THE
LAND
WARFARE
PAPERS

No. 103W SEPTEMBER 2014

Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight

Christopher R. Quick

A National Security Affairs Paper
published on occasion by
**THE INSTITUTE OF
LAND WARFARE**
ASSOCIATION OF THE
UNITED STATES ARMY
Arlington, Virginia

Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight

by

Christopher R. Quick

The Institute of Land Warfare
ASSOCIATION OF THE UNITED STATES ARMY

AN INSTITUTE OF LAND WARFARE PAPER

The purpose of the Institute of Land Warfare is to extend the educational work of AUSA by sponsoring scholarly publications, to include books, monographs and essays on key defense issues, as well as workshops and symposia. A work selected for publication as a Land Warfare Paper represents research by the author which, in the opinion of ILW's editorial board, will contribute to a better understanding of a particular defense or national security issue. Publication as an Institute of Land Warfare Paper does not indicate that the Association of the United States Army agrees with everything in the paper but does suggest that the Association believes the paper will stimulate the thinking of AUSA members and others concerned about important defense issues.

LAND WARFARE PAPER NO. 103W, September 2014

Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight

by Christopher R. Quick

Lieutenant Colonel Christopher R. Quick is currently the J39 Information Operations Branch Chief for Special Operations Command Forward–West Africa in Kelly Barracks, Stuttgart, Germany. He previously served as the Information Operations Branch Chief and Director of Communication Synchronization for U.S. Army Cyber Command/Second Army at Fort Belvoir, Virginia.

This paper represents the opinions of the author and should not be taken to represent the views of the Department of the Army, the Department of Defense, the United States government, the Institute of Land Warfare or the Association of the United States Army or its members.

Inquiries regarding this and future Land Warfare Papers should be directed to: Director, AUSA's Institute of Land Warfare, 2425 Wilson Boulevard, Arlington VA 22201, e-mail *sdaugherty@ausa.org* or telephone (direct dial) 703-907-2627 or (toll free) 1-800-336-4570, ext. 2627.

Contents

Foreword

According to the author of this monograph, the Army should create a Total Army Cyber Force that builds Cyber Mission Force (CMF)-like teams in the reserve component that are trained to the joint standard but capable of conducting a wide range of missions in support of Army and joint requirements. Building an "operational cyberspace reserve" would be cost effective, provide agile and adaptive leaders and integrate experienced network operators who use innovation and initiative to support Army and U.S. Cyber Command requirements.

By leveraging the mixture of talented reserve component personnel already in uniform and with a combination of military and civilian training and experience, says Lieutenant Colonel Quick, the Army can mitigate the short-term stress on active component units. It would further diminish emerging stressors with an accessible, trained and ready surge capacity that represents more than 50,000 man-days of support annually without requiring mobilization. These forces are capable of conducting steady-state operations, consequence management, crisis response and homeland defense for the Army and state entities as required.

If adopted, this concept would bolster the Army's capability and increase the available number of CMF teams from 41 to 61 for the Army, at a fraction of the cost, and start providing reserve component CMF teams as early as Fiscal Year 2015.

Gordon R. Sullivan
General, U.S. Army Retired
President, Association of the United States Army

26 September 2014

Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight

Introduction

The creation of U.S. Cyber Command (USCYBERCOM)—a four-star command—and the subsequent creation of service-level three-star commands[1] that conduct the full spectrum of operations in cyberspace[2] have placed a new level of emphasis on those qualified to work in the evolving cyber career field. While getting a qualified work force in place has always been a challenge for the information technology (IT) community, it has been exacerbated by the emerging need to recruit, develop and retain a qualified force capable of meeting the skill requirements levied by USCYBERCOM and the Department of Defense (DoD). USCYBERCOM has stated that it wants to develop an estimated 5,000 military and civilian personnel to make up a larger Cyber Mission Force (CMF)[3] to serve in three capacities: protect critical national information systems, support combatant commanders abroad and defend the DoD networks. However, the task of developing the force in sufficient numbers resides primarily within the active component (AC) of each of the services (Army, Navy, Air Force, Marines).

The Army, which states that it "wants to be the service of choice for U.S. Cyber Command" has developed a "pretty good plan" for recruiting and developing cyber talent out to 2017, according to Lieutenant General Edward C. Cardon, current commander of U.S. Army Cyber/Second Army.[4] The plan calls for the development of 41 teams[5] that conduct operations in support of Army and joint commanders. However, the sheer volume of requirements levied on the Army to support the defense of the nation, combatant commanders and Army missions outweighs the number of highly qualified personnel and teams available today and into the foreseeable future. To recruit, develop and retain the right number of personnel with the appropriate skill sets, the Army must balance priorities with changing budgetary constraints, a narrow training pipeline and the constant struggle between working in the public and private sectors.

A potential solution for the Army is to develop a sustainable, agile and diverse force that expands the operational force by integrating the reserve component (RC) into the CMF to mitigate the stress on the active force and alleviate emerging force requirements in the future. Utilization of capabilities already resident in the RC effectively employs Army resources, uses the RC in roles for which they are well suited and mitigates the current shortfall of qualified cyber personnel. Further, using RC personnel taps into a force pool with skills that are hard to grow in the AC. It further relieves a portion of the current Army requirements by leveraging a mixture of talented people already in uniform with a combination of military and civilian training and experience. It further diminishes emerging stressors with an accessible, trained and ready surge capacity capable of steady-state operations, consequence management, crisis response and homeland defense.

Bringing Experience to the Fight

The RC has always been a vital member of the fight; the cyber domain should be no different. The Army has long acknowledged the need to utilize forces in a reserve status for operational and strategic depth, as well as to diversify the quality and experience of highly specialized career fields (such as IT). The Army RC is made up of the Army National Guard and the Army Reserve; each possesses unique skill sets and operates under distinct authorities in the performance of its duties. Binding these forces together is the Title 10 authority that enables the Secretary of the Army to "fulfill the current and future operational requirements of the unified and specified combatant commands" as well as to satisfy 12 missions outlined under the Secretary of the Army paragraph of that code (10 U.S. Code § 3013):

1. Recruiting;
2. Organizing;
3. Supplying;
4. Equipping (including research and development);
5. Training;
6. Servicing;
7. Mobilizing;
8. Demobilizing;
9. Administering (including the morale and welfare of personnel);
10. Maintaining;
11. The construction, outfitting and repair of military equipment; and
12. The construction, maintenance and repair of buildings, structures and utilities and the acquisition of real property and interests in real property necessary to carry out the responsibilities specified in this section.[6]

What has not been clearly defined to date is the role of RC forces in the cyber fight.

For years RC forces have been actively engaged in the operations and defense of the Army's networks. These teams, units and individuals have been actively employed to protect and defend essential elements and applications of the DoD Global Information Grid (GIG) by ensuring its availability, integrity, authenticity and confidentiality nonrepudiation. Army Reserve and National Guard members have deployed to provide operational support for a number of real-world signal missions, including cyber and computer support to the National Military Command Center (NMCC), Joint Web Risk Assessment Cell (JWRAC), Army Web Risk Assessment Cell (AWRAC), Joint Task Force–Global Network Operations (JTF-GNO), Joint Forces Component Command–Network Warfare (JFCC-NW), National Security Agency (NSA), Defense Enterprise Computing Center–Columbus (DECC-C), Defense Information Systems Agency (DISA) Northern Command (NORTHCOM) and DISA Continental United States (CONUS). In addition, there are currently two reserve component signal commands (theater)[7] taking the lead in Central Command (CENTCOM) and in Pacific Command (PACOM) along with a host of smaller teams and individuals supporting AC commands at various levels (tactical to strategic).

Currently staffed with many of the critical skills required to conduct cyberspace operations, many of these units could easily transition to CMF-capable teams. Leveraging the civilian-acquired skills while working at high-tech firms in private-sector careers, both the Army National Guard and the Army Reserve allow the Army and industry partners alike to enhance their knowledge of cyber issues. It further fulfills items in the strategic focus areas laid out in the DoD cyber workforce study, which states, "Success in cyberspace is dependent on having a knowledgeable and skilled workforce that can adapt to the dynamic environment and adjust resources to meet mission requirements."[8] This exchange of personnel, ideas and knowledge is already available and only requires integrating the RC into the overall Army Cyberspace strategy.

What the Army National Guard Brings

As General Alexander stated during his testimony to Congress in 2013, "Despite the unique characteristics of cyberspace, states still matter because they can affect much of the physical infrastructure within their borders."[9] This is where the Army National Guard and its relationship with home states becomes vital to the ability to secure cyberspace. The Guard's established civilian roles and skills—acquired by working full-time private-sector jobs in hometown communities—capture a centralized repository of experience currently in high demand in the AC. The skills honed by Guard members who live and work in their communities can easily transition from Title 32 duties to Title 10 service, bringing diverse knowledge and confidence already established between the private sector and the government, which is central to any cybersecurity policy.

The Army National Guard's geographic dispersion across the 50 states enables its traditional M-Day units[10]—including the Virginia Information Operations Support Command (VA IOSC) and its subordinate battalion the Virginia Data Processing Unit (VA DPU), two theater information operations groups, theater signal brigades and the 54 state-allocated computer network defense teams (CND-Ts)—to address numerous network defense issues. This group of skilled IT professionals with cybersecurity experience consists of more than 2,000 Soldiers who enhance the Army's cyberspace capabilities. A concept for 10 CPTs is already developed and prepared for implementation to support the CMF when approved by the Chief of Staff, Army. When approved and established, these CPTs within the Guard will be able to assist local communities, state leaders and the Army while bringing expertise in the identification and mitigation of potential cyberspace attacks.

Finally, the Army National Guard has invested in the development of their Professional Education Center (PEC) located at Camp Robinson in North Little Rock, Arkansas. The PEC is the national training center for the Army National Guard and has been a full-service training and conference facility since the early 1970s. This training facility, housed on a 75-acre campus with 25 buildings and a staff of more than 400 personnel, provides instruction to more than 20,000 members of the military force. Key to this training facility is the infrastructure, which includes closed training networks, laboratories, partner relationships and industry training. Through this investment the Army National Guard is able to train Citizen-Soldiers currently employed by leading-edge technology companies with critical skills and experience in cyberspace.

What the Army Reserve Brings

The Army Reserve brings a wealth of knowledge from its years of conducting computer network operations. Units within the Army Reserve have been a foundational element providing operational and strategic depth through numerous conflicts and at all levels of warfare. Since 2001 the Army has tasked the Army Reserve to acquire a new range of support in the information operations field, with a broad requirement to take advantage of the high-technology skills of Reservists already employed in the IT industry.[11] Utilizing the workforce that has already developed and matured working in IT, either for the military or private sector, the Army Reserve can easily integrate into cyber roles and functions.

As Lieutenant General Jeffrey W. Talley, Chief, Army Reserve/Commanding General, United States Army Reserve Command, stated in the 2013 Army Reserve Posture Statement to Congress, "For only 6 percent of the Army Budget, the Army Reserve provides almost 20 percent of the Total Force."[12] The power of the Army Reserve sits in its standing troop programmed units (TPUs) for cyberspace organizations including the Army Reserve Cyber Operations Group (formerly the Army Reserve Information Operations Command); two theater information operations groups, two theater signal brigades (support to U.S. Pacific Command and U.S. Central Command Regional Cyber Centers) and the Military Intelligence Reserve Command. This readily available force consists of more than 3,500 Soldiers either in transition to support cyberspace operations or awaiting a strategy to enhance the Army's cyberspace capabilities. The Army Reserve already has two units prepared to transition and integrate into the Cyber Mission Force when approved by the Chief of Staff, Army.

The Army Reserve Title 10 status also enhances the Army's ability to reach into the Army Reserve cyber units through a number of different duty statuses, including active duty for training (ADT), active duty for operational support (ADOS), mobilization and annual training (AT). This model works well for Army Reserve response to crisis or performance of short-duration missions to develop and validate cyber teams for the Army and joint training-readiness standards.

Finally, the Army Reserve has invested in building cyber team training infrastructure, which includes closed training networks, laboratories, partner relationships and industry training. The Army Reserve, working with Army Cyber Command (ARCYBER) and U.S. Cyber Command, has also been strengthening public partnerships with academia, industry and other government organizations. These include exchanges, Science, Technology, Engineering and Math (STEM) programs, expanded fellowships, inclusion in cyber research, experiments and exercises. The cost benefit of utilizing Citizen-Soldiers employed in leading-edge technology companies is an easy win for the U.S. Army.

Developing a Total Army Cyber Force

Defining the need for a Total Army Cyber Force. The development of any force in the U.S. military is driven by a requirement to fill a defined gap with qualified, trained and ready forces. The Army, in collaboration with USCYBERCOM, has developed a plan for an initial force to conduct operations in the next three to five years. Labeled the "Cyber Mission Force," USCYBERCOM's plan calls for the creation of three types of forces: "national mission forces" to protect computer systems that undergird electrical grids, power plants and other infrastructure deemed critical to national and economic security; "combat mission forces" to help commanders abroad plan and execute attacks or other offensive operations; and "cyber protection forces" to fortify the Defense Department's networks.[13] The Army, for its portion of the force, is contributing 41 teams[14] built from the AC that will support the three mission areas outlined above.

According to General Cardon, the challenge to building a Total Army Cyber Force is the uncertainty that comes hand-in-hand with the development in this field: "It changes so fast, it is probably not possible to predict what the size of the force needs to be several years out."[15]

Army Regulation 525-29 states, "While in an era of persistent conflict, the Army must continue to generate forces in a condition where the global demand for land forces exceeds the available supply."[16] The USCYBERCOM plan of action for trained and ready cyber forces far exceeds the current capacity of the Army AC. To meet both the current and the emerging requirements in cyberspace, the Army should use the RC as an operational force to fill this capability gap. The Office of the Secretary of Defense (OSD) already supports this concept, as stated in its unit cost and readiness report for active and reserve components for Fiscal Year (FY) 2013. As stated in this report, DoD must maintain a force large enough to deploy rapidly in sufficient numbers to seize and hold the initiative in support of U.S. objectives while ensuring that sufficient follow-on forces are available for sustained operations.[17]

To accomplish this goal, the Army must balance its cyber force with an increased focus on five key factors that play a role in the AC/RC-mix decisions:

- sourcing for continuous presence and surge demands;
- mission duration, predictability and frequency;
- responsiveness of the force based on complexity, urgency of task, unit integration, mission or role;
- retention and sustainment; and
- cost of manning and equipping for specific units/capabilities.[18]

As stated in the OSD report, the first three factors relate to the ability to accomplish the mission and are thus critically important. The next two items (retention and sustainment, cost), while important, are considered secondary factors in determining the right combination of AC and RC forces.[19] The obstacles facing the Army today are comparable to those of decades past, and the lack of a proficient workforce has been a major limitation. Former Secretary of Defense Robert Gates stated several years ago that DoD was "desperately short of people who have capabilities in [defensive and offensive cybersecurity war skills] in all the services." Since the ability to operate effectively in cyberspace continues to evolve, it is essential that the Army support continuing education, certification and development of a force that meets ongoing requirements; mitigates current gaps with the right mix of AC/RC cyber personnel; and builds a long-term strategy that expands the knowledge and skills of the Army's ability to confront the dynamic environment of cyberspace.

What the AC looks like. Starting in 2014 and over the next three years, USCYBERCOM will build and employ a CMF comprising more than 130 teams. These highly trained teams will be organized into three complementary forces:

- The National Mission Forces will employ 13 teams from across the services and will focus on securing U.S. private networks powering critical infrastructure such as transportation systems and other vital industries.[20] The National Mission Forces set of teams will be the early focus for resources to protect critical U.S. infrastructure prior to building and employing the two other types of teams.
- The Combat Mission Forces will comprise 27 teams that will enable "combatant commands in their planning process for offensive cyber capabilities."[21]

- The bulk of USCYBERCOM's effort—the Cyber Protection Force (CPF)—will help operate and defend the DoD information environment and will comprise more than 60 protection force teams that defend dot-mil networks, which are targeted millions of times per day.[22]

The Army, for its portion of the CMF, plans to support the USCYBERCOM requirement by building 41 of the 133 planned teams[23] across the three mission areas. For now, these units will be based out of Fort Meade, Maryland (home of USCYBERCOM) and Fort Gordon, Georgia (home of the Army's new Cyber Center of Excellence). Recruiting and training is ongoing and is scheduled across the next three years to meet the goal of being fully operational by FY 2016. The 41 teams will be aligned much like the USCYBERCOM teams (national, combatant command and service) with the bulk of the forces aligned with the CPF. The teams will work under the direction and control of ARCYBER/Second Army but would be organic to either the 7th Cyber Protection Brigade or the 780th Military Intelligence Brigade (Cyber).

How the RC fits. As General Keith Alexander, then commander of USCYBERCOM, stated before the Senate Armed Services Committee in March 2013, "We are building cyber mission teams now, with the majority supporting the combatant commands and the remainder going to USCYBERCOM to support national missions."[24] He went on to say that he would create CPTs; however, the majority of those teams would be supporting national and combatant commanders, with a small number left for the services to protect their own networks. The obvious gap comes in conducting cyberspace operations across the wide variety of Army networks. While the Army has allocated CPTs to protect its networks, the sheer volume of the requirement far exceeds the scheduled number of teams dedicated to the task.

This is where the RC cyber force can step into the breach and address critical needs that the Army is unable to fill now and in the future. Key to the integration and synchronization of the RC cyber force into the overall Army cyber strategy is building to the single standard established by USCYBERCOM. Using skills already obtained, RC units that are closely aligned with cyber (Computer Network Operations, Signal and Signals Intelligence) can transition quickly into the desired type of unit as directed by the Army. Based on analysis and the best suited mission types and roles as determined by ARCYBER, the RC teams would employ a baseline CMF (protection) team model along with a fourth team that would provide direct support intelligence analytic support to the Army.

This RC cyber protection force would primarily use the CPT as its baseline model and tailor the support of the CPT team based on the requirements levied by ARCYBER/Second Army. These teams would comprise sub-teams that would specialize in various functions as outlined by USCYBERCOM and would allow greater flexibility and capacity to the Army. Generally, the teams should consist of dedicated cyberspace operators, analysts, planners and leaders who would conduct operations to protect specified missions or national assets throughout cyberspace. They should have the capability to conduct information assurance evaluations and inspections and advanced analytics to conduct forensics, malware analysis, vulnerability assessment and mitigation, threat replication, intelligence analysis (cyber focused) and proactive and dynamic cyber defense with more advanced tools.

Potential mission areas for the RC teams could include:

- providing cyberspace inspections of critical infrastructure to enhance security with the ability to support finance, power, health, logistics, communications and other critical communities;

- assisting government and private-sector information technology professionals in the mediation/repair of major cyber vulnerabilities;
- increasing resilience of critical infrastructure, repairing and mitigating the damage caused by cyberspace attack and facilitating power recovery operations after man-made or natural disaster;
- providing technical support/advice to state, regional and local governments, including Title 32 cyberspace operations support capability to law enforcement activities; and
- providing a ready and available pool of cyberspace domain tactical and operational units to support combatant commands' theater strategy, either by mobilizing and deploying overseas into theater or by providing reach-back support from bases in CONUS.

The Army National Guard and the Army Reserve bring unique but symbiotic cyber capabilities to the Army that can easily be streamlined to enhance the Army CMF. Army RC strategy for training, readiness and employment of these forces should be managed under one umbrella strategy due to their similar capabilities and time-constrained availability. Further, if the Army establishes a single RC Training Readiness Authority Strategy for integration, mobilization and missioning in the CMF, fiscal risk can be significantly reduced and mitigated with great benefit to the Army.

Model of Employment

The Army has acknowledged "the critical contribution and integration of the Army's RC forces to [Army Force Generation, or ARFORGEN] as fundamental to meeting our nation's security requirements."[25] Following the current Army model of employment, RC cyber forces would use ARFORGEN as both a model and a process overlaid on the CMF requirements from USCYBERCOM. ARFORGEN is defined as the structured progression of unit readiness over time, resulting in recurring periods of availability of trained, ready and cohesive units.[26] The Army could draw on an RC talent pool with an amalgam of quantifiable skills, proficiencies and accomplishments that come from military and civilian life. Using CMF structure, these RC cyber units will prepare for operational deployment in support of combatant commanders and other Army requirements.[27]

How the RC cyber ARFORGEN would work. To secure a steady and predictable supply of trained and ready cohesive RC units for these categories of forces in a manner that is most cost-effective, the nation must commit resources to operationalize the Army's reserve component.[28] This applies equally to the newly-minted cyber force that is currently under development across DoD. These teams in turn will provide the Army and USCYBERCOM the operational depth and strategic agility necessary to protect critical national information systems, support combatant commanders abroad and defend the DoD networks in a sustainable manner.

To produce four tailored CPT teams (two Army National Guard, two Army Reserve) the Army would require 20 RC cyber teams. These teams would follow a 1-to-4 dwell time over a 12-month time frame,[29] with each of the CPTs arrayed across the force pools (reset, train/ready, available) in various states of preparation to conduct a full range of cyberspace operations. Army Cyber/Second Army, as the headquarters responsible for cyberspace, would collaborate with Army Forces Command (FORSCOM), the Army National Guard and U.S. Army Reserve Command (USARC) to develop a resourcing strategy for units to synchronize reset plans, resource shortfalls and provide predictability and visibility of readiness via the Unit Status Report (USR) as the unit progresses through reset.[30]

During the reset phase (year 1) the focus is on the individual personnel and begins to loosely align team leadership and regenerate team equipment. Personnel off-ramping from a deployment cycle or an active status are allowed liberal leave to reintegrate with their families; regeneration of team staff begins; and individual Soldier professional military education (PME) is assessed, scheduled and begun. Since most, if not all, of cybersecurity professionals are accredited by professional cyber organizations, individuals are encouraged to maximize a learning continuum that provides a variety of training environments, including traditional classroom training; virtual training; hands-on laboratories; and realistic, operational exercises. This extensive training makes the reset phase the critical foundational element to satisfy the different skill sets and knowledge levels required.

While all Soldiers require foundational knowledge to manage information that balances information assurance with security and privacy, leadership must master the sharing of knowledge, create understanding and ensure decisionmaking associated with mission command. Leaders must have the technical and tactical know-how to exercise strategic leadership and critical thinking in the development and use of cyberspace strategies, plans, policies, enabling technologies and procedures to support military commanders. During this phase, leaders will refresh technical skills while concurrently developing the ability to lead CMF teams in support of commanders' objectives. At the end of the reset, units are trained and resourced to begin collective training.

Following reset, teams **transition to the train/ready** phase (years 2, 3, 4). The focus is on reestablishing core skills required to conduct the dynamic mission in cyberspace through sub-team collective training and the progressive build-up of readiness to accomplish less complex missions. This culminates in the completion of a Maneuver Combat Training Center (MCTC) rotation or other cyber-related exercises such as Cyber Flag, Cyber Guard or Cyber Mission Readiness Exercise (MRX) validation exercise. During the train/ready (TR) stage of the ARFORGEN model, RC cyber forces would progress through three phases of train/ready (TR1, TR2 and TR3) with the third TR stage ending with the RC CPT ready for the available pool. Each of the TR stages would be completed over a 12-month cycle, allowing 36 months (three years) for the sub-team and subsequently the RC CPT organization to become fully trained and ready to accept missions from ARCYBER and/or USCYBERCOM. Each TR stage would focus on hitting aim points established by the Army in critical areas of preparation. These would include personnel (P), sustainment (S), readiness (R) and training (T)—like any other Army unit in the ARFORGEN model.

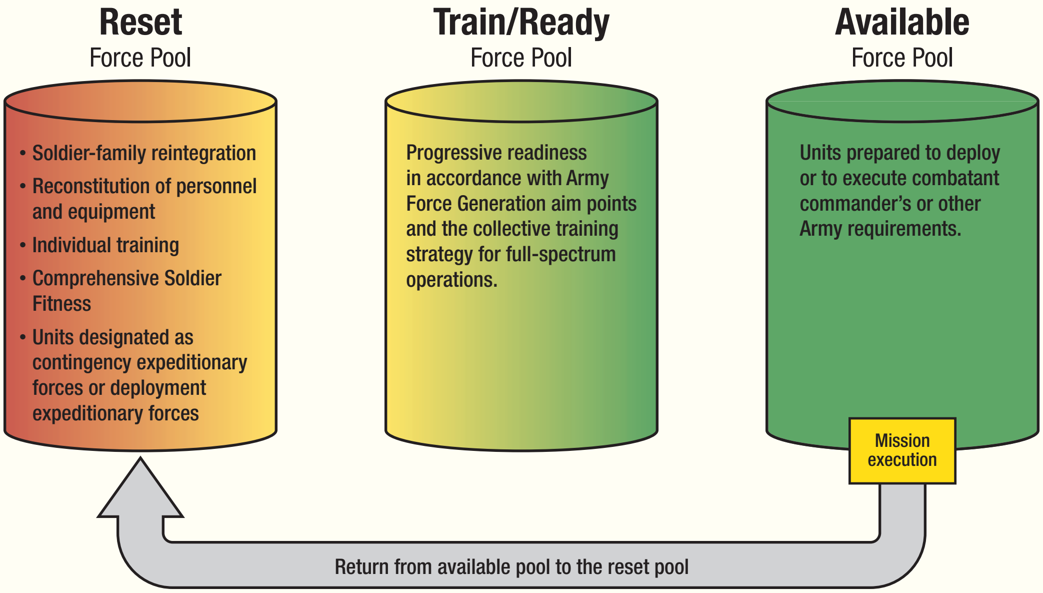
During TR1 (year 2) the sub-teams would focus on continuous organizational and individual learning needs, reinforced by relevant content that enables proficiency training, on-the-job training, exercises and expanded use of cyberspace ranges, all of which place emphasis on obtaining and maintaining qualifications. Teams would finish individual PME and begin collective training, reaching initial operating capacity (IOC) at the sub-team (squad) level. Sub-teams would be tracked as strategic depth and capable of surge capacity if required by the Army. Additionally, the sub-teams would use existing Army sub-team missions or exercises to train and prepare their sub-unit tasks and CPT missions. This might include left seat–right seat staff rides with their active duty counterparts.

During TR 2 (year 3) the sub-teams would continue organizational training, reinforced through exercises and cyberspace ranges, with emphasis on obtaining and maintaining sub-team qualifications. RC CPT leadership would begin exercising formal control of the teams with the goal of obtaining IOC for teams at the end of the cycle. Sub-teams would achieve full operating capacity (FOC) with all individual PME and sub-team validation and training being completed. The determination would be made if the RC CPT would fill a USCYBERCOM requirement and be slotted to obtain additional training to meet USCYBERCOM standards. Additionally, sub-teams would be available for missions from ARCYBER/Second Army and the RC CPT units would be tracked as strategic depth and capable of surge capacity as a full CPT if required by the Army.

During TR 3 (year 4) the RC CPTs would continue organizational training, reinforced through exercises and cyberspace ranges, with emphasis on obtaining and maintaining CPT qualifications at the Army or joint qualification level. CPT leadership would have formal control of the team and all sub-teams. CPT validation and training would be completed at the end of this cycle with the RC CPT and its sub-teams at FOC and available for missions from ARCYBER/Second Army. The team would be tracked as operational depth and capable of surge capacity as a full CPT if required by the Army.

The mission force or available force category (year 5) is the period when the RC CPTs are at their highest state of readiness and are either deployed or ready to deploy worldwide to conduct cyberspace operations. RC cyber forces (two Army National Guard, two Army Reserve) would conduct missions in support of USCYBERCOM or in support of ARCYBER/ Second Army. Their status would be considered "active" and they could be employed as contingency forces or surge forces depending on requirements from the Army and USCYBERCOM. The term "active" would mean the forces are on active duty or in an available status and could deploy within a short time frame. These RC CPTs would conduct a mobilization validation exercise with certification by ARCYBER or Second Army oversight based on established skills and training standards for individuals, leaders and teams. This model is similar to the way the Army already trains its combat forces for deployment to theater. The ARFORGEN

ARFORGEN Force Pools


Reset
Force Pool
• Soldier-family reintegration
• Reconstitution of personnel and equipment
• Individual training
• Comprehensive Soldier Fitness
• Units designated as contingency expeditionary forces or deployment expeditionary forces
Train/Ready
Force Pool
Progressive readiness in accordance with Army Force Generation aim points and the collective training strategy for full-spectrum operations.
Available
Force Pool
Units prepared to deploy or to execute combatant commander's or other Army requirements.
Mission execution
Return from available pool to the reset pool

model provides a predictable timeline for the Army and reduces the time required for highly compensated and time-constrained cyber reservists to one year of mobilization in five years. It also provides a model that assures the active force commander that forces presented will be qualified, trained and ready for deployment to the joint cyber standard required.

Conclusion

The Army should create a Total Army Cyber Force that builds CMF-like teams in the RC that are trained to the joint standard but capable of conducting a wide range of missions in support of Army and joint requirements. Building an operational cyberspace reserve would be cost effective, provide agile and adaptive leaders and integrate experienced network operators who use innovation and initiative to support Army and USCYBERCOM requirements.

By leveraging the mixture of talented RC personnel already in uniform and with a combination of military and civilian training and experience, the Army can mitigate the short-term stress on AC units. It further diminishes emerging stressors with an accessible, trained and ready surge capacity that represents more than 50,000 man-days of support annually without requiring mobilization.[31] These forces are capable of conducting steady-state operations, consequence management, crisis response and homeland defense for the Army and state entities as required. If adopted, this concept would bolster the Army's capability and increase the available number of CMF teams from 41 to 61 for the Army, at a fraction of the cost, and start providing RC CMF teams as early as FY 2015.

Endnotes

[1] Army Cyber Command/Second Army, Marine Forces Cyber Command, Air Forces Cyber/24th Air Force and U.S. Fleet Cyber Command/10th Fleet.

[2] Major Carrie Cox, "Commander of U.S. Cyber Command, Gen. Keith Alexander to speak on campus Feb. 13," Virginia Tech News, 31 January 2014, http://www.vtnews.vt.edu/articles/2014/01/013114-corps-genalexander.html.

[3] Ellen Nakashima, "Pentagon to boost cybersecurity force," *Washington Post*, 27 January 2013, http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity.

[4] Dan Verton, "Army grapples with future cyber-workforce issues," *fedscoop*, 24 October 2013, http://fedscoop.com/army-grappling-future-cyber-workforce-issues.

[5] Jared Serbu, "Army ponders proper shape, size of cyber workforce," *FedNewsRadio*, 28 October 2013, http://www.federalnewsradio.com/398/3492533/Army-ponders-proper-shape-size-of-cyber-workforce.

[6] U.S. Code, Title 10, Subtitle B, Part I, Chapter 303, § 3013, "Secretary of the Army," Cornell University Law School's Legal Information Institute, http://www.law.cornell.edu/uscode/text/10/3013.

[7] 335th Signal Command (Theater), U.S. Central Command; 311th Signal Command (Theater), U.S. Pacific Command.

[8] Department of Defense, *Department of Defense Cyberspace Workforce Strategy*, 4 December 2013, http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed(final).pdf.

[9] General Keith B. Alexander, "Statement of General Keith B. Alexander, Commander, U.S. Cyber Command, before the Senate Armed Services Committee," Statement for Record, 12 March 2013, http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf.

[10] M-Day means "Mobilization Day," which stands for a traditional Army National Guard Soldier who drills 48 Multiple Unit Training Assemblies and a 15-day Annual Training period a year as per statutory regulations.

[11] Travis Good, "Army Reserve Trains for Information Assurance," *Signal Online*, January 2004, http://www.afcea.org/content/?q=node/42.

[12] Lieutenant General Jeffrey W. Talley, Chief, Army Reserve/Commanding General, United States Army Reserve Command, and Command Sergeant Major James M. Lambert, Acting Command Sergeant Major, U.S. Army Reserve, *U.S. Army Reserve Posture Statement 2013*, http://issuu.com/warrior-citizen/docs/arps_2013_6-11-13.

[13] Jason Healey, "Cyber Command Expanding Five Fold," *Atlantic Council*, 29 January 2013, http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-command-expanding-five-fold.

[14] Serbu, "Army ponders proper shape, size of cyber workforce."

[15] Lieutenant General Edward C. Cardon, Commanding General, United States Army Cyber Command, quoted in Dan Verton, "Army grapples with future cyber-workforce issues," *fedscoop*, 24 October 2013, http://fedscoop.com/army-grappling-future-cyber-workforce-issues.

[16] Department of the Army, Army Regulation 525-29, *Military Operations: Army Force Generation*, 14 March 2011, http://www.forscom.army.mil/graphics/r525_29.pdf.

[17] Office of the Secretary of Defense, Unit Cost and Readiness for Active and Reserve Component of the Armed Forces, Report to Congress, 26 April 2013, http://www.ngaus.org/sites/default/files/pdf/OSD%20CAPE%20Reserves%20Costing%20Report.pdf, (draft) and 20 December 2013, http://www.ngaus.org/sites/default/files/CAPE%20FINAL%20ACRCMixReport.pdf (final).

[18] *Ibid*.

[19] *Ibid*.

[20] Aliya Sternstein, "Pentagon plans to deploy more than 100 cyber teams by late 2015," *Nextgov*, 19 March 2013, http://www.nextgov.com/defense/2013/03/pentagon-plans-deploy-more-100-cyber-teams-late-2015/61948.

[21] *Ibid*.

[22] *Ibid*.

[23] Chandler Harris, "U.S. Cyber Command Force Faces Growing Pains," *Clearancejobs.com*, 18 December 2013, http://news.clearancejobs.com/2013/12/18/u-s-cyber-command-force-faces-growing-pains.

[24] Alexander, "Statement . . . before the Senate Armed Services Committee," 12 March 2013.

[25] Department of the Army, *Army Posture Statement 2012*, Report to Congress, 17 February 2012, https://secureweb2.hqda.pentagon.mil/vdas_armypostureStatement/2012/addenda/addenda_g.aspx.

[26] General Charles C. Campbell, "ARFORGEN: Maturing the Model, Refining the Process," *ARMY*, June 2009, http://www.ausa.org/publications/armymagazine/archive/2009/6/Documents/Campbell_0609.pdf.

[27] *Army Posture Statement 2012*, https://secureweb2.hqda.pentagon.mil/vdas_armypostureStatement/2012/addenda/addenda_g.aspx.

[28] *Ibid*.

[29] A 12-month time frame equates to one year in a reset status, two years in a train/ready status and one year in an available status.

[30] *Army Posture Statement 2012*, https://secureweb2.hqda.pentagon.mil/vdas_armypostureStatement/2012/addenda/addenda_g.aspx.

[31] 24 weekend days—15 days Active Duty for Training per Soldier per year—each Theatre Information Operations Group (TIOG) has approximately 315 authorized billets.

Glossary

AC	Active Component
ADOS	Active Duty for Operational Support
ADT	Active Duty for Training
ARCYBER	Army Cyber Command
ARFORGEN	Army Force Generation
AT	Annual Training
AWRAC	Army Web Risk Assessment Cell
CENTCOM	Central Command
CND-Ts	Computer Network Defense Teams
CMF	Cyber Mission Force
CONUS	Continental United States
CPF	Cyber Protection Force
CPT	Cyber Protection Team
DECC-C	Defense Enterprise Computing Center–Columbus
DISA	Defense Information Systems Agency
DoD	Department of Defense
FOC	Full Operating Capacity
FORSCOM	Army Forces Command
GIG	Global Information Grid
IOC	Initial Operating Capacity
IT	Information Technology
JFCC-NW	Joint Forces Component Command–Network Warfare
JTF-GNO	Joint Task Force–Global Network Operations
JWRAC	Joint Web Risk Assessment Cell
MCTC	Maneuver Combat Training Center
M-Day	Mobilization Day
MRX	Mission Readiness Exercise
NMCC	National Military Command Center
NORTHCOM	Northern Command
NSA	National Security Agency
PACOM	Pacific Command
PEC	Professional Education Center
PME	Professional Military Education
RC	Reserve Component
STEM	Science, Technology, Engineering and Math
TPUs	Troop Programmed Units
TR	Train/Ready
USARC	U.S. Army Reserve Command
USCYBERCOM	U.S. Cyber Command
USR	Unit Status Report
VA DPU	Virginia Data Processing Unit
VA IOSC	Virginia Information Operations Support Command