, midterm and longer-term cyber requirements, but it requires planning and investment now in training, development, and integrations of the RC CMF. This analysis accomplishes this through inspection of policy, current requirements, constructs, mission areas and initiatives for RC forces to determine the benefits or drawbacks to successful generation of a Total Force (AC/RC) CMF.

Contents

Abstract iii
Introduction 1
U.S. Cyber Policy 1
U.S. Cyber Mission Force (CMF) 3
CMF Requirements 3
CMF Cyber Operations (CO) Mission Areas 4
CMF Authorities (U.S. Code / Titles of Authority 10-50) 5
U.S. Army Cyber Organization and Mission Areas 5
Active Component (AC) 5
Reserve Component (RC) 6
Army CMF Training and Development 9
AC Cyber Individual and Collective Training Model 9
RC Cyber Individual and Collective Training Model 10
i. Institutional CMF Schooling 10
ii. Civilian Acquired Skills and Certification 11
iii. Partnerships (Civilian Industry and Other Governmental) 11
iv. Collective Training (Day to Day, Exercise, and Emergency). 12
Integration of RC Cyber Mission Forces 13
Types of RC Forces (State Active Duty, Tile-10, Title-32). 14
RC CMF Location Requirements 16
RC Sources and Resourcing Authorities (12301-12304) 16
End Notes 20
Appendix A: Glossary 23
Bibliography 24

Digital Collections

Introduction

The year was 2008 and the U.S. Department of Defense (DoD) was under attack. The attack originated not from within the traditional domains of land, seas, air or space, but through the cyberspace domain. This cyber-attack compromised the U.S. classified military networks with a worm that infected and propagated a malicious code throughout the network.[1] At the same time, unrelated to the attack, U.S. Army Active Component (AC) organizations, augmented by Reserve Component (RC) Soldiers,[i] were conducting Computer Network Operations (CNO) support to a major military exercise. Shortly after the attack was recognized, the CNO exercise halted and all efforts refocused on addressing the threat. These same RC Soldiers, originally on short-term military orders, stayed and eventually mobilized for longer periods to provide the surge capacity needed to mitigate and counter the attack. RC support to the operation, later known as Buckshot Yankee,[ii] is an example of a "pick-up game" that would not have occurred if a few leaders did not have foresight to incorporate the AC and RC Cyber Mission Force(s) (CMF). This real life 2008 cyber-attack is a stark vignette depicting the need for a Total Force (AC/RC) CMF concept. The Army's RC is uniquely postured to fill current, midterm and longer-term cyber gap requirements, but it requires planning and investment now in training, development, and integrations of the RC CMF. This analysis will inspect policy, current requirements, constructs, mission areas and initiatives for training, development and integration of RC forces to determine the benefits or drawbacks to successful generation of a Total Force (AC/RC) CMF.

U.S. Cyber Policy

[i] For the purposes of this paper, the term Reserve Component (RC) includes both the U.S. Army Reserve (USAR) and the U.S. Army National Guard (ARNG) immaterial of duty status, unless otherwise specified.
[ii] Operation "Buckshot Yankee" was the Pentagon's, previously classified, operation to counter the most significant breach of U.S. military computer networks up until 2008. (Lynn 2010, 97)

Between 2001 and 2013, the nation's number one threat was terrorism and it received the highest priority for allocation of intelligence resources. In 2013, the Director National Intelligence (DNI) identified the potential for cyber-attacks as the primary U.S. strategic threat.[2] The rationale for this shift was routed in U.S. heavy reliance, "on the Internet and the systems and data of cyberspace for a wide range of critical services … [which leaves] us vulnerable in the face of a real and dangerous cyber threat."[3] These growing cyber-security threats, identified in earlier versions of the *National Security Strategy* (NSS), were reinforced in the 2015 NSS calling for a greater emphasis on building partnership capacity to address cyber threats.[4]

Within the military instrument of national power, the nested *National Military Strategy* (NMS) categorizes one of the key defense capabilities as a CMF able to, "defend us against both high technology threats and terrorist dangers."[5] The existing and emerging requirements for CMFs are greater than the Army's AC currently has personnel available or trained to support U.S. Cyber Command (USCYBERCOM) and U.S. Army Cyber Command (ARCYBER) requirements. In order for the U.S. Army to meet its obligations to the joint force mission it is only prudent to sustain the, "full-spectrum military that includes strong Reserve and National Guard forces … [which] provide the force depth needed to achieve victory while simultaneously deterring other threats."[6]

Based upon the 2015 *Army Posture Statement*, of the 980,000 Total Force Soldiers required for the Army to execute all current and future missions, over 54 percent of Army's overall capacity is in the RC.[7] With a recognized resource-constrained environment, even if there is cyber funding, it is important to be good resource stewards through, "streamlining functions, eliminating redundancies, and producing more integrated and effective organizations."[8]

Therefore, key policy documents provide indication that in an environment where the mission of tomorrow is ill defined and budgets become constrained there is an increasing need for a Total Force (AC/RC) concept. With 54 percent of the capacity, the Army's RC is uniquely postured to fill gap requirements directly correlating toward the Army meeting strategic goals and objectives laid out in the 2015 *Department of Defense Cyber Strategy*.[9]

U.S. Cyber Mission Force (CMF)

CMF Requirements

Investment in or definition of CMF requirements, by DoD and individual service components, have been underway for years. These efforts considerably predate the 2010 creation of USCYBERCOM, the 2005 *Joint Concept of Operations for the Global Information Grid NetOps* (NetOps CONOPS), or the Joint Task Force – Computer Network Defense (JTF-CND) in the late nineteen nineties. However, in 2012 the DoD began major investment to build a common CMF to meet growing cyber-threats. The 2014 *Quadrennial Defense Review* provided further refinement on CMF organization supported in 2015 by the *Department of Defense Cyber Strategy* that laid out the military strategy to meet key cyber-threats.

The CMF strategy focuses on building, "cyber capabilities and organizations for the DoD's three cyber missions: to defend DoD networks, systems, and information; defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and to support operational and contingency plans."[10] To meet these requirements the strategy lays out five strategic goals and corresponding implementation objectives.[11] Of particular relevance is strategic goal one, focused on the requirement to build and retain a CMF capable of conducting CO, and implementation objectives to: build technical capabilities for CO; validate and

continually refine an adaptive command and control (C2) mechanism for CO; establish an enterprise-wide cyber modeling and simulation capability; and assess CMF capacity.[12]

Once operational, this force will be, "nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components."[13] The CMF will be organized into 133 teams: 13 National Mission Teams (NMTs), 08 National Support Teams (NSTs), 27 Combat Mission Teams (CMTs), 17 Combat Support Teams (CSTs), 18 National Cyber Protection Teams (CPTs), 24 Service CPTs, and 26 Combatant Command or DoD Information Network (DODIN) CPTs.[14] National mission forces will operate under the control of USCYBERCOM. Many of these 133 teams will also be integrated within Unified Combatant Command (UCC) planning and operations.[15] Although there is a need for further study into each service component's best practices or economies of scale, due to scope, this analysis singularly focuses on the 41 ARCYBER teams generating in support of Army and joint CMF requirements.[16]

CMF Cyber Operations (CO) Mission Areas

The 2013 Joint Publication 3-12(R), *Cyberspace Operations*, defined successful mission execution of military CO in and through cyberspace as, "integrated and synchronized employment of offensive, defensive, and DODIN operations, underpinned by … operational preparation of the environment."[17]

These critical missions are, based on intent, categorized in joint doctrine as DoD Information Network (DODIN), Defensive Cyberspace Operations (DCO) and Offensive Cyberspace Operations (OCO). In addition to these, the Army's 2013 *Army Cyberspace Operations Capabilities Based Assessment* (Cyber CBA) likewise validated the need for Cyber Support (CyberSpt) and Cyber Situational Awareness (CySA).[18]

Digital Collections
Maxwell AFB, AL

DODIN operations are steps to, "design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks."[19] DCO are active and passive actions taken in defense of military and friendly cyberspace.[20] This includes internal defensive measures and necessary response actions (DCO-RA) taken externally to the DODIN to defend the network.[21] Subsequently, OCO operations are a very specialized portion of the CMF; these cyber warriors have the mission to, "project power by the application of force in and through cyberspace."[22] Coupled with these, CyberSpt operations are the supporting activities executed to support OCO, DCO, and DODIN operations, while CySA operations are, "the immediate knowledge of friendly, adversary and other relevant information regarding activities in and through cyberspace."[23]

CMF Authorities (U.S. Code / Titles of Authority 10-50)

The CMFs execute their missions in support of joint forces under the authorities provided to the Army Forces through U.S. Constitutional and Federal Law. The Key statutory authorities applying to the DoD, "include Title 10, United States Code (USC), Armed Forces; Title 50, USC, *War and National Defense;* and Title 32, USC, *National Guard*."[24] Discussed later are aspects of these authorities that provide unique advantages or disadvantages to the AC and RC forces executing CO.

U.S. Army Cyber Organization and Mission Areas

Active Component (AC)

DoD organizes these responsibilities, authorities and capabilities under U.S. Strategic Command (USSTRATCOM). USSTRATCOM, "is responsible for CO to secure, operate, and defend the DODIN, and to defend US critical cyberspace assets, systems, and functions as directed by the President or SecDef, against any intrusion or attack, and does so through a sub

unified command, USCYBERCOM."[25] Each service generates and organizes forces differently to meet service and joint CMF requirements. In 2010, the U.S. Army organized the AC cyberspace workforce primarily under the C2 framework of ARCYBER / Second Army. Unlike USCYBERCOM, ARCYBER has mission responsibility for both cyber and information operations. Assigned or attached forces execute these missions in support of Army or joint missions. At this point, of the Army's 41 CMF teams, 20 teams will be CPTs and the remaining 21 teams will be NMT, NST, CMT, and CSTs in support of national missions.

Prior to the creation of the Army's cyber branch, Soldiers under "Operations Support", within Signal (SC), Military Intelligence (MI), Information Operations (IO), and the Electronic Warfare (EW) career fields executed CO. In September 2014, the Army approved the 17 series career field to provide centralized management and professional development.[26] At present, the AC Army has moved forward assessing new Soldier while providing a Voluntary Transfer Incentive Program (VTIP) for qualified Soldiers wishing to transfer to the new cyber branch.

Reserve Component (RC)

Unlike the Army's AC that has moved forward in implementation of the cyber branch and aligning CMF under ARCYBER, the USAR (Title-10) and ARNG (Title-32) are slow but making progress on roles and definition of what comprises the reserve CMF. Although moving cautiously, some of the distinct advantages many of these RC Soldiers have are their ties to the communities, full-time employment in the civilian information technology (IT), and their dispersion across the country. At present the proposed 21 Army RC CPTs – 10 USAR and 11 ARNG – are not identified within the Army's 41 or part of the DoD's 133 teams identified within the 2015 *Department of Defense Cyber Strategy*.

i. Army Reserve Component Forces (USAR)

Digital Collections
Air University–Maxwell AFB, AL

Within the Army Reserve (Title-10), there are a number of organizations[iii] considered, to differing degrees, part of the RC CMF. Two key organizations, the Army Reserve Cyber Operations Group (ARCOG) and Military Intelligence Readiness Command (MIRC), have been involved in ARCYBER and USCYBERCOM's development of the CMF offensive and defensive requirements from both a full and part time capabilities standpoint. These USAR units, based upon their individual unit stationing orders, are located throughout the U.S. Northern Command (USNORTHCOM), Pacific Command (USPACOM) and European Command (USEUCOM) Area of Responsibility (AOR).

The ARCOG serves as one of the USAR's main capabilities specializing in DCO and DODIN operations while the MIRC specializes in OCO. The ARGOC formed from two Data Processing Units (DPU) merged years ago as part of the Chief Army Reserve's Joint Reserve Component Virtual Information Operations (JRVIO) concept. Although it has evolved over time, eventually being renamed the Army Reserve Information Operations Command (ARIOC) and more recently known as the ARCOG, one of its primary missions has always been to, "incorporate full use of the broad array of sophisticated information skills resident in the reserve component."[27] As part of this mission set, the ARCOG has continuously supported the Army's Computer Emergency Response Team (ACERT) requirements, within the South West Asia Cyber Center (SWACC), since 2001. In 2011, this mission transitioned to the USAR and the ARCOG to train, develop, and deploy the ACERT capability of the SWACC. In January 2014, as part of the USAR plan to build ten CPTs between now and fiscal year 2021, the ARCOG developed a concept plan to continue evolving to meet requirements and support operational cyber roles.

[iii] Within the Army Reserve (Title-10) there is currently one Army Reserve Cyber Operations Group (ARCOG), one Defense Information Support Agency Army Reserve Element (DISA ARE), two Theater Signal Commands (335th and 311th SC(T)), one Military Intelligence Readiness Command (MIRC), and two Theater Information Operations Groups (151 and 152 TIOG) that support or are considered part of the RC CMF.

This restructuring request will provide an overall capacity of ten USAR CPTs with, "a minimum of two CPTs for operational employment on a rotational basis and additional teams for expanded capacity."[28] Since these are Title-10 forces, the best use of these teams would be as service retained forces capable of filling federal contingency and programed UCC requirements.

ii. Army National Guard Forces (ARNG)

Unlike centrally consolidated Title-10 organizations, with a *Stafford Act* requirement and limited authorities to respond to domestic threats under the *Posse Comitatus Act*,[iv] ARNG units can assist local and state governmental agencies nationwide to defend critical infrastructure networks.[29] Within the ARNG (Title-32), cyber capabilities primarily fall under the Virginia Information Operations Support Command (VA IOSC) and its subordinate the Virginia Data Processing Unit (VA DPU); 54 state Computer Network Defense Teams (CNDT); Signal Brigades; and 02 TIOGs. These ARNG units, dispersed throughout the USNORTHCOM and USPACOM AOR, are in direct support of the 50 state Governors during a non-federalized status. For example, the ARNG CNDT provides vulnerability assessments and on a daily basis defends the guard's cyber backbone network (GUARDNET) connecting 3,000 armories across 11 different time zones.[30]

Similar to the USAR ARCOG, the VA DPU has evolved to allow part-time Soldiers the ability to conduct CO in areas like web risk and vulnerability assessments in support of the state, federal, and ARCYBER requirements.[31] In 2014, the ARNG signed a memorandum of understanding aligning an ARNG CPT in an active duty Title-10 status to ARCYBER.[32] The activation of the 1636th CPT represented a first for the Army National Guard. This was followed, in December 2015, by the ARNG releasing its plan for 10 ARNG CPTs.[33] [34] These

[iv] The *Posse Comitatus Act* ,"prohibits federal forces from direct participation in domestic law enforcement but those restrictions don't apply to the National Guard. (Luke 2014)

Army CPTs, along with Air Guard Cyber operations squadrons, spread through 23 states by the end of fiscal 2019 will afford the National Guard further capacity support to the 10 Federal Emergency Management Agency (FEMA) regions.[35] Therefore, integration within state and local agencies, not restricted by the *Posse Comitatus Act*, and having ties to Department of Homeland Security (DHS) places the ARNG (Title-32) CPTs in the best position to support USNORTHCOM's mission for Defense Support of Civil Authorities (DSCA).

Army CMF Training and Development

The individual training model for years was asymmetric within the differing Army "cyber warrior" career fields and CMF organizations. This lack of symmetry is why, in January 2014, HQDA EXORD 057-14 re-designated the Army's Signal Center of Excellence (SIGCoE) as the Cyber Center of Excellence (CyberCoE) and in 2015 the *U.S. Army Cyber Center of Excellence Strategic Plan* identified, "performance in the cyberspace domain requires a fundamental shift in Army strategy, doctrine, force development and operational techniques."[36] This transition will ensure the Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities (DOTMLPF) is synchronized for Army Cyber, SC and EW joint force capabilities, while further leveraging the U.S. Army Intelligence Center of Excellence (ICoE) to achieve cyberspace dominance.[37] [38]

AC Cyber Individual and Collective Training Model

Coupled with the individual training provided by the CyberCoE, in order to create a fully qualified and mission ready CPT, the Army's Cyber Protection Brigade implemented a twenty-week training plan.[v] It is comprised of cyber core preparation, industry certifications, individual

[v] Army's Cyber Protection Brigade twenty-week training plan is implemented through internal training program focuses on professional development, classroom instruction, virtualized, and online training to develop operational capability in support of cyber exercise, operational support, and real world operations. (U.S. Army Cyber Protection Brigade 2015)

cyber courses (ICC), methodology, and the Joint Network Attack Course (JNAC) leading toward a Joint Qualification Review (JQR) and designation as a fully mission capable cyber operator. [39] Further incentivizing the CMF, the Army has also recently expanded, "cyber educational programs, including training with industry, fellowships, civilian graduate education, and utilization of inter-service education programs including the Air Force Institute of Technology and the Naval Postgraduate School."[40]

RC Cyber Individual and Collective Training Model

i. Institutional CMF Schooling

In addition to tapping into AC schooling and training, currently both USAR and ARNG have schools providing portions of the CMF developmental training. The largest location providing a breath of IT and cyber training is the ARNG's Cyber Operations Training Center (COTC) located at the Professional Education Center (PEC) in Little Rock, Arkansas. The COTC gears its mission toward development and education through many approved TRADOC and USCYBERCOM courses that provide cyber skills to the joint force.[41] As part of force development and operational techniques, the PEC has done an analysis of the current AC training model and developed, in coordination with the CyberCoE, a course designed to achieve the USCYBERCOM Individual Training Equivalency Board (ITEB) standards. Once the COTC training – pilot projected January 2016 – is certified it will be a satellite campus for the CyberCoE to train RC CMFs.[42]

The USAR also conducts some courses at the Cyber Security Training Center (CSTC) – formerly a part of the Army Reserve Readiness Training Center – located at Fort McCoy, Wisconsin. Unlike the PEC, the CSTC has not developed a full training pathway to achieve

ITEB for RC CMF and currently focuses on information assurance (IA), computer network defense (CND), and certification training for DoD.[43]

Overall, the methodology of the COTC and CSTC training centers provide the opportunity for RC CMF to gain the required training through RC friendly courses. Their strategies take into account the complexity of gaining military training while being cognizant of the impact, to civilian employers, created when employees attend long AC CMF training courses.

ii. Civilian Acquired Skills and Certification

Equally important to formal training is the unique experience gained by RC Soldiers employed in organizations directly or indirectly involved in IT and CO. For instance the ARCOG has RC Soldiers employed as civilians within governmental, contracting, corporate (IT or security), academia, and financial organizations. In some cases, this duality can also be a draw back. When the civilian acquired skills lie in RC Soldiers working in DoD and civilian CMF positions there is the potential their mobilization or deployment in support of CO, would hinder the organizations they left.[vi] Although this may be true in some cases, the overall advantage with civilian acquired skills is these RC Soldiers, regardless of location, have the opportunity to maintain currency in training, certification, and operational experience not afforded if they were not working in civilian IT or CO industries.

iii. Partnerships (Civilian Industry and Other Governmental)

In like manner, the USAR Private Public Partnership (P3) vision is for generating readiness through RC units partnered to develop, integrate, and direct mutually supporting relationships. These partnerships support the USAR's overall mission to provide trained, equipped, and ready Soldiers.[44] In February 2015 Lieutenant General Talley, Chief of the Army Reserve, launched

[vi] In some DoD employment cases, RC Soldiers would also move from their civilian to a military capacity within the same organization providing no additional resource to the organization.

the new cybersecurity P3 due to the need for experts in both the civilian and military sectors.[45] Cyber P3, "strives to recruit more cyber warriors, improve the skills of those already in the field, connect potential cyber professionals with employers, and generates interest in military and cyber security career fields."[46] Initially this program consists of 06 universities,[vii] 12 corporate partners, and the Federal Bureau of Investigation (FBI).

Due to perpetual change, for the RC to be an effective part of the CMF, there is a need for "immersion" and civilian jobs in the cyber career field.[47] The initial focus, "is on those really, truly, tip of the spear cyber security defenders in the Army Reserve," because technology and threats change constantly.[48] Further develop of this program helps address part of a concern raised in 2013 by Lieutenant General Cardon, Commander ARCYBER, that, "the elite cyber teams the Army's trying to build aren't particularly well-suited for part-time work."[49]

iv. Collective Training (Day to Day, Exercise, and Emergency).

Collective training for RC CMF has some flexibility and accomplishable through differing opportunities depending on the unit's location in the RC Army Force Generation (ARFORGEN)[viii] cycle and prior planning. This training varies in length, funding and the amount of interaction with AC forces.

For USAR forces there are internal opportunities to execute complex ARFORGEN externally evaluated collective training as part of the Combat Support Training Program (CSTP) during training year two and three. Units usually execute this training during the USAR's Warrior Exercises (WAREX) or Combat Support Training Exercises (CSTX) ranging from 15-21 days.

[vii] The university part of the partnership looks for ways to sponsor scholarships and funding for academic cyber security training while seeking schools, "that offered non-traditional courses and distance learning to meet the needs of its soldiers, many of whom have full-time jobs." (Tan 2015)

[viii] The RC's ARFORGEN model is part of the RC training transformation through integration of the Sustainable Readiness Model (SRM) and Objective T-Level into the "Plan, Prepare, and Provide" approach. T-Level is an assessment of the unit's ability to provide the capabilities for which designated. (Commander, U.S. Army Reserve Command n.d.) Traditionally it has been a 1:5 model providing the required supply-based combat support and service support to Total Force requirements. (U.S. Army Reserve 2011)

ARNG also has similar exercises, like Cyber Shield, focused on certification, confirmation, and validation of RC CMF capabilities.[50]

Overseas Deployment Training (ODT) facilitates RC participation in external UCC exercises. These training opportunities, averaging 16-21 days, facilitate RC CMF participation in, "high pay-off ODTs that accomplish unit Mission Essential Task List (METL), provide a unit assessment, and support mission critical theater engagement."[51] RC CMF gain another opportunity for collective training with the AC through participation in the cyber portions of Combat Training Center (CTC) rotations or Warfighter Exercises (WFX) that average 29 day. External Evaluations (EXEVAL) along with the Army Total Force Policy (ATFP) are two final methods for RC CMF collective training in complex environments.[52] ATFP facilitates AC/RC engagement, "to foster relationships and develop mutually supportive training partnerships to include access to AC facilities whenever it supports training."[53]

Participation in cyber training and exercises[ix] are all unique EXEVAL opportunities. These programs facilitate training the RC CMF on a part-time, exercise, and recurring basis while fostering relationships required for successful integration of AC/RC CMFs.

Integration of RC Cyber Mission Forces

It is equally important to understand similarities and differences of RC CMF in order to achieve unity of effort. Based upon their classification there are many categories of Soldiers and Civilians who provide different benefits and drawbacks when working to integrate them into CFM requirements. The base blocks for understanding RC forces is through the different types,

[ix] Cyber training or exercises having cyber components and unique EXEVAL opportunities are: Cyber Flag or Guard (USCYBERCOM), Global Thunder (STRATCOM), Terminal Fury (PACOM), Austere Challenge (EUCOM), NSA Cyber Defense Exercise (NSA), World Class OPFOR (ARCYBER), Cyber Avenger (ARCOG), Cyber Shield (ARNG), Cyber Patriot (STEM), Cyber Collegiate (STEM) are all unique EXEVAL opportunities.

authorities, and unique restrictions like the *Posse Comitatus Act* limitations affecting integration.[54]

Types of RC Forces (State Active Duty, Tile-10, Title-32).

i. USAR Forces (Title-10)

The USAR, similar to the AC, is composed solely of Title-10 (federal control and federal paid) forces.[x] These Soldiers fall under the C2 of the President, as the Commander-in-Chief. Additionally while in a duty status, Soldiers are governed by the military Uniform Code of Military Justice (UCMJ). This federal duty status makes the USAR subject to *Posse Comitatus Act* limitations.

A traditional Troop Programed Unit (TPU) is composed primarily of Ready Reserve Soldiers who have a part-time statutory drilling obligation. Along with a few RC Soldiers on active duty, in an Active Guard/Reserve (AGR) status, Ready Reserve Soldiers participate in paid monthly training assemblies totaling 24 days or 48 Inactive Duty Training (IDT) periods per fiscal year. Dependent of funding, these Soldiers also have an authorization of between 14 and 29 days of active duty Annual Training (AT) each fiscal year.

Soldiers who no longer have an active drilling obligation are able to move for the remainder of their service obligation to the Individual Ready Reserve (IRR), thus removing their drilling participation unless activated during a Presidential call up. Within the IRR, there are also Soldiers who participate in the Individual Mobilization Augmentee (IMA) or Drilling Individual Mobilization Augmentee (DIMA) programs. These two programs facilitate rapid expansion of

[x] Although this research primarily focuses on the Soldier, there is also a RC Civilian population composed of Military Technicians (MILTEC) and Department of the Army Civilians (DAC) who, along with AGR Soldiers, performs the daily operational functions not executable during IDT drills. (U.S. Army Reserve 2002)

the Army to meet, "contingency, pre-mobilization, mobilization, sustainment, and / or demobilization operations."[55]

ii. ARNG Forces (State Active Duty, Title-32, Title-10)

Unlike the USAR, the ARNG is composed of three different force types providing unique capabilities for state Governors. These forces also require equally unique understanding on how to best utilize them in support Homeland Defense, Homeland Security, and DSCA requirements.

ARNG forces on Sate Active Duty (state control and state funded) are Soldiers on active duty in direct support of the individual state Governor. These forces are available for utilization in support of emergency response or for routine support to state and local authorizes. These Soldiers fall under the C2 of the state Governor, as the Commander-in-Chief, and are under state law and not the military UCMJ. They are not subject to the *Posse Comitatus Act* and available for law enforcement.[56]

ARNG Title-32 (state control and federal funded) Soldiers differ from State Active Duty. These part-time Soldiers receive federal funding, but remain under the C2 of the state Governor and still overseen under state law. A key advantage during a Presidential disaster or emergency declaration is their activated with federal funding while still not being subject to *Posse Comitatus Act* limitations.[57]

The last type is ARNG Title-10 (federal control and federal funded) Soldiers federalized and equivalent to other Title-10 forces under the C2 of the President and subject to the military UCMJ. This federal C2 makes them subject to *Posse Comitatus Act* limitations. Although there are exceptions, this is the status normally utilized for Soldiers mobilized or deployed overseas. [58]

One example of an ARNG Title-10 exception is the 1636th CPT.[59] However, many of the 10 proposed ARNG CPTs will be composed of ARNG Title-32 Soldiers. These forces have contact

with state and local organizations on a routine basis making them uniquely positioned to support the DSCA protection of state and local critical infrastructure mission.

RC CMF Location Requirements

In order for RC CMF "immersion", there is a requirement to have access to Top Secret classified systems. Unfortunately, a majority of the reserve centers are not normally equipment with this type of equipment. Until there are mobile Sensitive Compartmented Information Facilities (SCIF) available, one solution is to extend these systems to RC locations – very expensive and security intensive – or to collocate RC CMF with locations already having classified access. Facilities already created under DoD Directive 3325.11, *Joint Reserve Intelligence Program (JRIP),* are ideal locations for RC CMF. Another possibility for RC CMF to gain access to the required classified systems, while also achieving unity of effort, is to integrate or collocate with organizations – DoD or DHS – who already execute CO. The ARCOG and the VA DPU have units already collocated in some of these facilities.

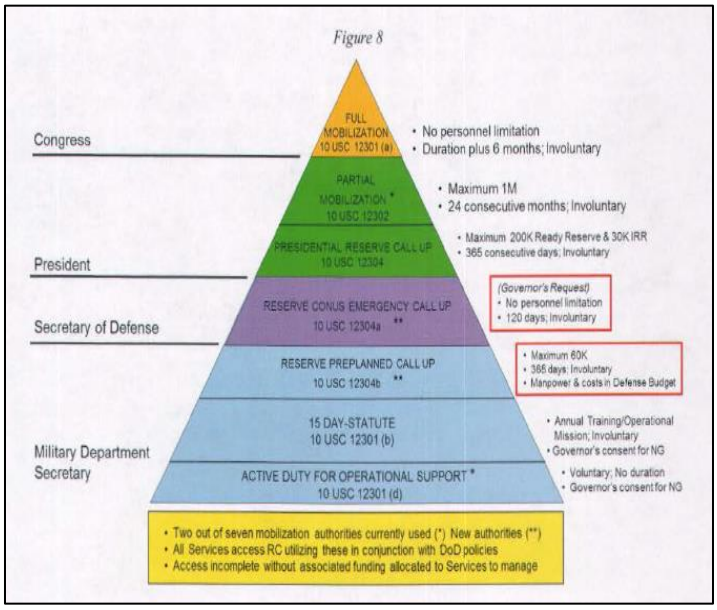
RC Sources and Resourcing Authorities (12301-12304)

The figure provided below in the Report to Congress, *Unit Cost And Readiness For The Active And Reserve Components Of The Armed Forces*, lays a good framework of the major authorities (Title 10 USC § 12301, 12302, and 12304)[xi] available to involuntarily access RC

[xi] Title 10 USC § 12301. 12301(a), last utilized during WWII, requires a congressional declaration of war, but supports full mobilization of the RC forces for the duration required and is primarily for rapid expansion in the event of external threat.[xi] 12301(b), under the authority of the Service Secretary, is a short term involuntary recall of a unit or individuals at any time to active duty for a period not to exceed 15 days per fiscal year. For utilization of ARNG Soldiers it further requires consent of the state's Governor. 12301(d) is the only voluntary recall, but it still requires the Service Secretary authorization and the consent of the Service Member. "This authority has no limits to the number of personnel; however, Services Secretaries are responsible to provide pay and benefits within Service budgets and in alignment with manpower and personnel end-strength policies."

Title 10 USC § 12302. 12302, utilized most recently during Operation Noble Eagle and Enduring Freedom, requires a Presidential declaration of national emergency and allows for a partial mobilization limited to one million Soldier for a maximum of 24 consecutive months while also making provisions for repeated mobilization.

forces in an active status to meet requirements outside of a thirty day requirement. There is also one provision – 10 USC § 12301(d) – that allows for voluntary recall.[60] The major drawback – vocalized by AC forces – to the integration of RC forces under these provisions, outside of national emergencies, is the prior planning, coordination, and extended lead-time it takes to get authorization for this funding.



Conclusion

As cyberspace continues to play an important role in projection of military power, in an environment where the mission of tomorrow is ill defined and budgets are becoming constrained, there is an increasing need for a Total Force (AC/RC) concept. The Army's RC is uniquely postured to fill current, midterm and longer-term cyber requirements, but it requires planning and investment now in training, development, and integrations of the RC CMF.

In the past training, development, and integration of RC forces has been a lower priority as new Army capabilities were developed. The primary focus was on addressing the AC first resulting in a "bolt on" approach to integration of RC once the AC capabilities were developed.

Title 10 USC § 12304. 12304, requires a Presidential, "determination of RC augmentation requirements for named operational missions." It is further restricted to 200 thousand for no more than 365 days per contingency. This authority also makes provisions for repeated mobilizations under differing contingencies. 12304a, utilized for Hurricane Sandy 2012, requires the Secretary of Defense authorization, "in response to a state Governor's request for federal assistance. This is a new authority that has no limit on the number of personnel but is limited to a period of mobilization not to exceed 120 days." 12304b, currently without an example of usage, "requires Service Secretary authority for preplanned and pre-budgeted requirements in support of combatant commands," and is, "limited to 60,000 personnel at any one time for a maximum of 365 consecutive days. (The Department of Defense 2013)

However, within the Army CMF development, both the USAR and ARNG have been involved in the standup of the Army's CMF organizations and mission forces from the beginning.

The current focus should be on "tip of the spear" RC CMF. At present the proposed 21 Army RC CPTs – 10 USAR and 11 ARNG – are not identified within the Army's 41 or part of the DoD's 133 teams identified within the 2015 *Department of Defense Cyber Strategy*. The USAR ARCOG CPTs, once approved, will provide an overall capacity of 10 CPTs, at a minimum rotational rate of two per fiscal year, within the RC ARFORGEN 1:5 training model. The best utilization of these Title-10 CPTs is as service retained forces capable of filling federal contingency and programed UCC requirements. The ARNG CPTs are a combination of Title-10 and Title-32 forces. The ARNG (Title-10) 1636th CPT, in support of ARCYBER, already presents a unique opportunity for the ARNG to have forces "immersion" in the military cyber career field. The remaining 10 proposed CPTs are composed of ARNG Title-32 Soldiers. Integration within state and local agencies, not restricted by the *Posse Comitatus Act*, and having ties to DHS and the 10 FEMA regions places theses ARNG (Title-32) CPTs in the best position to support USNORTHCOM's DSCA mission.

The RC training and development is flexible and accomplishable through differing opportunities depending on where in the ARFORGEN cycle the unit is located. In addition to attending AC training, with continued development, the COTC and CSTC training centers will provide the opportunity for RC CMF to gain the required training through RC friendly courses. ODT, CTC or WFX rotations, EXEVAL, and the ATFP are all unique cyber training and exercises opportunities. Civilian acquired skills and further develop of the Cyber P3 programs support core mission proficiency and help alleviate concerns RC CPTs are not, "particularly

well-suited" for the CMF.[61] In summation, these programs foster relationships required for successful integration of AC/RC CMFs.

When it comes to integration of RC CMF, within an understanding of the different types, authorities, funding, and unique restrictions, the USAR and ARNG are key, "enablers for Total Army requirements, both augmenting and relieving stress on the active Army."[62] Although the RC moved cautiously in building the RC CMF, some of the distinct advantages of many RC Soldiers are their ties to the communities, full-time employment in civilian IT, and their dispersion across the country. Additionally, unlike Title-10 USAR or AC organizations bound by the *Posse Comitatus Act* limitations, the ARNG in there direct support role to the Governors, during non-federalized status, can provide assistance to state and local authorities during civil support operations. Finally, it is important to position USAR units in proximity to AC CMF and provide access to classified facilities for all RC CMF. If this is not feasible, facilities already created under JRIP provide a good alternative. Placing RC CMF Soldiers daily, weekly and monthly within the state, federal and AC CMF will also facilitate ease of integration and access when a cyber-threat occurs.

All of these efforts support AC/RC CMF training, integration, and development in preparation for mobilization or deployment in support of CO missions. "Given the heavy reliance on military computer networks and critical infrastructure, it is essential that the Army be able to defend key systems and ensure the continuity of critical network functions in the face of disruption. The mission to defend our network is a priority."[63] The Army's RC CMF is uniquely postured to meet this challenge.

Air University Eaker Child Research Information Center
Digital Collections
Air University, Maxwell AFB, AL

End Notes

[1] Lynn, William F. III, Department of Defense. "Defending a New Domain: The Pentagon's Cyberstrategy." Foreign Affairs. Volume 89, Number 5, 10/11 2010: 97-108, 105.

[2] The Department of Defense. *The Department of Defense Cyber Strategy.* DoD Cyber Strategy, Washington D.C.: The Department of Defense, 2015, 9.

[3] Ibid, i.

[4] The White House. *National Security Strategy.* National Security Strategy, Washington D.C.: The White House, 2015, i-ii.

[5] Ibid, 11.

[6] The Department of Defense. *The National Miltiary Strategy of the United States of America.* National Miltiary Strategy , Washington D.C.: The Department of Defense, 2015, 7.

[7] Department of the Army. *Army Posture Satement.* Congressional Report, Washington D.C.: Department of the Army, 2015.

[8] The Department of Defense. *The National Miltiary Strategy of the United States of America.* National Miltiary Strategy , Washington D.C.: The Department of Defense, 2015, 15-16.

[9] The Department of Defense. *The Department of Defense Cyber Strategy.* DoD Cyber Strategy, Washington D.C.: The Department of Defense, 2015.

[10] Ibid, Cover Letter.

[11] Ibid, 13-28.

[12] Ibid,13-19.

[13] Ibid, 6.

[14] The Department of Defense. *Quadrennial Defense Review 2014.* Quadrennial Defense Review, Washington D.C.: The Department of Defense, 2014, p 41

[15] The Department of Defense. *The Department of Defense Cyber Strategy.* DoD Cyber Strategy, Washington D.C.: The Department of Defense, 2015, 6.

[16] Federal News Radio Custom Media. "Army ponders proper shape, size of cyber workforce." *Federal News Radio.* October 28, 2013. http://federalnewsradio.com/defense/2013/10/army-ponders-proper-shape-size-of-cyber-workforce/ (accessed 10 12, 2015).

[17] Joint Chiefs of Staff. "JP 3-12(R), Cyberspace Operations." *Joint Electron Library.* 02 05, 2013. http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm (accessed 09 03, 2015), vii.

[18] Army Cyber Command, Leavenworth Support Element. *Army Cyberspace Operations Capabilities Based Assessment (Cyber CBA).* Capabilities Based Assessment, Fort Leavenworth: Leavenworth Support Element, 2013, FACER

[19] Joint Chiefs of Staff. "JP 3-12(R), Cyberspace Operations." *Joint Electron Library.* 02 05, 2013. http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm (accessed 09 03, 2015), vii.

[20] Ibid.

[21] Ibid, II-2.

[22] Ibid, vii.

[23] Army Cyber Command, Leavenworth Support Element. *Army Cyberspace Operations Capabilities Based Assessment (Cyber CBA).* Capabilities Based Assessment, Fort Leavenworth: Leavenworth Support Element, 2013, FACER

Muir S. Fairchild Research Information Center
Digital Collections
University–Maxwell AFB, AL

[24] Joint Chiefs of Staff. "JP 3-12(R), Cyberspace Operations." *Joint Electron Library.* 02 05, 2013. http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm (accessed 09 03, 2015), III-2.

[25] Ibid, ix.

[26] Seffers, George I., Technology Editor. "U.S. Army Builds Cyber Branch One Step at a Time." *AFCEA.* 04 01, 2015. http://www.afcea.org/content/?q=Article-us-army-builds-cyber-branch-one-step-time (accessed 10 12, 2015).

[27] Army Reserve Cyberspace Operations Group. *Concept Plan for ARCOG (W8MBAA) and Cyber Protection Teams.* Concept Plan, Adelphi, MD: USAR ARCOG, 2014, 4.

[28] Ibid, Executive Summary.

[29] Key, Kyle Capt. "Cyber Warriors flex digital muscle at 2014 Cyber Shield Exercise." *U.S. Army.* June 05, 2014. http://www.army.mil/article/127453/ (accessed 12 10, 2015).

[30] Ibid.

[31] Puryear, Cotton. "Virginia cyber warriors join multi-state exercise at Camp Atterbury." *Virginia National Guard.* April 08, 2015. http://vaguard.dodlive.mil/2015/04/08/7302/#sthash.3eM0vfhU.OhzwvzdT.dpuf (accessed 12 10, 2015).

[32] Milord, Mike, Army Cyber Command. "Army Cyber Command, Army Guard sign memorandum to integrate cyber protection team." *U.S. Army.* 06 05, 2014. http://www.army.mil/article/127442/ (accessed 12 07, 2015).

[33] Milord, Mike, Army Cyber Command. "Army Guard's first cyber protection team activated, receives new insignia." *U.S. Army.* October 22, 2014. http://www.army.mil/article/136721/ (accessed 12 07, 2015).

[34] Washington Report. "Army Guard Begins Creating 10 Cyber Teams." *NGAUS.* March 03, 2015. http://www.ngaus.org/newsroom/news/army-guard-begins-creating-10-cyber-teams (accessed 10 12, 2015).

[35] Soucy, Jon SFC, National Guard Bureau. "National Guard set to activate additional cyber units." *U.S. Army.* 12 09, 2015. http://www.army.mil/article/159759/National_Guard_set_to_activate_additional_cyber_units/?from=RSS (accessed 12 10, 2015).

[36] U.S. Army Cyber Center of Excellence. *U.S. Army Cyber Center of Excellence Strategic Plan.* Strategic Plan, Fort Gordon: U.S. Army CyberCoE, 2015, 2.

[37] U.S. Army Cyber Center of Excellence. *U.S. Army Cyber Center of Excellence.* n.d. http://cybercoe.army.mil/index.php/291-cybercoe/1045-cyber-center-of-excellence (accessed 12 08, 2015).

[38] U.S. Army Cyber Center of Excellence. *U.S. Army Cyber Center of Excellence Strategic Plan.* Strategic Plan, Fort Gordon: U.S. Army CyberCoE, 2015, 3.

[39] U.S. Army Cyber Protection Brigade. *Cyber Protection Brigade Overiew.* Organizational Briefing, Fort Gordon: CPB, 2015.

[40] Vergun, David. "Army may create cyber career field for civilians." *U.S. Army.* 04 15, 2015. http://www.army.mil/article/146485/Army_may_create_cyber_career_field_for_civilians/ (accessed 10 12, 2015).

[41] National Guard Professional Education Center. *Cyber Operations Training Center (COTC).* n.d. http://www.pec.ng.mil/COTC (accessed 12 08, 2015).

[42] U.S. Army Cyber Command. "ARCYBER RC Working Group: Executive Summary." *ARCYBER RC Integration Working Group.* Ft. Belvoir: U.S. Army Cyber Command, 2015. 01.

[43] U.S. Army CyberCoE. *Cyber Security Training Center (CSTC) - Fort McCoy, WI.* n.d. https://ia.signal.army.mil/mccoy/default.asp (accessed 12 08, 2015).

[44] U.S. Army Reserve. *Private Public Partnership Office (P3O) United States Army Reserve.* n.d. http://www.usar.army.mil/Featured/PrivatePublicPartnership.aspx (accessed 10 08, 2015).

[45] Tan, Michelle, Staff writer. "Army Reserve partnership aims to grow cyber warriors." *ArmyTimes.* 02 16, 2015. http://www.armytimes.com/story/military/guard-reserve/2015/02/16/army-reserve-cyber-partnership/23351603/ (accessed 10 12, 2015).

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Federal News Radio Custom Media. "Army ponders proper shape, size of cyber workforce." *Federal News Radio.* October 28, 2013. http://federalnewsradio.com/defense/2013/10/army-ponders-proper-shape-size-of-cyber-workforce/ (accessed 10 12, 2015).

[50] Key, Kyle Capt. "Cyber Warriors flex digital muscle at 2014 Cyber Shield Exercise." *U.S. Army.* June 05, 2014. http://www.army.mil/article/127453/ (accessed 12 10, 2015).

[51] Commander, U.S. Army Reserve Command. "Army Reserve Command Training Guidance (CTG) - Fiscal Years (FY) 2016 – 2017." *MEMORANDUM FOR Commanders, Army Reserve Operational, Functional, Training, and Support Commands.* Fort Bragg: Headquarters, USARC, n.d.

[52] Ibid.

[53] Ibid.

[54] Luke, Ivan, Joint Military Operations Department. "DOD Operations in the Homeland: Context and Issues for the Commander." *NWC 2067C.* U.S. Naval War College, 07 2014, 3.

[55] U.S. Army Human Resources Command. *IMA Program Overview.* n.d. https://www.hrc.army.mil/staff/ima%20program%20overview (accessed 12 03, 2015).

[56] Luke, Ivan, Joint Military Operations Department. "DOD Operations in the Homeland: Context and Issues for the Commander." *NWC 2067C.* U.S. Naval War College, 07 2014, 3.

[57] Ibid.

[58] Ibid.

[59] Milord, Mike, Army Cyber Command. "Army Guard's first cyber protection team activated, receives new insignia." *U.S. Army.* October 22, 2014. http://www.army.mil/article/136721/ (accessed 12 07, 2015).

[60] The Department of Defense. "Unit Cost and Readiness for Active and Reserve Component of the Armed Forces." *The National Guard Association of the United States.* 12 20, 2013. http://www.ngaus.org/sites/default/files/CAPE%20FINAL%20ACRCMixReport.pdf (accessed 10 12, 2015).

[61] Federal News Radio Custom Media. "Army ponders proper shape, size of cyber workforce." *Federal News Radio.* October 28, 2013. http://federalnewsradio.com/defense/2013/10/army-ponders-proper-shape-size-of-cyber-workforce/ (accessed 10 12, 2015).

[62] U.S. Army Reserve. *United States Army Reserve Vision & Strategy An Operational Force Providing Strategic Depth in an Era of Persistent Conflict.* USAR Vision & Strategy, Washington D.C.: U.S. Army Reserve, 2011, 20.

[63] Department of the Army. *Army Strategic Planning Guidance 2013.* Strategic Planning Guidance, Washington D.C.: Department of the Army, 2013, 6.

Air University–Maxwell AFB, AL

Appendix A: Glossary

AC	Active Component
AC/RC	Active / Reserve Component
ARCERT	Army Computer Emergency Response Team
ARCOG	Army Reserve Cyber Operations Group/ Army Reserve Information Operations Command
ARCYBER	U.S. Army Cyber Command
ARFORGEN	Army Force Generation
ARNG	U.S. Army National Guard
ASCC	Army Service Component Command
AT	Annual Training
ATFP	Army Total Force Policy
C2	Command and Control
CEH	Certified Ethical Hacker
CMF	Cyber Mission Force
CMT	Combat Mission Teams
CND	Computer Network Defense
CNDT	Computer Network Defense Teams
CNO	Computer Network Operations
CO	Cyber Operations
COTC	Cyber Operations Training Center
CPT	Cyber Protection Teams
CST	Combat Support Teams
CSTC	Cyber Security training Center
CSTP	Combat Support Training Program
CSTX	Combat Support Training Exercises
CTC	Combat Training Center
Cyber CoE	U.S. Army Cyber Center of Excellence
CyberSpt	Cyber Support
CySA	Cyber Situational Awareness
DAC	Department of the Army Civilians
DCO	defensive cyberspace operations
DCO-RA	defensive cyberspace operations - response action
DHS	Department of Homeland Security
DIMA	Drilling Individual Mobilization Augmentee
DISA ARE	Defense Information Support Agency Army Reserve Element
DNI	Director of National Intelligence
DoD	Department of Defense
DODIN	DoD Information Network
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities
DPU	Data Processing Units
DSCA	Defense Support of Civil Authorities
DTF	Digital Training Facilities
DTMS	Army Digital Training Management Systems
EW	Electronic Warfare
EXEVAL	External Evaluations
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FTX	Field Training Exercise
IA	Information Assurance
ICC	Individual Cyber Courses
ICoE	U.S. Army Intelligence Center of Excellence
IDT	Inactive Duty Training
IMA	Individual Mobilization Augmentee
IO	Information Operations
IRR	Individual Ready Reserve
IT	Information Technology
ITEB	Training Equivalency Board
JNAC	Joint Network Attack Course
JQR	Joint Qualification Review
JRIP	Joint Reserve Intelligence Program
JRVIO	Joint Virtual Reserve Component Information Operations
M-Day	ARNG Traditional Part-Time Soldiers
METL	Mission Essential Task List
MI	Guard's Cyber Backbone Network
MI	Military Intelligence
MILTEC	Military Technicians
MIRC	Military Intelligence Readiness Command
NetOps CONOPS	Joint Concept of Operations for the Global Information Grid NetOps
NMS	National Military Strategy
NMT	National Mission Teams
NSS	National Security Strategy
NST	National Support Teams
OCO	offensive cyberspace operations
ODT	Overseas Deployment Training
P3	Private Public Partnership
PEC	Professional Education Center
RC	Reserve Component
RIOCC	Reserve Information Operations Coordination Center
SC	Signal
SCIF	Sensitive Compartmented Information Facilities
SecDef	Secretary of Defense
SIGCoE	U.S. Army Signal Center of Excellence
SRM	Sustainable Readiness Model
STEM	Science, Technology, Engineering, and Mathematics Education
SWACC	South West Asia Cyber Center
TIOG	Theater Information Operations Groups
TPU	Troop Programed Units
TRADOC	U.S. Army Training and Doctrine Command
TSC	Theater Signal Commands
U.S.	United States
UCC	Unified Combatant Command
ULO	Unified Land Operations
US CYBERCOM	U.S. Cyber Command
US EUCOM	U.S. European Command
US NORTHCOM	U.S. Northern Command
US PACOM	U.S. Pacific Command
US STRATCOM	U.S. Strategic Command
USAR	U.S. Army Reserve
USC	U.S. Code
VA IOSC	Virginia Information Operations Support Command
VTIP	Voluntary Transfer Incentive Program
WAREX	Warrior Exercises
WFX	Warfighter Exercises

U.S. Fairchild Research Information Digital Collections Air University Maxwell AFB

Bibliography

Army Cyber Command, Leavenworth Support Element. *Army Cyberspace Operations Capabilities Based Assessment (Cyber CBA).* Capabilities Based Assessment, Fort Leavenworth: Leavenworth Support Element, 2013.

Army Reserve Cyberspace Operations Group. *Concept Plan for ARCOG (W8MBAA) and Cyber Protection Teams.* Concept Plan, Adelphi, MD: USAR ARCOG, 2014.

Commander, U.S. Army Reserve Command. "Army Reserve Command Training Guidance (CTG) - Fiscal Years (FY) 2016 – 2017." *MEMORANDUM FOR Commanders, Army Reserve Operational, Functional, Training, and Support Commands.* Fort Bragg: Headquarters, USARC, n.d.

Department of the Army. *Army Posture Satement.* Congressional Report, Washington D.C.: Department of the Army, 2015.

Department of the Army. *Army Strategic Planning Guidance 2013.* Strategic Planning Guidance, Washington D.C.: Department of the Army, 2013.

Federal News Radio Custom Media. "Army ponders proper shape, size of cyber workforce." *Federal News Radio.* October 28, 2013. http://federalnewsradio.com/defense/2013/10/army-ponders-proper-shape-size-of-cyber-workforce/ (accessed 10 12, 2015).

Joint Chiefs of Staff. "JP 3-12(R), Cyberspace Operations." *Joint Electron Library.* 02 05, 2013. http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm (accessed 09 03, 2015).

Key, Kyle Capt. "Cyber Warriors flex digital muscle at 2014 Cyber Shield Exercise." *U.S. Army.* June 05, 2014. http://www.army.mil/article/127453/ (accessed 12 10, 2015).

Luke, Ivan, Joint Military Operations Department. "DOD Operations in the Homeland: Context and Issues for the Commander." *NWC 2067C.* U.S. Naval War College, 07 2014.

Lynn, William F. III, Department of Defense. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs. Volume 89, Number 5*, 10/11 2010: 97-108.

Milord, Mike, Army Cyber Command. "Army Cyber Command, Army Guard sign memorandum to integrate cyber protection team." *U.S. Army.* 06 05, 2014. http://www.army.mil/article/127442/ (accessed 12 07, 2015).

—. "Army Guard's first cyber protection team activated, receives new insignia." *U.S. Army.* October 22, 2014. http://www.army.mil/article/136721/ (accessed 12 07, 2015).

National Guard Professional Education Center. *Cyber Operations Training Center (COTC).* n.d. http://www.pec.ng.mil/COTC (accessed 12 08, 2015).

Puryear, Cotton. "Virginia cyber warriors join multi-state exercise at Camp Atterbury." *Virginia National Guard.* April 08, 2015. http://vaguard.dodlive.mil/2015/04/08/7302/#sthash.3eM0vfhU.OhzwvzdT.dpuf (accessed 12 10, 2015).

Seffers, George I., Technology Editor. "U.S. Army Builds Cyber Branch One Step at a Time." *AFCEA.* 04 01, 2015. http://www.afcea.org/content/?q=Article-us-army-builds-cyber-branch-one-step-time (accessed 10 12, 2015).

Soucy, Jon SFC, National Guard Bureau. "National Guard set to activate additional cyber units." *U.S. Army.* 12 09, 2015. http://www.army.mil/article/159759/National_Guard_set_to_activate_additional_cyber_units/?from=RSS (accessed 12 10, 2015).

Tan, Michelle, Staff writer. "Army Reserve partnership aims to grow cyber warriors." *ArmyTimes.* 02 16, 2015. http://www.armytimes.com/story/military/guard-reserve/2015/02/16/army-reserve-cyber-partnership/23351603/ (accessed 10 12, 2015).

The Department of Defense. *Quadrennial Defense Review 2014.* Quadrennial Defense Review, Washington D.C.: The Department of Defense, 2014.

The Department of Defense. *The Department of Defense Cyber Strategy.* DoD Cyber Strategy, Washington D.C.: The Department of Defense, 2015.

The Department of Defense. *The National Miltiary Strategy of the United States of America.* National Miltiary Strategy , Washington D.C.: The Department of Defense, 2015.

—. "Unit Cost and Readiness for Active and Reserve Component of the Armed Forces." *The National Guard Association of the United States.* 12 20, 2013. http://www.ngaus.org/sites/default/files/CAPE%20FINAL%20ACRCMixReport.pdf (accessed 10 12, 2015).

The White House. *National Security Strategy.* National Security Strategy, Washington D.C.: The White House, 2015.

U.S. Army Cyber Center of Excellence. *U.S. Army Cyber Center of Excellence.* n.d. http://cybercoe.army.mil/index.php/291-cybercoe/1045-cyber-center-of-excellence (accessed 12 08, 2015).

U.S. Army Cyber Center of Excellence. *U.S. Army Cyber Center of Excellence Strategic Plan.* Strategic Plan, Fort Gordon: U.S. Army CyberCoE, 2015.

U.S. Army Cyber Command. "ARCYBER RC Working Group: Executive Summary." *ARCYBER RC Integration Working Group.* Ft. Belvoir: U.S. Army Cyber Command, 2015. 01.

U.S. Army Cyber Protection Brigade. *Cyber Protection Brigade Overiew.* Organizational Briefing, Fort Gordon: CPB, 2015.

U.S. Army CyberCoE. *Cyber Security Training Center (CSTC) - Fort McCoy, WI.* n.d. https://ia.signal.army.mil/mccoy/default.asp (accessed 12 08, 2015).

U.S. Army Human Resources Command. *IMA Program Overview.* n.d. https://www.hrc.army.mil/staff/ima%20program%20overview (accessed 12 03, 2015).

U.S. Army Reserve. *Private Public Partnership Office (P3O) United States Army Reserve.* n.d. http://www.usar.army.mil/Featured/PrivatePublicPartnership.aspx (accessed 10 08, 2015).

U.S. Army Reserve. *United States Army Reserve Vision & Strategy An Operational Force Providing Strategic Depth in an Era of Persistent Conflict.* USAR Vision & Strategy, Washington D.C.: U.S. Army Reserve, 2011.

—. "US Army Reserve Military Technician Information Handbook." *Civilian Personnel Advisory Center.* November 20, 2002. http://www.mccoy.army.mil/Civilians/documents/Military_Technician_Handbook.pdf (accessed 12 09, 2015).

Vergun, David. "Army may create cyber career field for civilians." *U.S. Army.* 04 15, 2015. http://www.army.mil/article/146485/Army_may_create_cyber_career_field_for_civilians/ (accessed 10 12, 2015).

Washington Report. "Army Guard Begins Creating 10 Cyber Teams." *NGAUS.* March 03, 2015. http://www.ngaus.org/newsroom/news/army-guard-begins-creating-10-cyber-teams (accessed 10 12, 2015).

Fairchild Research Information Center
Digital Collections