Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA)

APPENDIX E
FSA Report
V0.9

23 December 2010

Combined Arms Center - Capability Development Integration Directorate
(CAC-CDID), 806 Harrison Drive, Bldg 470
Fort Leavenworth, KS 66027-2326

DEPARTMENT OF THE ARMY

COMBINED ARMS CENTER,
CONCEPT DEVELOPMENT DIVISION
CAPABILITY DEVELOPMENT INTEGRATION DIRECTORATE (CAC-CDID)
806 HARRISON DRIVE
FT LEAVENWORTH, KANSAS 66027

OVERALL CLASSIFICATION OF THIS REPORT:

UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO)

Cyber / Electromagnetic (C/EM) Contest
Capabilities Based Assessment
Prepared by the Concept Development Division,
Capability Development Integration Directorate (CDID), Combined Arms Center
USACAC, Ft Leavenworth KS 66027

Table of Contents

Table of Figures

Table of Tables

Functional Solution Analysis (FSA) Report for the Cyber / Electromagnetic (C/EM) Contest Capabilities Based Assessment (CBA)

Section I - Introduction

1-1 Purpose

(U//FOUO) This report documents the Functional Solution Analysis (FSA) portion of Cyber/Electromagnetic (C/EM) Contest Capabilities Based Assessment (CBA). The C/EM CBA conducted a review of how Army forces operate in and through both the cyberspace domain and the electromagnetic spectrum as a holistic and integrated part of full spectrum operations (FSO), in order to identify outcomes-based, integration-focused, and resource-informed solutions which will enable the U.S. Army to prevail in the cyber-electromagnetic contest. The solutions considered include potential changes to doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF).

1-2 Organization of the Document

(U//FOUO) This document is organized into an Introduction, Solutions for each of the DOTMLPF, and the Recommended Solution Approaches (RSA) Worksheet (Appendix A). The Introduction section provides the purpose, scope, and methodology for the FSA. Section 3, Solutions, provides detailed individual potential solutions considered to mitigate the gaps as determined from the FNA and identify residual gaps, if any, after the solutions are considered.

1-3 Scope

(U//FOUO) The FSA identified DOTLMPF solutions for capability gaps and needs across all Army echelons (Joint/Combatant Command (COCOM) down to Company level).

(U//FOUO) The FSA examined solutions for the 2016-2028 timeframe, although many of these solutions could be (and should be) implemented in the near term.

(U//FOUO) Although the FNA prioritized gaps by likelihood of occurrence and operational impact of occurrence, the FSA identified and assessed solutions for each FNA gap or need. No gap was left behind.

(U//FOUO) The FSA considered only Army or Joint service Programs of Record (POR) as programmed capabilities. A POR system was assumed to continue to be funded and fielded as scheduled.

(U//FOUO) Because of constraints on time and the limited availability of costing information, the study team performed an initial assessment of the affordability of each solution based on available information and expertise. Therefore, some solutions do not have detailed cost benefit analysis.

1-4 Methodology

Study Process

(U//FOUO) Following the JCIDS methodology, the C/EM Contest CBA was conducted in four Phases as depicted in Figure 1 below.

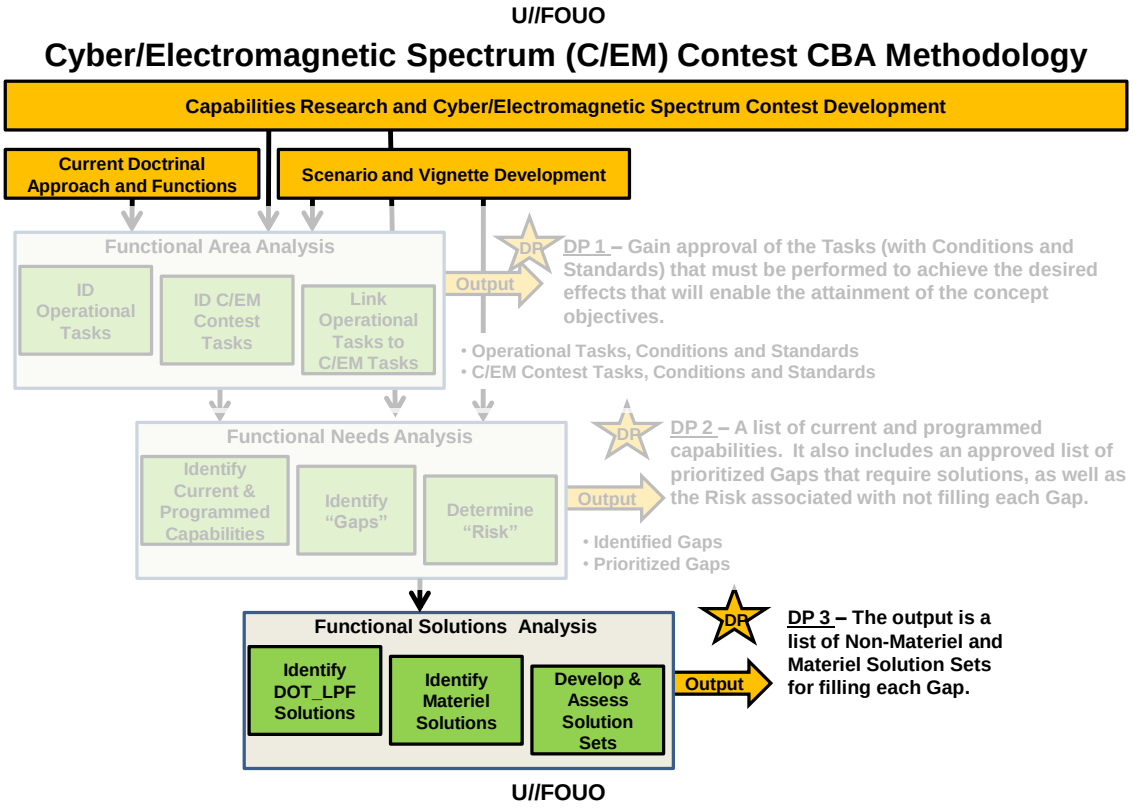
1. (U//FOUO) Beginning in January 2010, Phase I involved an extensive literature search, concurrent with the building of both the study plan and ICDT study team. While there were over 200 source references for the C/EM Contest, the Primary References listed earlier provided the basis for developing the CBA along with the applicable studies listed. Throughout the analysis, the study team continually used these references and supporting documentation to ensure analytic rigor was supported and defined.

2. (U//FOUO) Phase II was a Functional Area Analysis (FAA) that identified Required Capabilities (RCs) and then further developed the tasks, conditions, and standards (T/C/S) necessary to support the identified RCs. In March 2010, an executive level ARCIC Cyber Seminar was conducted to review the required capabilities that had been developed and solidified in TRADOC Pam 525-7-8 Cyberspace Operation Concept Capabilities Plan 2016-2028. Required capabilities were analyzed for redundancies, context and holistic inclusion of the C/EM Contest. This improved list of RCs was then staffed to the Army C/EM study team and became the baseline for follow on CBA workshops. In March 2010, the C/EM CBA FAA Workshop produced a refined list of tasks/conditions/standards based upon these RCs, approved concepts and requirements and ensure these were linked to the Army Universal Task List (AUTL) and the Universal Joint Task List (UJTL).

3. (U//FOUO) Phase III was the Functional Needs Assessment (FNA) and began in late April, 2010. The FNA assessed the ability of current and programmed capabilities to accomplish the RCs and tasks identified during the FAA. From the JCIDS standards, the FNA considered only Army Programs of Record (POR) as a programmed capability which includes systems fielded as part of an approved Operational Needs Statement and assumed that these programmed capabilities would meet their objective requirements by 2028. FNA Workshop #1, conducted in May 2010, looked at the T/C/S, the Army's current capabilities, and developed an initial draft of capability gaps. In June 2010, FNA Workshop #2, conducted a more in depth look at the specifics of each gap to ensure the gap standards were met. If a recommended solution did not meet the established requirements and

standards, analysis was conducted to bring the gap to the standard or those recommended solutions were removed from the study. Many of these "good idea" solutions have aspects that could support future analysis but, due to their immature nature, could not be included at the time of this study.

4. (U//FOUO) Phase IV was the Functional Solution Assessment (FSA). The FSA developed and assessed potential doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) approaches to solving capability gaps identified in the FNA.



(U//FOUO) Figure 1: Cyber/Electromagnetic Contest CBA

(U//FOUO) The FSA is normally composed of three sub steps, the DOTLMPF Analysis, the Ideas for Materiel Approaches (IMA); and the Analysis of Materiel Approaches (AMA). Because of the nature of this particular C/EM CBA, the analysis team focused on the first sub-step.

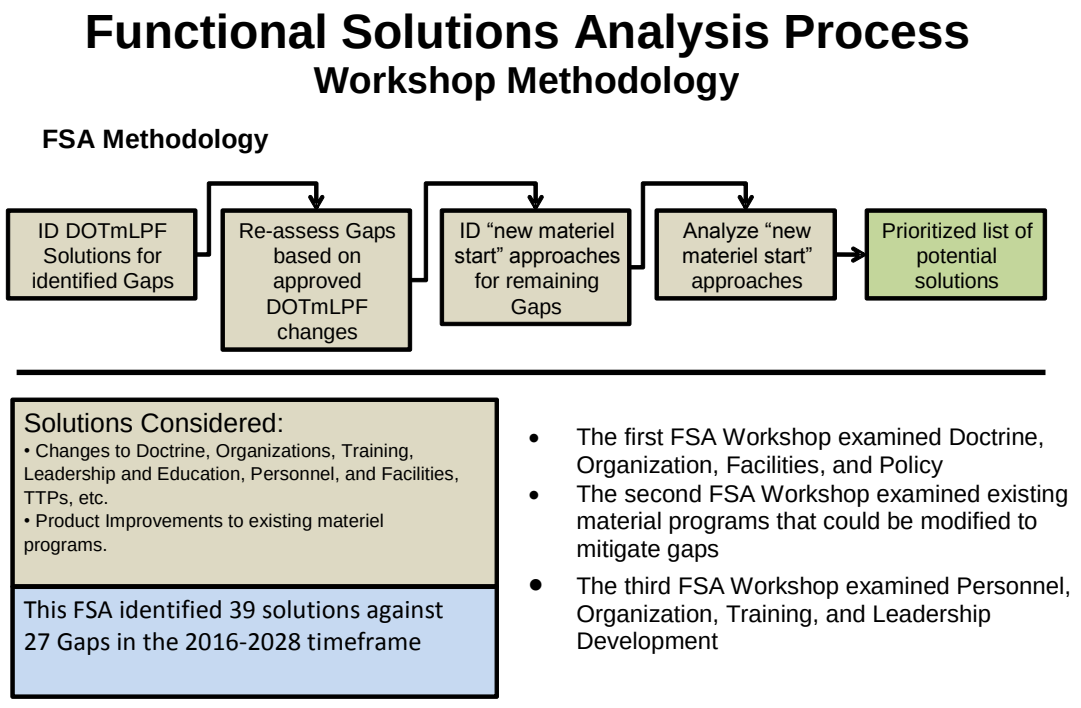
(U//FOUO) DOTLmPF Analysis. The first sub-step in the FSA was to determine whether a non-material approach could fill the capability gaps identified in the FNA. Non-materiel approaches include changes in DOTLPF, improvements or modifications to existing materiel systems (small "m" in DOTLmPF), or acceleration of existing developmental programs. Solutions are identified and considered in the following order of priority:

- (U//FOUO) Changes to doctrine, organizations, training, leader development, personnel, facilities, TTPs, etc.
- (U//FOUO) Product improvements to existing materiel programs
- (U//FOUO) Joint, Interagency or Foreign materiel approaches

(U//FOUO) If the analysis sponsor determines that the capability can be partially or completely addressed by a purely DOTLPF approach, the sponsor will coordinate with the appropriate Department of Defense (DoD) component to take action through the process outlined in Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3180.01, "Joint Requirements Oversight Council (JROC) Programmatic Processes for Joint Experimentation and Joint Resource Change Recommendations". If the sponsor determines that DOTLmPF changes (to include product improvement or modification) are inadequate and a materiel approach is required, the FSA process continues to sub-step 2. Some capability proposals involve combinations of DOTLmPF changes and materiel changes. The combinations continue through the FSA process at sub-step 2.

Specific FSA Methodology

(U//FOUO) As depicted in Figure 2, the study team gathered Army and Joint Service subject matter experts (SME) and held 3 FSA workshops to identify a wide range of DOTLmPF solutions that could either completely or partially mitigate the capability gaps identified in the FNA.



(U//FOUO) Figure 2: Functional Solution Analysis Process

(U//FOUO) FSA Workshop #1 kicked off in August with FSA Workshop #2 and #3 conducted in September 2010. The objective of FSA Workshop #1 was to develop viable initial solutions to mitigate C/EM capability gaps for echelons company through ASCC and the GENFOR. FSA Workshop #1 specifically developed solutions for Doctrine, Organization, materiel, Facilities and Policy. FSA Workshop #2 developed a viable Materiel solution strategy to mitigate C/EM capability gaps. The workshop made potential Materiel solution recommendations in terms of modifying existing programs, and if necessary, recommended new programs. FSA Workshop #3 developed an initial solution strategy to mitigate the C/EM capability gaps for Personnel, Training, and Leader Development and Education. The workshop specified expertise and skill requirements by echelon (company through ASCC).

The SMEs then proceeded to review each gap and presented potential doctrine, organization, training, leadership and education, personnel, or facilities solutions. They also generated a variety of material solutions that involved accelerating programs already underway, product-improving current systems, or adapting programmed platforms or payloads to mitigate a gap.

(U//FOUO) The SMEs were asked to assess each solution with respect to technical risk, supportability, affordability, operational risk, functional area impact, cross-function impact, or impact on other DOTLmPF actions.

(U//FOUO) After reviewing and categorizing the inputs from the workshop, the study team selected promising potential solutions and solutions sets. The resulting solution sheets are listed in Section 3 of this document. The end result of this FSA was the identification and assessment of solutions and solution sets to the capability gaps identified in the FNA.

(U//FOUO) Consideration was given to solution feasibility, affordability and DOTMLPF implications. The results were a listing of DOTMLPF solutions that were strategically responsive and deliver approaches when and where they're needed, feasible with respect to policy, sustainment, personnel limitations and technological risk, and finally realizable. The resulting solutions can be prioritized into adapting the Network Modernization Strategy, adapting the E/W Element to become C/EM, adapting the 29-series personnel to integrate and synchronize C/EM, and incorporating C/EM into doctrine, training, leader development, and policies.

(U//FOUO) The study team recognized that the Army currently has constrained resources and a no growth policy. Recommended ideas that required large expenditures, growing personnel numbers, or new organizations were examined but not included in the final report. Solutions that could utilize current Army capacity and capabilities were emphasized. Solution sets that have low implementation costs, could satisfy many gaps, and satisfied the highest priority gaps are considered the highest priority due cost effectiveness.

(U//FOUO) As a final step, the study team provided the draft C/EM CBA solution set as input to the December 2010 Unified Quest Cyber/Electromagnetic Contest Seminar. At this seminar, subject matter experts from industry, academia, and the military came together to evaluate a number of important issues under the rubric of the C/EM Contest. The Operations Panel subject matter experts worked diligently for two and a half days to refine and 'operationalize' the solutions to the C/EM Capabilities-based Assessment, with a special emphasis on doctrinal, organizational, acquisition, and policy issues. CBA recommendations were refined based on the insights from this seminar.

SECTION II -Solutions

2-1 Doctrine

Introduction

(U//FOUO) The C/EM Contest crosses all echelons and formations, recognizes that combined arms operations spans both the cyberspace domain and the electromagnetic spectrum (EMS), and that cyber and the EMS must be thought of as maneuver space during FSO. This study has determined that the C/EM Contest impacts all personnel. Whether a Soldier, Civilian or Contractor is in garrison or deployed their daily operations are enhanced by cyberspace and the EMS. This relationship requires that an understanding of the C/EM Contest, and how it supports FSO, must become an institutional part of the Army. The Cyberspace domain and the EMS are inherent aspects of FSO and both mediums will be congested and contested. Commanders and staffs must recognize these principles and act accordingly. C/EM must be accounted for in combined arms maneuver (CAM) and wide area security (WAS). For those personnel who specifically operate daily in the C/EM environment, doctrinal support for how C/EM is integrated and holistically supports FSO becomes more critical. A framework is required that unites the tactical, operational and strategic levels of warfare and is incorporated throughout the Army doctrinal hierarchy.

FSA Methodology for Developing Doctrine Solutions

(U//FOUO) The FNA identified 21 gaps as having Doctrine aspects. During the first FSA Workshop, doctrine was examined by 45 subject matter experts (SME). The SMEs broke into 3 working groups to collaborate about which pieces of doctrine needed updating to mitigate C/EM gaps. The groups considered the entire hierarchy of doctrine across all echelons.

FNA Gaps with Doctrine Aspects

C/EM Integrating Entity (Gap 02)
Access (Gap 04)
Legal Advisement for C/EM (Gap 06)
Establish, Operate, and Manage Enterprise Network (Gap 11)
Transition Network C2 (Gap 15)
Integrate CyNetOps with Mission Partners (Gap 19)
Network Defense in Depth (Gap 20)
Access Critical Network Info, Services, & Applications (Gap 24)
Non-Attributed Network (Gap 26)
Dynamic Cyber Defense (Gap 28)
Cyber Attack (Gap 32)
Threat Hardware & Software Analysis (Gap 33)
Cyber Vulnerability Assess & Operational Testing (Gap 36)

EA Asset Deconfliction (Gap 37)
C/EM Situational Awareness, COP (Gap 40)
Conduct Electronic Attack (Gap 45)
C/EM Modeling and Simulation (Gap 46)
Detect Jamming (Gap 50)
Spectrum Impact Analysis (Gap 52)
Spectrum Use Prioritization (Gap 54)
Defend/Protect Individuals and Platforms (Gap 57)

Fundamental Principles and Common Ideas for Army and Joint Doctrine.

The Unified Quest Seminar Operations Panel developed fundamental principles and common ideas that would properly focus the Army on the C/EM challenges and opportunities in the years ahead. The panel also developed ideas for doctrine specific to echelons, from BCT to Theater Army, and considerations for the emerging concepts of combined arms operations and wide area security. The Panel defined nine fundamental principles, changes in certain doctrinal terms, and other doctrinal nuances that should be commonly expressed as part of both Army and Joint doctrine (these follow below). These recommendations are a fundamental aspect of the five doctrinal solutions proposed by this CBA.

Principle #1: The cyberspace domain and the electromagnetic spectrum are inherent aspects of the operational environment, and the C/EM contest is inherent to full spectrum operations. These mediums will be simultaneously congested and contested. Commanders and staff must recognize the opportunities/vulnerabilities and act accordingly. Commanders and their units face a 'five domain and spectrum warfight.'

Principle #2: Commanders must consider cyberspace and the EMS as part of their overall operation. This means that commanders must visualize and describe desired C/EM conditions as part of their overall operation. This includes an appreciation that mediums can be 'maneuver space' – areas where positional advantage is possible. They must likewise consider C/EM activities to be part of an expanded notion of combined arms.

Principle #3: Units simultaneously occupy and act in five domains (air, cyber, land, sea, space) while leveraging the electromagnetic spectrum. Actions in and through any of these mediums can impact the others. Moreover, commanders must combine physical actions, inform &influence activities, and C/EM activities to accomplish desired objectives.

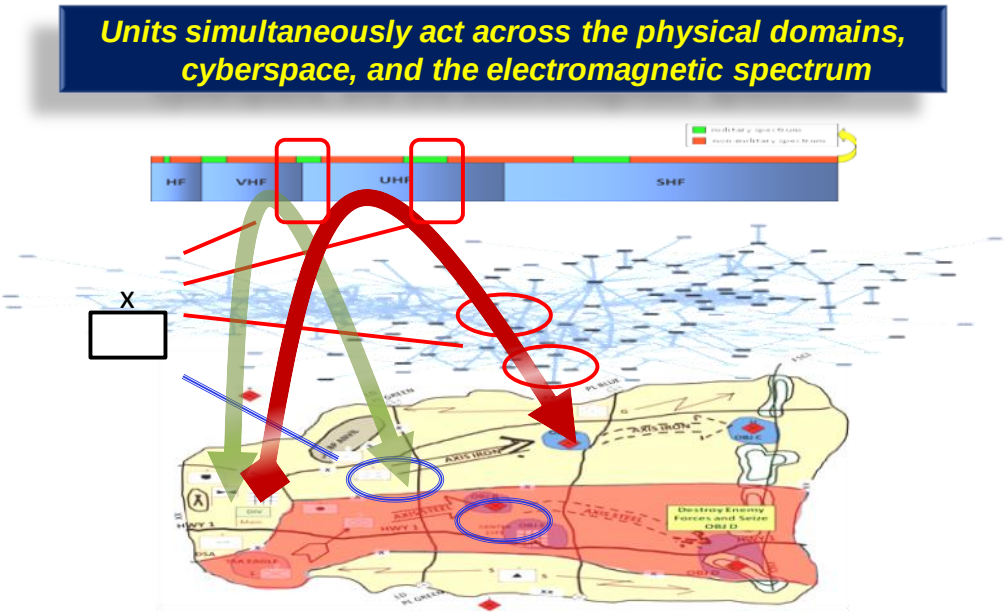


Figure 3: Unit Action Across Domains and Spectrum

Principle #4: Commanders create effects in the physical domains, cyberspace, and the spectrum through physical/kinetic, cyber, and electronic means.

Principle #5: The future operational environment will be contested on many levels. The U.S. Army's Capstone Concept recognizes the importance of cyberspace and the EMS to human societies in general and specifically to military operations. TRADOC's Operational Environment assessment foresees threats that are "hybrid, innovative, adaptive, globally connected, full spectrum and networked, embedded in the clutter of local populations and possess a wide range of old, adapted and advanced technologies."[1] They are prepared to maneuver against us in cyberspace and the EMS, in combination with both conventional and asymmetric means.

Human society is making ever increasing use of cyber and the EMS for communication and interaction. Increased use of social networking is blurring the lines between military and political competition. On a daily basis, the competition of ideas rages across the Internet, between state and non-state actors, on sites such as Facebook, Twitter, and YouTube. Since cyberspace is a virtual domain, it only communicates representations of reality. This allows some degree of the control of the 'lens' by which people see reality. Therefore cyberspace and the spectrum are powerful vehicles for shaping attitudes and perceptions, either for influence or deception.

[1] Future adversaries (state and non-state actors) will hide among populations, in the congested EMS and across the complex web of the internet in order to further their objectives. See the TRADOC assessment, ***Operational Environment2009-2025,*** August 2009, pages 8-9.

Principle #6: Cyberspace and the spectrum are 'commons' which defy geographic boundaries and echelon-driven restrictions. In many regards cyberspace and the EMS defy geographic boundaries, which means units can impact outside of their area of operations, and can be impacted by actors outside their area of operations. This principle argues for redefinition of several of our current doctrinal terms which are currently geographically defined. It also requires that staffs be capable of horizontal and vertical integration of assigned capabilities, supporting capabilities, and parallel operations (by external actors) within the unit's area of operations.

Principle #7: C/EM activities as inherently joint. Given the 'commons' principle above, C/EM activities must be understood as inherently joint activities. Individual units will rarely act independently and instead units must account for, integrate, and synchronize Joint capabilities within their operations as well as other contributing elements and capabilities.[2]

Principle #8: The essential tasks of the C/EM Contest. The five tasks that constitute the C/EM contest need to be clearly established in doctrine. They are:

- Establish a network that enables effective mission command, then operate and defend it
- Build and maintain C/EM situation awareness
- Attack & exploit enemy systems
- Defend & protect individuals and platforms
- Integration (holistic blending of organic and supporting capabilities to achieve desired conditions in cyberspace and the spectrum, C/EM capabilities fully integrated into the overall operation)

Principle #9: Always prepare for degraded conditions that occur in cyberspace and/or the EMS. Our commanders must train their units to strive to gain C/EM advantages, but at the same time must prepare their units for those moments where the environment will preclude favorable C/EM conditions, and/or those times where highly adaptive adversaries will gain C/EM advantages.

Recommended Changes to Doctrinal Terms.

The operational panel frequently discussed areas where existing doctrinal terms were either insufficient, or nonexistent. In order to fully internalize the C/EM contest as part of FSO, it is vital to have a common lexicon for Soldiers, commanders and mission partners. To that end, the panel made an effort to develop improved terms which will enable a foundation for the understanding of the C/EM contest. Some of the modifications include incorporating C/EM concepts into existing language. The panel identified three categories of terms.

[2] US Army Intelligence Center of Excellence, "Fixing Cyber: An Optimum Future for Army Electromagnetic/Cyber Operations."

The first category includes existing terms fully applicable to fighting across the physical and cyber domains, and the EMS. They include 'freedom of action' and 'positional advantage'.

The second category includes terms which the panel modified to address the inherent nature of cyberspace and the spectrum to the operational environment and full spectrum operations. These include:

- **Area of influence**, "A geographical area ***which may include portions of cyberspace and the EMS*** wherein a commander is directly capable of influencing operations by maneuver, ***and other*** systems normally under the commander's command or control;"
- **Area of interest**, "That area of concern to the commander ***(whether physical, cyber, or the EMS)***, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission."
- **Area of Operations,** "An operational area defined by the joint force commander for land and naval forces *which may include portions of cyberspace and the EMS*."
- **Avenue of Approach,** "A route, through air, cyberspace, ground, and/or the EMS, of an attacking force of a given size leading to its objective or to key terrain in its path.."
- **Key terrain**, "Any physical locality/area, ***or portion of cyberspace and/or the EMS***, where the seizure or retention of which affords a marked advantage to either combatant."

The third category includes other terms which require expansion to address the C/EM contest but the panel lacked time to develop definitions. These terms include combined arms, Intelligence Preparation of the Battlefield, maneuver, reconnaissance, situational awareness and situational understanding.

Doctrinal Nuances

The Operations Panel identified a series of considerations specific to certain echelons, and to the emerging concepts of combined arms maneuver and wide area security.

Nuances for BCTs: [FM 3-90.6]. In the near term, BCT commanders must realize that they will largely rely on higher echelon capabilities to set the C/EM conditions they desire. Pre-approved and tailored mission support packages will serve to accommodate commander's future mission needs. BCT C/EM capabilities, whether organic or tailored support packages, will need higher echelon support to enable BCT planning, database access and advanced analytics.[3] BCTs should also expect to be assigned missions that support the larger C/EM fight, such as site exploitation, gaining

[3] US Army Intelligence Center of Excellence , "Fixing Cyber: An Optimum Future for Army Electromagnetic/Cyber Operations." p.7

close access to adversary networks, or executing kinetic/physical actions that generate C/EM effects.

Nuances for Divisions and Corps: [FM 3-92]. At the corps and division level, the emphasis is on setting conditions for BCTs. It is important to build an appropriate mix of assigned and supporting assets to properly accomplish the five C/EM tasks based on mission priority and asset availability. Since corps/division bridge the operational and tactical levels of war, many of the of the C/EM activities will reflect a campaign perspective vice individual engagements.

Nuances for Army Service Component Commands (ASCC): [FM 3-93]. The ASCC is the Army's regional or geographic component to the combatant commander (COCOM). The ASCC is where the full national/joint/service "whole of government" approach comes together. One of its roles is setting Joint theater conditions over time, which in the future will include setting C/EM conditions. The ASCC will need to partner with all appropriate JIIM partners to build necessary C/EM situation awareness, and set the necessary conditions for future operations. The ASCC is critical for building the right planning teams, and conducting the appropriate planning for C/EM considerations within contingency planning. The ASCC gains and maintains C/EM advantage by having knowledge of adversaries in the COCOM AOR through their regionally focused MI Brigade; existing C/EM infrastructure, and possessing some C/EM expeditionary capabilities. Those capabilities are complemented by the ability to "reach" back to COCOM and national-level assets.

Specifically from a C/EM perspective, the ASCC is critical in the building of 'standing' C/EM situation awareness. ASCC contingency planning must work C/EM requirements into joint planning groups. It would be appropriate to assumes that any coalition/host nation networks are already compromised. Planning needs to address a fully congested/contested C/EM environment and plan accordingly. The impacts in the physical domains must be understood as C/EM conditions contest change (e.g. changes in logistic support caused by lack of network connectivity). When given a JTF mission, the ASCC must request the right additional augmentation to address the full joint C/EM contest.

Combined Arms Maneuver / Wide Area Security Nuances. In Combined Arms Maneuver there is the need for responsiveness and agility which increases the premium on agility with regards to changing battlefield conditions and flexibility in employing assets. The dispersion and long duration of Wide Area Security (WAS) missions increases the decentralization of a myriad of assets to lower echelons. Moreover, WAS increases the need for integration between BCTs/ISR and networks as decentralizing more assets to BCTs which increases their network requirements. This dispersion and increased density of assigned assets, dramatically increases the need for favorable C/EM conditions. This may exceed the organic capacity of a BCT, meaning that additional C/EM capabilities will have to be assigned or made available to the BCT.

Identified Potential Solutions

D01 – Army Capstone Doctrine – Modify FM 3-0 Operations

Description (U//FOUO) FM 3-0 will soon be completely revised. This capstone doctrine will assist the Army to internalize the C/EM Contest through the warfighting functions: Movement and Maneuver, Intelligence, Fires, Sustainment, Mission Command (Command and Control), and Protection.

Rationale (U//FOUO) Upon the next revision of the FM 3-0, expand the focus on the MC and C/EM relationship and include a more thorough understanding of how C/EM activities support all aspects of FSO. Expand Chapter 6 to more holistically include the integration and synchronization of cyber/electromagnetic activities into the commanders' operation by including the doctrinal principles and common terms identified by the UQ C/EM Contest Seminar.

D02 – Army Warfighting Functional Doctrinal Publications – Modify FM 2-0 Intelligence, FM 4-0 Sustainment, FM 6-0 Mission Command and Control, FM 3-09 Fire Support, FM 3-30 Protection, and FM 6-02 Signal Operations

Description (U//FOUO) Revise these FMs to more holistically include cyber/electromagnetic activities and the principles, terms, and nuances of C/EM operations to each of the WfF doctrinal publications.

Rationale (U//FOUO) The Warfighting Functional doctrinal publications require the inclusion of cyber/electromagnetic activities. This is due to the very nature of the C/EM Contest, which is the dimension of full-spectrum operations which aims to gain advantage, maintain that advantage, and place adversaries at a disadvantage in the increasingly contested and congested cyberspace domain and electromagnetic spectrum and is an integral part of full spectrum operations (FSO includes all WfFs).

D03 – Elements of Army Combat Power Doctrinal Publications – Rewrite FM 3-13 as the Inform and Influence Activities FM

Description (U//FOUO) The Warfighting Functions are supported by Information which provides the commander the ability to understand and visualize the operational environment. Due to its importance in the C/EM Contest, FM 3-13 is a key C/EM doctrinal manual.

Rationale (U//FOUO) FM 3-13 is undergoing an Army service review and will be revised upon approval of FM 3-0 Change 1. Revise this FM to more closely align with the understanding of Inform and Influence Activities (IIA) and C/EM Operations.

D04 – Rewrite FM 3-36 as the Cyber/Electromagnetic Activities FM

Description (U//FOUO) Write new Cyber/EM doctrine, which supports and integrates the competencies of Electronic Warfare (EW), Electromagnetic Spectrum Operations (EMSO) and Cyber as they relate to integrating and enabling C/EM activities, effects and capabilities. Ensure each of the subordinate FMs (EW, EMSO and Cyber) are revised to include a section describing how their capabilities are integrated in support of the C/EM activities and how/who will participate in the C/EM Working Group to coordinate C/EM effects. Write subordinate doctrine: FM 3-36.1 Army Electronic Warfare Operations (move and modify from current FM 3-36); FM 3-36.2 Cyberspace Operations; FM 3-36.3 Electromagnetic Spectrum Operations.

Rationale (U//FOUO) Currently, FM 3-36 EW provides Army doctrine for electronic warfare (EW) planning, preparation, execution, and assessment in support of full spectrum operations. While it covers the EW aspect of the C/EM contest, inclusion of the cyber and EMSO aspects must be accomplished to provide the ability to integrate and understand the full capability sets needed for the C/EM Contest.

D05 – Other & Supporting Doctrine Solutions

Description (U//FOUO) Adding C/EM considerations to the following doctrine will address the remainder of the gaps.

Rationale (U//FOUO) Most of these publications currently do not address C/EM at all or use antiquated verbiage to describe the contest.

Full Spectrum Operations Doctrine

- (U//FOUO) FM 3-90 Tactics: Include C/EM activities and C/EM activities integration in Chapters 1, 2, 3, 5, and 6

Reference Doctrine

- (U//FOUO) FM 5-0 Army Planning and Orders Production: Integrate C/EM operations into COP in Appendix F; increase information sharing between NetOps and Intel communities in Appendix C; create requirement for orders and annexes in Appendix G
- (U//FOUO) FM 7-15 AUTL: Include ARCYBER and C/EM tasks in Chapters 2, 3, and 5
- (U//FOUO) FM 1-02 Operational Terms and Graphics: Update and/or develop cyber Operational Terms and Graphics for incorporation in Chapter 1, 2, 5, and 9

Supporting Doctrine

- (U//FOUO) FM 1-01 Generating Force Support for Operations: Update definitions of FSO in Chapter 2; Include ARCYBER in Chapter 4

- (U//FOUO) FM 1-04 Legal Support to the Operational Army: Integrate support requirements for C/EM activities and investigations to include related coordination issues in Chapter 2, 4, and 5
- (U//FOUO) FM 2-19.4 BCT Intelligence Operations: Increase information sharing between the NetOps and Intelligence communities in Chapters 2 and 3
- (U//FOUO) FM 3-09.31 TTP for Fire Support for the Combined Arms Commander: Discuss the C/EM targeting process (including BDA) and incorporate into the COP in Chapters 1 and 4
- (U//FOUO) FM 3-19.13 Law Enforcement Investigations: Update Chapter 11 Computer Crimes Investigations.
  (U//FOUO) FM 3-14 Space Support: Increase information sharing between NetOps, Intelligence and Space communities
- (U//FOUO) FM 3-36 Electronic Warfare: Integrate C/EM targeting, operations and assessments in Chapter 4. Develop procedures for inclusion into the COP in Chapter 5.
- (U//FOUO) FM 3-90.6 BCT: Include C/EM activities integration; BCT commanders must realize it is unlikely they will have a full suite of C/EM capabilities at their command, but rather pre-approved and tailored mission support packages. Pre-approved and tailored mission support packages will serve to accommodate commander's future mission needs. BCT C/EM capabilities, whether organic or tailored support packages, will need higher echelon support to enable responsive BCT planning, deconfliction, gain and loss analysis, database access and advanced analytics.[4] BCTs should also expect to be assigned missions that support the larger C/EM fight, such as site exploitation, gaining close access to adversary networks, or executing kinetic/physical actions that generate C/EM effects.
- (U//FOUO) FM 3-91/FM 71-100 Division Operations : Include C/EM integration in Chapters 1-5; Include C/EM role in wide area security (WAS). At the corps and division level, the emphasis is on setting conditions for BCTs.
- (U//FOUO) FM 3-92/FM 100-15 Corps Operations: Include CyberOps integration in Chapters 2 and 3; Include C/EM role in wide area security (WAS)
- (U//FOUO) FM 3-93 Theatre Army Operations (DRAFT): Include C/EM integration and C/EM targeting process; Include role in setting C/EM conditions, partnering with JIIM partners to build necessary C/EM capabilities and situation awareness. The ASCC is where the full national/joint/service "whole of government" approach comes together. One of its roles is setting Joint theater conditions over time, which in the future will include setting C/EM conditions. The ASCC will need to partner with all appropriate JIIM partners to build necessary C/EM situation awareness, and set the necessary conditions for future operations. The ASCC is critical for building the right planning teams, and conducting the appropriate planning for C/EM considerations within contingency planning. The ASCC gains and maintains C/EM advantage by having knowledge of adversaries in the COCOM AOR through their regionally focused MI Brigade;

[4] US Army Intelligence Center of Excellence , "Fixing Cyber: An Optimum Future for Army Electromagnetic/Cyber Operations." p.7

existing C/EM infrastructure, and possessing some C/EM expeditionary capabilities. Those capabilities are complemented by the ability to "reach" back to COCOM and national-level assets. The ASCC is critical in building a 'standing' C/EM situation awareness. ASCC contingency planning must work C/EM requirements into joint planning groups. Planning needs to address a fully congested/contested C/EM environment and plan accordingly. The impacts in the physical domains must be understood as conditions change in the C/EM contest (e.g. changes in logistics). When given a JTF mission, the ASCC must request the right additional augmentation to address the full joint C/EM contest.

- (U//FOUO) FM 6-02 Signal Support to Army Operations: Describe the art of fighting through a degraded network that explains how anomalies (malicious and non-malicious) are detected, how causation is determined, and how response actions are developed and executed in Chapter 2. Layout the network mission sets, supported commander, NetOps framework, and net focus IAW approved operational context concept in Chapter 3. Describe integrating networks with mission partners (e.g. Afghan Mission Network) and mention integrating entities such as NetOps fusion cells, LNOs, and cross domain solutions in Chapter 3.
- (U//FOUO) FM 6-02.43 Signal Soldiers' Guide: Discuss the prioritization of network resources based on approved mission threads in Chapter 1. Increase information sharing between NetOps and Intelligence in Chapter 2.
- (U//FOUO) FM 6-02.70 EMSO: Address restrictive and permissive coordination issues for C/EM ops and C/EM Targeting & BDA in Chapters 1-6
- (U//FOUO) FM 6-02.71 NetOps: Officially discuss what an enterprise is and describe each portion of the Army Enterprise Network (IAW the high level system view) that covers the Network Service Center cloud, home/TDY, post/camp/station, and deployed environments (Chapter 1). Additionally, describe the art of utilizing situational awareness to C2 and determine actions in and through the network (Chapter 1). Moreover, increase information sharing between NetOps and Intel (Chapter 2). Furthermore, similar to FM 3-90 (Tactics), discuss a true, integrated network defense-in-depth, with a listing of the right roles and responsibilities from the strategic to the company level (Chapter 3).
- (U//FOUO) FM 6-20.10 The Targeting Process: Include C/EM targeting and BDA in Chapters 1, 3, and Appendix B
- (U//FOUO) FM 6-20.40 TTP for Brigade Operations (Heavy): Describe integrating networks with partners, increase information sharing between NetOps and Intel communities in Chapters 1 and 2
- (U//FOUO) FM 6-20.45 Signal Support to Theater Operations: Describe integrating networks with partners, increase information sharing between NetOps and Intel communities in Chapters 1 and 2
- (U//FOUO) FM 6-20.50 TTP for Brigade Operations (Light): Describe integrating networks with partners, increase information sharing between NetOps and Intel communities in Chapters 1 and 2
- (U//FOUO) FM 6-22 Army Leadership: Describe and integrate the Cyber/Electromagnetic Contest as well as how it relates to a military leader's technical knowledge.

Residual Gap Assessment

(U//FOUO) The identified potential solutions will adequately mitigate C/EM doctrine gaps; however these must be implemented in conjunction with other aspects of DOTMLPF to fully mitigate the gaps as a whole.

Cost

(U//FOUO) The cost of implementing the identified potential solutions is moderate and is comparable to the current approach. Doctrine will be revised through the normal doctrine review process.

2-2 Organization

Introduction

(U//FOUO) The Army lacks the proper organization to effectively conduct the C/EM contest. Army staffs lack an integrating entity that can provide commanders an understanding of the C/EM Contest and the ability to plan, coordinate, synchronize and integrate C/EM activities and operations. Units lack the proper organizational structure to provide network access, transition network C2 and conduct Cyber Defense. These capabilities are required to stay apace of commercial technologic advancements and to prevent the introduction of game-changing technologies by adversaries.

FSA Methodology for Developing Organization Solutions

(U//FOUO) During the FNA, ~~104~~ gaps were identified with organizational aspects. The C/EM CBA Team conducted a series of working groups, teleconferences and workshops. FSA Workshop #1 was the primary venue conducted with subject matter experts that assisted in the development of the primary organizational solutions. Refinement has continued with subject matter experts resulting in better organizational solution resolution.

FNA Gaps with Organizational Aspects

- (U//FOUO) Cyber/Electromagnetic Integrating Entity (Gap 02): Battalion level and above staffs lack the appropriate organization for situational awareness, expertise/capability to integrate all aspects of the C/EM contest (situation awareness, offense, defense, and support), and the necessary 'practitioner' expertise for the C/EM tasks that they must execute. Each echelon lacks sufficient expertise/capability to request C/EM capabilities resident at higher echelons.
- (U//FOUO) Establish, Operate, and Manage an Enterprise Network/Network Enabled Mission Command (Gap 11): The Army lacks the capability to provide network access to all organizations that do not have organic network assets (too few Expeditionary Signal Battalions and no Signal support at the maneuver company level). Additionally, Signal elements at the Corps and Division, as well as the Theater Tactical Signal Brigades (TTSB) lack the ability to perform emerging missions (JTF-enabled HQ and Regional Network Operations Security Center respectively).
- (U//FOUO) Transition Network C2 (Gap 15): NETCOM lacks an organizational element that coordinates transition from generating to operating forces.
- (U//FOUO) Network Defense in Depth (Gap 20): Brigades/BCTs S6s, as well as Expeditionary Signal Battalions lack designated Information Assurance / Computer Network Defense (IA/CND) structure. TNOSCs and Network Enterprise Centers structure lacks the ability to support the current/future IA/CND requirements. Cyber Brigade organizational structure lacks NetOps related

positions to develop synergy between NetOps related positions to develop synergy between NetOps and CyberWar elements and increase information sharing.

- (U//FOUO) Access Critical Network Info, Services, & Applications (Gap 24): The Army lacks the capability to provide network access to critical information, services, and applications to all organizations that do not have organic network assets (too few Expeditionary Signal Battalions to support theater operations).

Organization and Personnel Solutions Relationships

The following solutions are linked to each other because the functions cannot be performed without the other. As an example you cannot have structure without the personnel to fill the positions, and you cannot have personnel without structure to put them in. Specifically Solutions O01 and P01 are linked because O01develops the C/EM Element and P01 develops the personnel filling that Element. O01 is linked to O02 because it lays the foundation for the C/EM Element and O02 adds the additional skills required to conduct the holistic C/EM contest. O01, O02, P01, P02, and P03 are all linked because O01 and O02 build the C/EM Element with all the skills required and P01, P02 and P03 develop the practitioners and technicians to fill these positions.

O01 - Create the C/EM Staff Element and Working Group, Battalion through ASCC
O02 - Add required C/EM personnel/skill sets to the C/EM Element, Battalion through ASCC
P01 - Create C/EM Integration Specialists for battalion through ASCC C/EM Elements
P02 - Provide Cyber Warfare Expertise (Develop new 35A Cryptologic Cyber Analyst and 35-Series C/EM Offensive Technical Analyst from existing 35-series specialties)
P03 - Develop new 25-series enlisted Cyber Defense MOS, officer cyber defense ASI, and cyber defense specialty within Civilian Career Program 34 from existing 25-series specialties

Identified Potential Solutions

O01 – Create the C/EM Staff Element and Working Group, Battalion through ASCC (No growth - Bundled solution with P01, P02, P03)

Description (U//FOUO) This solution provides a ‘no growth’ creation of a C/EM Staff Element and Working Group, battalion through ASCC, in order to provide C/EM planning, integration and synchronization. This C/EM element/working group will accomplish two primary functions:

- integrate and synchronize C/EM capabilities and activities to achieve desired conditions in cyberspace and the electromagnetic spectrum;
- Integrate C/EM capabilities and activities into the combined arms operation.

These two functions can be successfully achieved by transforming and expanding the mission of the existing EW Element and associated EW Working Group. This provides an integration capability to plan, coordinate and synchronize C/EM activities as part of the Mission Command warfighting function.

C/EM Staff Element and Working Group Overview

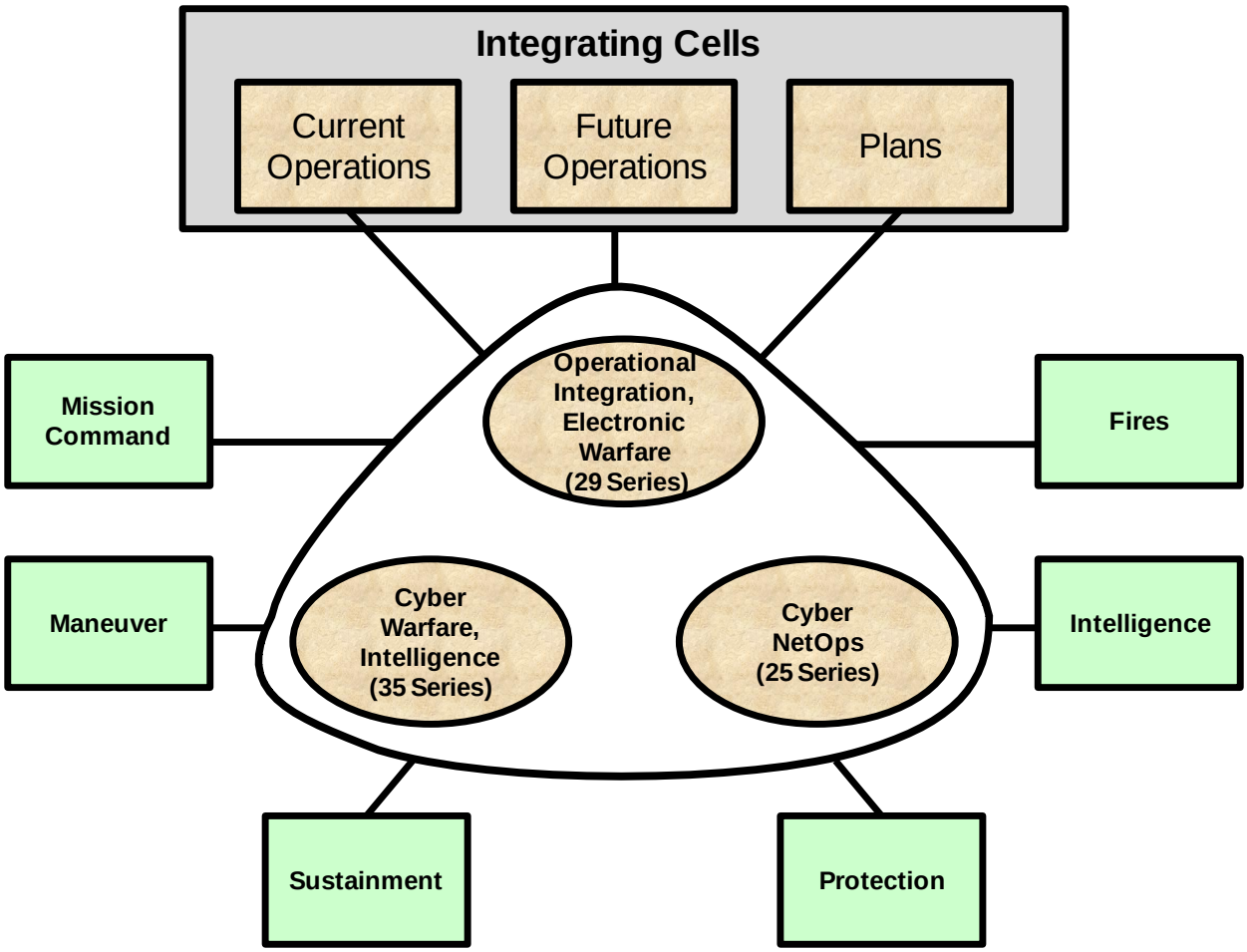
(U//FOUO) *Function #1: Integrate and synchronize C/EM capabilities and activities to achieve desired conditions in cyberspace and the electromagnetic spectrum.* The C/EM staff element and working group seek to unify the offensive and defensive aspects of C/EM activities (including cyber warfare, cyber NetOps, EA, EP, ES). They orient on the commander's stated conditions to gain and maintain advantages for cyberspace and the electromagnetic spectrum. To this end, the element/working group serves as the source of C/EM situation awareness and continually assesses progress toward desired conditions. The element/working group performs vertical and lateral synchronization across echelons to achieve the best results from assigned and supporting capabilities. The element/working group seeks to garner maximum benefit from parallel operations in cyberspace and the spectrum (either of these mediums are respectful of echelons, and it is quite possible that other formations & agencies will be active in cyberspace/spectrum that is of importance/relevance to the command). The element/working group integrates all appropriate capabilities (C/EM and/or physical), in order to achieve these desired conditions.

(U//FOUO) *Function #2: Integrate C/EM activities as part of combined arms operations.* The C/EM staff element and working group also works to ensure that both cyberspace and the spectrum are leveraged to maximum effect to achieving the unit's overall mission. This could include setting conditions in cyberspace and the spectrum to facilitate a unit's main effort, or perhaps providing the means for successful inform and influence activities.

(U//FOUO) Both functions will be accomplished by holistically integrating within the three Operations integrating cells (current operations, future operations, and plans). The element/working group coordinates the critical components of C/EM activities across all the warfighting functions and staff elements (G/S2, G/S3, G/S6, etc.), both vertically and horizontally. This will include integration with external staffs, organizations and coalition partners (JIIM). Given the very dynamic nature of C/EM activities, the C/EM element requires a presence in the current operations cell, and may need co-located representatives from the G/S2, G/S3, G/S6, etc. to achieve real time awareness and direct dynamic actions and response actions to unfolding challenges and opportunities. (Figure 3 below).

(U//FOUO) To integrate and synchronize C/EM capabilities for a holistic and synergistic effect the C/EM element and working group must be able to coordinate and synchronize C/EM and all aspects of the C/EM contest to include all of the components of Cyber Operations (CyNetOps, Cyber SA, CyberWar, Cyber Spt), EW and EMSO. These

include integrating offensive and defensive C/EM synchronization functions, NSA targeting, and Dynamic Cyber Defense actions throughout operational processes. This Element will coordinate and integrate Signals Intelligence enabled CyberWar with Cyber NetOps capabilities.



(U//FOUO) Figure 4: C/EM Element & Working Group Integration

C/EM Staff Element Tasks

(U//FOUO) Analysis performed during the December 2010 Unified Quest C/EM Contest Seminar developed a refined initial list of required tasks for the C/EM Element, by echelon, to integrate and synchronize C/EM capabilities and activities as part of full spectrum operations. This list encompasses C/EM Element staff integrator and planner tasks (cyber, EW and EMSO) and coordination tasks (Table 1).

Cyber/Electromagnetic Element Tasks

- Plan, integrate, coordinate, and assess the holistic employment of the full range of C/EM capabilities in unit operations
- Plan and request offensive and defensive C/EM capabilities and actions into the scheme of maneuver as part of the MC WFF, to include degraded operations
- Synchronize and integrate offensive and defensive C/EM capabilities and actions into the scheme of maneuver as part of the MC WFF
- Facilitate and conduct C/EM vertical and horizontal integration and synchronization of operations across the WFF
- Synchronize operations with space, high altitude, cyber, airborne and electromagnetic capabilities
- Develop, consolidate, analyze, determine, disseminate and integrate Commander's C/EM SA and update the common operational picture
- Support other internal activities (IIA, MISO, functional and integrating processes)
- Facilitate law enforcement and CI activities as they apply to C/EM activities
- Lead the C/EM Working Group
- Plan, assess and direct friendly electronics security measures
- Prioritize C/EM effects and targets
- Deconflict C/EM activities with operations, to include intelligence
- Maintain a current assessment of available C/EM capabilities
- Serve as subject matter expert for C/EM and EW
- When designated, serve as the jamming control authority
- Prepare, submit for approval, and assess the implementation of C/EM activity fragmentary orders
- Determine, adjudicate and forward spectrum user requirements
- Conduct staff coordination
- Responsible for the Joint Restricted Frequency List (JRFL)
- Process frequency requirements
- Conduct frequency deconfliction and interference resolution for EA
- Request, obtain, and distribute frequencies for EA emitters
- Coordinate with network planners in matters concerning spectrum requirements
- Maintain and update databases
- Support C/EM TTP development
- Recommend and assess friendly EP related protection measures

(U//FOUO) Table 1: C/EM Element Tasks

C/EM Working Group Tasks

(U//FOUO) The C/EM Element chairs the C/EM Working Group to ensure appropriate planning, integration, and synchronization across the WfFs. The C/EM Working Group provides additional capacity and expertise to execute C/EM activities that are beyond the skill sets internal to the C/EM Element. C/EM Working Group Tasks were also identified to facilitate the internal (Army) and external (Joint) integration,

synchronization, and deconfliction of C/EM actions and provide the Working Group with the capability to make recommendations for specific C/EM actions (Table 2).

Cyber/Electromagnetic Working Group Tasks

- Plan, integrate, coordinate, and assess the holistic employment of the full range of C/EM capabilities in unit operations
- Plan and request offensive and defensive C/EM capabilities and actions into the scheme of maneuver, to include degraded operations
- Synchronize and integrate offensive and defensive C/EM capabilities and actions into the scheme of maneuver
- Facilitate and conduct C/EM vertical and horizontal integration and synchronization of operations across the WFFs
- Synchronize operations with C/EM capabilities in other domains such as aerial, high altitude and space.
- Plan, assess and direct friendly electronics security measures
- Prioritize C/EM effects and targets
- Deconflict C/EM activities with operations, to include intelligence
- Determine, adjudicate and forward spectrum user requirements
- Conduct frequency deconfliction and interference resolution for EA
- Support C/EM TTP development
- Integrate C/EM into the operations process
- Identify and coordinate intelligence support requirements for unit C/EM operations
- Assess offensive and defensive C/EM requirements
- Maintain current assessment of C/EM resources available to the unit
- Prioritize C/EM effects and targets
- Recommend and assess friendly C/EM related protection measures

(U//FOUO) Table 2: C/EM Working Group Tasks

C/EM Staff Element and Working Group Expertise

(U//FOUO) The resident expertise required in the C/EM element/working group is driven by the tasks to be conducted. Taken together, the element and working group need the following skill sets (identified in the Functional Needs Analysis) to be successful:

- Establish, operate, and defend the network
- Ability to access intelligence
- Electronic Warfare
- Spectrum management (EMSO)
- Employ offensive C/EM and dynamic defense capabilities (e.g. cryptologic)
- Ability to access support activities (e.g. higher level C/EM capabilities, forensics, vulnerability assessment)
- Synchronization and Integration

Since the C/EM working group draws from the full range of skill sets and expertise across the staff, assigned units, and supporting capabilities; there should be few

shortfalls in the working group composition. The more significant question is what skill sets need to be resident on a permanent basis in the C/EM staff element. Staffing in this element is driven by the need to accomplish the two integration functions described above, and the need to achieve dynamic & rapid integration, yet must be tempered by available resources. Any shortfalls in the manning of the element will need to be compensated for by the activities of the working group.

Recommended Solution

(U//FOUO) Based on analysis of the current Army's force structure, the existing EW element and associated working group is the most logical source for providing an initial resolution for C/EM integration and planning gaps. Based on the 2008 approved EW Force Design Update, EW Elements are being added to unit TO&Es and are conducting operational integration for EW. Currently, the EW staff element performs 24 of 26 C/EM staff element tasks (specific to EW) and leads a working group that performs all 17 C/EM working group tasks (specific to EW). Based on these facts, the EW Element already includes the basis skill sets to conduct integration, participate in the operations process, and lead a working group, and boasts EW and spectrum management expertise.

(U//FOUO) This solution is 'bundled' with Solutions P01 (Create C/EM Integration Specialists for battalion through ASCC C/EM Elements, P02 (Provide Cyber Warfare Expertise), and P03 (Develop Cyber Defense Specialties). Once adapted, these solutions will provide both a C/EM planner/integrator and improved offensive and defensive specialists that has the acumen to effectively incorporate all aspects of the C/EM contest (cyberspace and EMS) into the commanders' decision making process.

(U//FOUO) Other 'no-growth' options were considered, such as 'dual-hatting' other existing staff elements as the C/EM integrator. Assigning these responsibilities to the G/S6 was not selected because of its necessary focus on operating and defending of the network. The G/S3 is considered to be fully occupied with the overall operations process. The G/S2 was also considered and not selected because of its necessary focus on the intelligence warfighting function. The existing staff structures lack the additional capacity, in a 'no growth' constrained environment, to take on the holistic integration of C/EM activities. In contrast, the EW staff element/working group already has an existing DOTMLPF structure that can be readily adapted for this purpose.

Costs (U//FOUO) O01 is a 'no growth' solution, based on the existing EW FDU resourcing, and is in concert with the MI Rebalancing and the Signal FAA initiatives. Current resourcing provides a minimal core C/EM staff element, so the C/EM Working Group will be relied upon to provide the full expertise needed to holistically synchronize and integrate C/EM activities. Although described more fully in solutions P01, P02, and P03, this solution (O01) will require some modification of existing training for personnel assigned to the C/EM staff element and working group. Initial analysis of potential training requirements indicates that this would be a minimal impact to the Army and will not limit the ability to field the 25, 29, and 35 series.

O02 – Add required C/EM personnel/skill sets to the C/EM Element, Brigade through ASCC (Limited growth - Bundled solution with O01, P01, P02, and P03)

Description (U//FOUO) Add a 35-Series C/EM Offensive Technical Analyst and a 25-Series Cyber Defense Technical Analyst to the C/EM Element and Working Group, Battalion through ASCC. In order to integrate and synchronize C/EM capabilities to achieve real time awareness and direct dynamic actions and response actions as shown in Figure 3 below, the C/EM Element requires additional Cyber Warfare, Intelligence 35-series and Cyber NetOps 25-series technical C/EM personnel/skill sets, BCT/BDE through ASCC. The C/EM element and working group must be able to coordinate and synchronize C/EM activities and all aspects of the C/EM contest as described in Solution O01, to include Cyber Operations (CyNetOps, Cyber SA, CyberWar, Cyber Spt), EW and EMSO. C/EM offensive and defensive capabilities are nested within the CyberWar and CyberNetOps expertise requirements. These are highly skilled experts that is the "technical backbone" required to support the operational planner and operations planning process. These skill sets are the technical SMEs that will work within the C/EM elements and will bridge technical capabilities to operational requirements. Additional analysis will be required post CBA to determine specific tasks by position within the C/EM element.

(U//FOUO) The EW FDU was approved in 2008 for a total of 3,728 positions but was only resourced for 1,664 positions by TAA 10-15. Based on TAA 10-15, the GENFOR positions and the full complement of tactical level positions (BCT and below) was not resourced but will be required to recomplete in TAA 12-17. These positions were originally identified as critical capabilities and are still required in order to fully integrate and synchronize C/EM capabilities and activities at the tactical levels and the tip of the spear for the Army modular forces.

Rationale (U//FOUO) The 25 and 35 series additional required capability would provide structure to coordinate and integrate CyberWar and CyberNetOps tasks from the brigade through ASCC, to include ARCYBER. This solution requires the addition of a 35-Series C/EM Offensive Technical Analyst and a 25-Series Cyber Defense Technical Analyst who has the ability to provide analysis to establish target identification and operational patterns and maintain intelligence information. The 35-series is specially trained in C/EM exploit and attack functions. Adding these specialists to the element will provide both offensive and defensive C/EM expertise required to integrate the necessary C/EM lethal and non-lethal effects with full spectrum operations. This solution helps to resolve Gap 02 - C/EM Integrating Entity and is supported by P01 – Create C/EM Integration Specialists for battalion through ASCC C/EM Elements, P02 – Develop new 35A Cryptologic Cyber Analyst and 35-Series C/EM Offensive Technical Analyst from existing 35-series specialties for ARCYBER and operational echelons (ASCC-BCT).

Costs (U//FOUO) O02 is a 'limited growth' solution and requires the addition of a 35-series and a 25B Information Technology Specialist or 255S Information Protection

Technician to the current EW Element structure. This solution adds approximately 102 compo 1, 84 compo 2, and 4 compo 3, 25X and 35A positions (ASCC, Corps, Division, BCT and functional and multifunctional brigades).

(U//FOUO) The EW FDU required 3,728 positions and was resourced for 1,664 positions by TAA 10-15. The remaining 2,064 positions not currently resourced are in brigades and battalions and include the 29-series integrators and 25E spectrum managers. To fully leverage the EW Element, the TAA 12-17 FDU recompete of the EW CMF positions will be a requirement.

(U//FOUO) The additional 25-series and 35-series positions can be filled by changing and moving MOSs from other existing organizations (zero sum gain), or by adding the two positions to the current organizations with the attendant personnel costs. Solution O01 in black (no cost), Solution O02 in black plus red and blue positions.

Echelon	Black is EW FDU-Requirement Solution O01, 29 series structure already in place Blue positions not resourced in TAA 10-15	Proposed C/EM Element and Position Titles Blue positions not resourced in TAA 10-15 Red positions add 25/35 series
ASCC 5.4	1xO6 29A EW Dir 1xO5 29A EW Deputy 1xCW3 290A EW Targeting	1xO6 29A C/EM Dir 1xO5 29A C/EM Deputy 1xCW3 290A C/EM Targeting 1x25B40 C/EM Defensive Analyst 1x35-Series C/EM Offensive Analyst
CORPS 4.1	1xO5 29A EW Ch 2xO4 29A EW Deputy/Plans 1xCW4 290A EW Targeting 1xE9 29E50 EW NCOIC 1xE7 25E40 Spectrum Mgr	1xO5 29A C/EM Ch 2xO4 29A C/EM Deputy/Plans 1xCW4 290A C/EM Targeting 1xE9 29E50 C/EM NCOIC 1xE7 25E40 Spectrum Mgr 1x25B40 C/EM Defensive Analyst 1x35-Series C/EM Offensive Analyst
Div 5.1	1xO5 29A EWCC Ch 1xO4 29A EWCC Deputy 1xCW4 290A EW Targeting 1xE9 29E50 EW NCOIC 1xE7 25E40 Spectrum Mgr	1xO5 29A C/EM Ch 1xO4 29A C/EM Deputy 1xCW4 290A C/EM Targeting 1xE9 29E50 C/EM NCOIC 1xE7 25E40 Spectrum Mgr 1x25B40 C/EM Defensive Analyst 1x35-Series C/EM Offensive Analyst

H/I/S BCT **Select Multifunctional and Functional Bdes**	1xO3/O4 29A EW Off 1xCW3/2 290A EW Targeting 1xE8/7 29E5/40 EW NCOIC 1xE6 29E30 EW NCO 1xE6 25E30 Spectrum Mgr 1xE5 29E20 EW NCO	1xO3/O4 29A C/EM Off 1xCW3/2 290A C/EM Targeting 1xE8/7 29E5/40 C/EM NCOIC 1xE6 29E30 EW NCO 1xE6 25E30 Spectrum Mgr 1xE5 29E20 EW NCO 1x25B30 C/EM Defensive Analyst 1x35-Series C/EM Offensive Analyst
Maneuver BN & Select Functional BNs	1xE7/6 29E4/30 EW NCOIC 1xE6/5 29E3/20 EW NCO 1xE6 25E30 Spectrum Mgr* **Selected Maneuver Battalions*	1xE7/6 29E4/30 EW NCOIC 1xE6/5 29E3/20 C/EM NCO 1xE6 25E30 Spectrum Mgr* **Selected Maneuver Battalions*

(U//FOUO) Table 3: C/EM Element

O03 – Modify Expeditionary Signal Battalion (ESB) structure to provide network connectivity and defense capabilities.

Description (U//FOUO) This proposed solution would convert ESB structure to a Joint Communications Support Element (JCSE) like organization, everything-over-Internet protocol (EoIP) format consisting of restructured teams that are modular and scalable and provides more communications packages based on less support/less transport requirements. The solution more than doubles the total pooled network support packages, increases the ARFORGEN available pooled support packages from 150 to 432, and ARFORGEN disadvantaged units will see an increase in support from 34% TO 98%, with no personnel bill.

Rationale (U//FOUO) Network access is required for all echelons in order to ensure the right individuals, receive the right information, at the right time, and in the right format to provide situational awareness and support the commander's critical information requirements. This solution helps to resolve Gap 11 Establish, Operate, and Manage an Enterprise Network/Network Enabled Mission Command and Gap 24 Access Critical Network Info, Services, & Applications.

Costs (U//FOUO) There would be little cost to modifying the ESB as Signal structure will be utilized to find bill payers.

O04 – Designate a NETCOM element to coordinate network C2 transition

Description (U//FOUO) Designate an element within NETCOM in order to coordinate network C2 transition authorities as a unit executes all phases of an operation.

Rationale (U//FOUO) This solution will help provide units the capability to effectively, efficiently, and seamlessly transition network C2 authorities by establishing an element within NETCOM that is responsible for these responsibilities. This solution helps to resolve Gap 15 Transition Network C2.

Cost (U//FOUO) There would be little cost to establishing an element within NETCOM element that is responsible for seamlessly transitioning network C2 authorities.

O05 – Reorganize Brigade/BCT S6 structure IAW the NetOps Construct

Description (U//FOUO) Create cells within the Brigade/BCT S6 specifically designated to execute the roles/responsibilities related to enterprise management, content management, and network defense functions.

O / W / E / Total 2 / 3 / 24 / 29		
S6 HQ		
25A00	O4	S6
53A00	O3	INFO SYS MANAGER
25U50	E8	SIGNAL SPT SYS CHIEF
SIGNAL SYSTEM INTEGRATION OVERSIGHT		
25W40	E7	SYS INTEGRATION CHIEF
25U30	E6	SIGNAL SYS OPS NCO
NETWORK MANAGEMENT		
250N (255N)	W2	NETWRK MGT TECH
25W40	E7	NETWORK OPS CHIEF
25E30	E6	ELECTRO SPECTRUM NCO
25B30	E6	DATA SYS INTEGRATOR
25N30	E6	NODAL OPS SYS NCO
25S30	E6	SATCOM OPS NCO
25U30	E6	SIG INFO SVC NCO
25N10	E4	NODE OPS SYS OPR-MNT
25B10	E3	LAN MGR
INFORMATION PROTECTION		
251A (255S)	W3	IA/CND TECH
25B40	E7	IA STAFF NCO
25B30	E6	IA STAFF ASST
25B30	E6	IA STAFF ASST
25B40	E7	COMSEC CUSTODIAN
25B30	E6	ASSIST COMSEC CUST
INFORMATION SERVICES		
254A (255A)	W2	IDM/CS TECH
25B40	E7	IDM STAFF NCO
25B30	E6	INFO SYS TEAM CHIEF
25B20	E5	SR INFO SYS SPC
25B10	E4	NETWORK SUP SPC
25U20	E5	SIGNAL SPT NCO
25U10	E3	SIGNAL SUP SYS SPC
25L20J2	E5	SR CBL/ANT SYS-SPL
25L10 J2	E4	CBL/ANT SYS-SPL

(U//FOUO) Table 4: Brigade/BCT S6 Structure

Rationale (U//FOUO) G6/S6 elements are required to provide commanders with NetOps capabilities from the BN and above level; yet while Division organizational structure and above assist the G6s in understanding and performing their roles/responsibilities in reference operating and defending the network; brigade/BCT organizational structure does not designate positions to execute IA/CND tasks. The result is the execution of IA/CND task is not given the same priority as "operate" tasks. Additionally, when cyber events occur, there is confusion as to who at the brigade/BCT is responsible to assist in response actions. This solution will help provide brigades/BCTs the capability to establish network defense in depth in order to protect against, monitor for, detect, analyze and dynamically respond to threats. This solution primarily helps solve Gap 20 Network Defense in Depth.

Cost (U//FOUO) Results in no cost to the Army due to the reorganization, allocation of already existing positions.

O06 – Franchise Theater Network Operations and Security Centers and Network Enterprise Centers

Description (U//FOUO) This proposed solution addresses organizational structure requirements at the TNOSCs and NECs in order to support the increase in IA/CND mission. This solution addresses gap 20

Rationale (U//FOUO) Help provide TNOSCs and NECs with personnel designated to protect the network against threats, as well as monitor for, detect, analyze, and respond to threat events

Cost (U//FOUO) Results in no cost to the Army due to the reorganization, allocation of already existing positions.

O07 – NetOps Positions in Cyber Brigades

Description (U//FOUO) Designate positions within the Cyber Brigades to develop synergy between NetOps and CyberWar elements and increase information sharing. This solution addresses gap 20.

Rationale (U//FOUO) Cyber Brigades will provide Dynamic Cyber Defense capabilities which can be enhanced by the knowledge, skills, and abilities of future cyber defenders existing within the NetOps community.

Cost (U//FOUO) Results in no cost to the Army due to the reorganization, allocation of already existing positions.

2-3 Training

Introduction

(U//FOUO) Currently the Army does not holistically incorporate the Cyber/Electromagnetic (C/EM) Contest into training. Although the common Soldier, Civilian and Contractor operates in the C/EM Contest on a constant basis, whether through the use of communication systems or employing counter-IED devices, little training is devoted to the C/EM Contest as a dimension of full spectrum operations (FSO). In order to fully integrate the C/EM Contest into FSO, a basic understanding of the C/EM Contest must be incorporated into common individual and collective training. C/EM training events should be integrated into Combined Arms Training Strategies. Warrior Skills, Common Skills, Warrior Leader Tasks, Common Core Portion of Professional Military Education (PME) and training for DA Civilians and Joint, Interagency, Intergovernmental, and Multinational (JIIM) partners need to incorporate basic C/EM knowledge. Basic C/EM knowledge should cover broad topics such as defining the C/EM Contest, integrating the use of cyberspace / the electromagnetic spectrum (EMS) into FSO, thinking of cyber and the EMS as maneuver space where positional advantage is possible, and the effects of the C/EM Contest on friendly operations and enemy capabilities. This basic C/EM knowledge is not meant to be an in-depth operator level on the specifics of conducting the C/EM Contest, but rather baseline awareness training for all Soldiers. Some Soldiers will require specific knowledge taught in highly specialized courses discussed in T04. In addition to incorporating the C/EM Contest into individual and collective training, the C/EM Contest should also be incorporated into collective training exercises such as field training exercises (FTX) and command post exercises (CPX) at home station and missions readiness exercise (MRX) at the Combat Training Centers (CTCs). The Army should expand already funded and integrated Electronic Warfare initiatives by incorporating C/EM objectives into EW training.

FSA Methodology for Developing Training Solutions

(U//FOUO) The FNA identified 18 gaps as having Training aspects. The C/EM CBA Team conducted a series of working groups, teleconferences and workshops which culminated in FSA Workshop #3 where 20 SMEs discussed possible Training solutions for the identified gaps.

FNA Gaps with Training Aspects

C/EM Integrating Entity (Gap 02)
Legal Advisement for C/EM (Gap 06)
Establish, Operate, Manage Enterprise Network (Gap 11)
Transition Network C2 (Gap 15)
Integrate CyNetOps with Mission Partners (Gap 19)
Network Defense in Depth (Gap 20)

Access Critical Network Info, Services, & Applications (Gap 24)
Non-Attributed Network (Gap 26)
Organic BDE C/EM Collect and Exploit Intelligence (Gap 29)
Cyber Attack (Gap 32)
Threat Hardware & Software Analysis (Gap 33)
Cyber Vulnerability Assess & Operational Testing (Gap 36)
EA Asset Deconfliction (Gap 37)
Cyber Threat Investigation Information Sharing (Gap 38)
C/EM Situational Awareness, COP (Gap 40)
Conduct Electronic Attack (Gap 45)
C/EM Modeling and Simulation (Gap 46)
Detect Jamming (Gap 50)

Identified Potential Solutions

T01 – Incorporate basic C/EM Contest knowledge into individual training

Description (U//FOUO) Add C/EM tasks to STP 21-1-SMCT (Soldier's Manual of Common Tasks [SMCT], Warrior Skills Level 1). The C/EM related proponents must identify the individual training tasks to incorporate C/EM into existing Electronic Warfare Common Warrior Tasks. The C/EM related proponents must develop individual and staff level IMMI training to be incorporated into the Army's Lifelong learning programs. In a school environment include C/EM online training through Skillport. LNOs need training to facilitate integration of mission partners. The C/EM related proponents, in coordination with the Staff Judge Advocate School, requires the capability to incorporate legal advisor training into their existing professional military education with emphasis on C/EM resource availability. (Gaps 02, 06, 11, 19. 32, 33, 36, 40, 45, 46, 50)

Rationale (U//FOUO) Soldiers and leaders at all echelons will be better equipped to incorporate C/EM capabilities into FSO if they have a basic understanding of the C/EM Contest. Legal advisors must have up to date knowledge regarding rules of engagement (ROE) for the C/EM Contest.

Cost (U//FOUO) The cost of implementing is moderate and is comparable to the current approach.

T02 – Incorporate C/EM into home station training

Description (U//FOUO) The C/EM related proponents must identify the collective training tasks to incorporate C/EM into the ASAT database so that C/EM training can be added into the Generating and Operational Forces Common Warrior Tasks. This will establish initial awareness training and follow on sustainment training. Requirements for Electronic Warfare collective training at home station exists. EW Mobile Training Teams currently support organizational training. Add C/EM materiel into mobile training team (MTT) Program of Instruction. (Gaps 02, 11, 19, 32, 33, 36, 37, 40, 45, 46, 50)

Rationale (U//FOUO) Soldiers and leaders at all echelons will be better equipped to incorporate C/EM capabilities into FSO if they have a basic understanding of the C/EM Contest.

Cost (U//FOUO) The cost of implementing is moderate and is comparable to the current approach.

T03 – Incorporate basic tasks that test C/EM knowledge into collective training and CTC events.

Description (U//FOUO) The C/EM related proponents must identify the Combined Army Training Strategy (CATS) for individual to battalion to enable the C/EM Contest to be incorporated into home station training and CTC exercises. Collective tasks should then be linked to appropriate FSO mission essential task list (METL) tasks. This training must be offered on campus, on-site, and online. Include degraded operations as well as attacks on friendly networks. Commanders and Soldiers, especially G/S-6 Soldiers, need to understand mission command systems and the unit's portion of the network. Deployed units need to be able to perform critical functions in the absence of or with a decreased presence of civilian contractors and field support representatives. This is critical for mission command on the move or when operating on a tactical network removed from a FOB. CTCs have recognized the importance of training EW during rotations and having properly trained O/Cs (Observer/Controller). CTCs have received funding to hire EW contractors in FY10 at NTC, JRTC, and JMRC. BCTP will contract EW SMEs in FY11. The FCOE is postured to deliver EW familiarization training and ASI 1J courses for O/Cs in the 1st quarter of FY11. The Army should utilize the EW SMEs already funded and expand the current CTC EW objectives to include C/EM (to include realistic cyber modeling and simulations). (Gaps 02, 11, 15, 32, 33, 37, 40, 45, 46, 50)

Rationale (U//FOUO) The Army's Training Concept 2012 – 2020 puts forth an Integrated Training Environment (ITE) which will mitigate training gaps where resources are limited or currently unavailable by providing resources for realistic training. When building the ITE the Army must be able to simulate cyberspace and the electromagnetic spectrum and be sure to incorporate this into full spectrum operations FSO scenarios.

Cost (U//FOUO) The cost of implementing is moderate and is comparable to the current approach.

T04 – Specialized Training and Certification

Description (U//FOUO) This solution encompasses specialized training that will be needed for personnel executing specific C/EM objectives and are not addressed T01-T03. Some specialized training could be included in pertinent existing MOS training. The Army should review, create, modify, and fully support training with industry partnerships and internships that enhance C/EM Soldiers and civilians skills. Required

specialized training includes the following topics (Gap 11, 19, 20, 24, 26, 29, 32, 38, 45, 46):

- Application development (including mobile applications)
- Non-attributable operations
- C/EM collection systems capabilities, integration, and use
- NET, Operator, and maintenance of EW Systems
- Integration of cyber threat information across Army units, law enforcement, and counterintelligence
- Integration of EA
- Cyber and EMS modeling and simulation
- Advanced Cyber Defense virtual training that focuses on monitoring, detection, analysis, and response
- Cyber Defense certification qualification process for cyber defense teams at all echelons and would be validated at specified stage

Rationale (U//FOUO) Some gaps cite specialized training requirements. For example Gap 24, Access to Critical Network Information, Services, and Applications require the Army to provide application development training to personnel performing related duties. These specialized skills would not be address in individual or collective training for all Soldiers.

Cost (U//FOUO) The cost of implementing is moderate and is comparable to the current approach.

T05 – Propose a Joint Cyber Training Enterprise

Description (U//FOUO) Propose a DoD/NSA/USCYBERCOM accredited Cyber Training Enterprise that brings together all aspects of Cyberspace Operations (establish, operate, manage, defend, exploit, and attack); supports the apprentice, journeyman, master development model; ensures learning and mentorship across training, operational, academia, and industry entities; and leverages existing Army or joint resources and partnerships in order to meet Army and JIIM requirements. This solution addresses Gaps 11, 19, 20, 24, 29, 32, and 36.

Rationale (U//FOUO) Currently there are pieces and parts of cyber training across the Army and other services (e.g. JCAC – Navy, 255S course – Army, UNWT – Air Force, Basic CNO Planners Course - Army). All add value and address training gaps, yet there are more efficiencies to be had if all cyber training can be brought under a cyber training enterprise in order to achieve unity and “jointness”, provide direction as to required skills, develop synchronization that creates more realistic training, and utilizes existing resources and partnerships to minimize costs.

Cost (U//FOUO) The cost of implementing is moderate and is comparable to the current approach.

T06 – Establish NetOps Training Program

Description (U//FOUO) Establish a NetOps training program which combines classroom training with immersive operational experiences to develop technical and management expertise for specialized follow-on assignments. This consists of six phases: Phase 0 is Admin/Security in order to ensure Soldiers receive the proper clearance. Phases I and II are Basic NetOps and Advanced NetOps respectively and would be implemented at home station IAW one of the four stated platforms (1 – Post w/Corps and above, which provides integrated NetOps training; 2 - Post w/Divisions, which provides integrated NetOps, as well as specific enterprise management, network defense, and content management training; 3 - all others (e.g. NG and Reserve locations); and 4 – CTCs). Phases III and IV are Duty Position and Mission Support, which would be conducted at regional sites (e.g. TNOSC-S). The last phase (Phase V) can be Deployment Support in which NetOps Cadre evaluate and critique Soldiers during MRXs and/or in the AOR. This solution addresses Gaps 11, 15, 19, 20, and 24.

Rationale (U//FOUO) Realistic training, high standards for technical competence, strong analytical skills, and immersion are key elements that shape the force. The current training program is position oriented vs. unit oriented. Because of the diversity of mission across similar units, as well as across strategic, operational, and tactical echelons, position oriented training in many cases, results in new arrivals lacking the knowledge and understanding of how to support the unit mission.

Cost (U//FOUO) The cost of implementing is moderate and comparable to the current approach.

T07 – Support IA Certification Qualification Requirements

Description (U//FOUO) Ensure training funds are provided in order to support the training institution's effort to meet DoD IA certification qualification requirements based on common roles/ responsibilities of MOS/AOC and grade (e.g. 25B20 - Sec+). This solutions addresses Gap 20.

Rationale (U//FOUO) DoD 8570.01-M (IA Workforce) mandates that individuals performing specific functions and filling Information Assurance Management/Technical and Computer Network Defense roles must possess the applicable industry certification in order to fill the position and have access to information and information assurance systems. The certification must be achieved within six months of arrival. Currently students are not required to achieve applicable certifications while at the training institution. This places the onus (both time and money) on units to ensure Soldiers are properly certified.

Cost (U//FOUO) The cost of implementing is moderate and is comparable to the current approach.

Residual Gap Assessment

(U//FOUO) The identified potential solutions will adequately mitigate C/EM training gaps; however these must be implemented in conjunction with other aspects of DOTMLPF to fully mitigate the gaps as a whole. Although Global Network Enterprise Construct (GNEC) and ITE address a range of gaps specifically related to an enterprise network and training environments, C/EM training must account for operations when these resources are not available to the warfighter. GNEC is not expected to be Fully Operational Capable (FOC) until FY2018. Training will need to address network related C/EM gaps until GNEC is FOC.

2-4 Materiel

Introduction

(U//FOUO) The materiel aspects of the Cyber/Electromagnetic (C/EM) contest affect all levels of the operating and generating forces. In many cases the Army lacks the capacity to conduct the necessary C/EM actions with current fielded materiel.

FSA Approach to Materiel Gaps

(U//FOUO) In the course of the development of the FNA, 20 gaps were identified as requiring materiel solutions. To identify these materiel gaps the study team collected subject matter expert's opinions and inputs through workshops, teleconferences, and working groups. The team gathered all the materiel solutions recommendations together and aligned the potential solutions to the materiel requirements of each gap. Materiel solutions adopted or modified to partially mitigate the gap were aligned with the gap. After reviewing the purposed materiel recommendations linked to the gaps the study team categorized the gaps into solution sets creating the minimal solutions required to mitigate the most gaps to a acceptable risk level.

FNA Gaps with Materiel Aspects

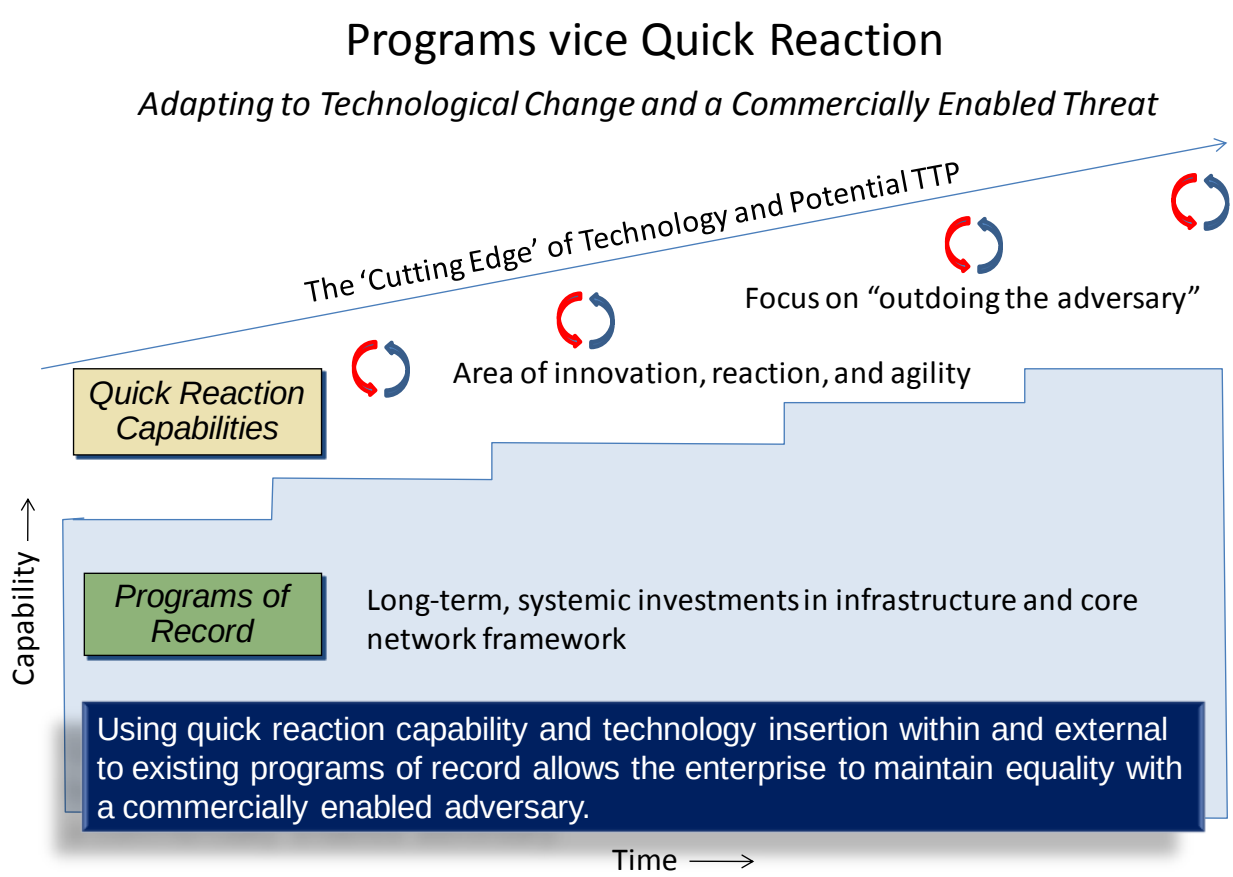
C/EM Integrating Entity (Gap 02)
Establish, Operate, Manage Enterprise Network/Network enabled Mission Command (Gap 11)
Single system and User ID (Gap 17)
Integrate CyNetOps with Mission Partners (Gap 19)
Network Defense in Depth (Gap 20)
Access Critical Network Info, Services, & Applications (Gap 24)
Organic BDE C/EM Collect and Exploit Intelligence (Gap 29)
Cyber Attack (Gap 32)
Threat Hardware & Software Analysis (Gap 33)
Cyber Vulnerability Assess & Operational Testing (Gap 36)
EA Asset Deconfliction (Gap 37)
C/EM Situational Awareness, COP (Gap 40)
Conduct Electronic Attack (Gap 45)
C/EM Modeling and Simulation (Gap 46)
Detect Jamming (Gap 50)
Dynamic Spectrum Management (Gap 51)
EMS Use Plan Export (Gap 53)
Spectrum Use Prioritization (Gap 54)
Defend/Protect Individuals and Platforms (Gap 57)
Research, Development, and Acquisition and Research, Development, Testing and Evaluation (Gap 61)

Programs of Record vice Quick Reaction Capabilities

(U//FOUO) In many cases, the Army relies on Programs of Record (PORs) to provide its capabilities. In some cases, due to unforeseen circumstances or rapidly emerging technologies, Quick Reaction Capabilities (QRCs) are developed in response. The balance between PORs and QRCs is particularly important for the C/EM Contest, given the rapid pace of emerging technology.

(U//FOUO) The primary purpose of PORs is to make long term, systemic investments in infrastructure and the core network framework for the Army. These PORs span years and seek widespread fielding across significant portions of the Army, as they represent the opportunity to make fundamental improvements over time. Although their development and fielding may take years, these programs benefit from long term investment and well-integrated support. These programs employ technical insertions wherever possible to maintain their efficacy.

(U//FOUO) Quick reaction capabilities are required to provide the Army a means to access 'cutting edge' technologies and provide innovative improvements to the Army in a short time frame. They also provide the means to quickly develop tools and weapons focused on adversary capabilities, and /or to react to an adversary's innovations. In either case, the emphasis is on "outdoing the adversary" in terms of action, reaction, and counteraction. QRCs are currently funded outside of the budget process and are based on operational requirements.



(U//FOUO) Figure 5: Programs of Record vice QRC Capabilities

Identified Potential Solutions

M01 – Pursue a modified Army Network Modernization Strategy (ANMS)

Description: (U//FOUO) This solution leverages the current Army Network Modernization Strategy and modifies it to address a wide array of C/EM capability gaps. This will be accomplished by modifying the Network Enabled Mission Command ICD and the LandWarNet (LWN) ICD. Future Integrated Electronic Warfare System (IEWS) CCDs will require networked EW capabilities which support this gap mitigation strategy. Recommended modifications include:

- Make situation awareness of cyberspace/EMS accessible as part of the Common Operational Picture (COP)
- Provide sufficient sensors and applications to enable shared real-time situational awareness of the status of cyberspace and the EMS to facilitate command and control at all echelons, and rapidly respond to early warning of C/EM attacks.
- Provide platforms and delivery systems for C/EM attack
- Enable dynamic electromagnetic spectrum management across echelons
- Enable collaborative and cooperative protection of individuals and platforms

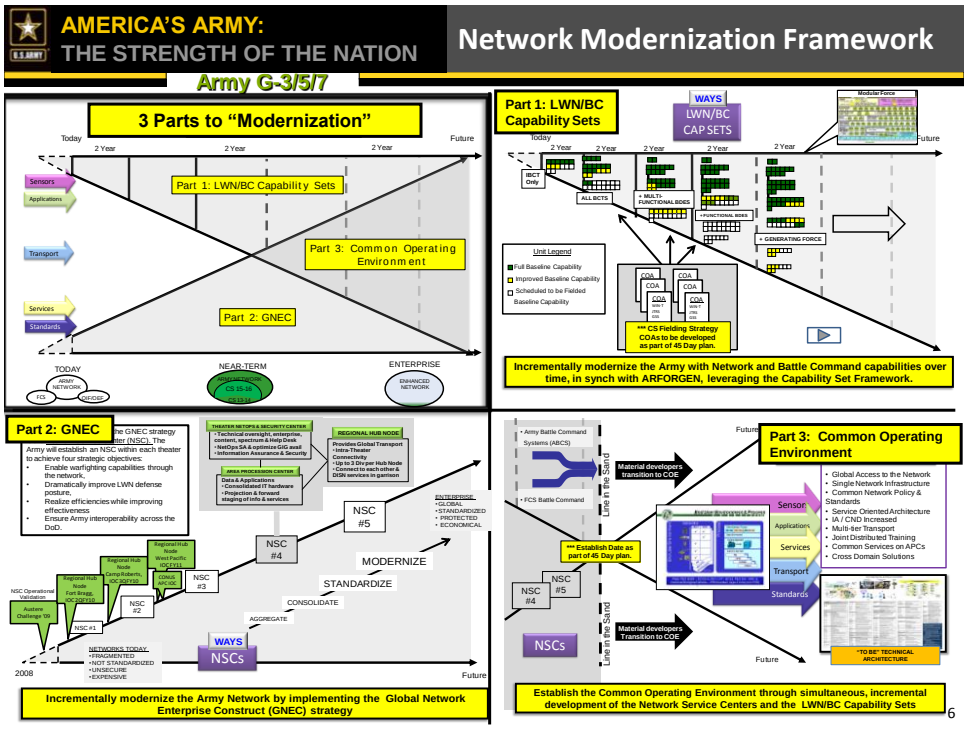
- Provide increased bandwidth and connectivity, to include an aerial tier to the network
- Creation of defensible C/EM infrastructure with the technological diversity and capacity to enable Army forces to respond to, bypass, and fight through C/EM attacks, and allow Army forces to continue to operate even when the overall enterprise is degraded or disrupted.
- Capability to operate networks under suboptimal conditions, including the loss of non-line-of-sight communications and global positioning systems, ensuring external threats, environmental conditions, or lack of interoperability between joint or partnered forces cannot prevent mission accomplishment.
- Redundant methods of transmitting, receiving, and storing information. This mitigates single points of failure.

The Current Strategy

(U//FOUO) The Army Network Strategy is intended to give the Army a single integrated enterprise over time which delivers the full range of necessary mission command capabilities to commanders and their staffs at all levels. The enterprise will allow an information environment with global access, standard infrastructure, a unity of command and control across cyberspace, and the capability to establish, operate, and maintain the enterprise. This will allow units seamless transition of command and control from the generating force to the operating force and from garrison operations to deployed operations. The enterprise will allow Soldiers access to a single system and user identification across the Army allowing access at home station, TDY, in garrison, or deployed. The enterprise will deliver all mission command essential capabilities.

(U//FOUO) The Army Network Modernization Strategy has three lines of effort:

1) Implement the Global Network Enterprise Construct (GNEC)
2) Deliver LandWarNet capability sets over time, aligned with the ARFORGEN process, which incrementally modernize the Army with Network and Mission Command capabilities over time, in synch with ARFORGEN, leveraging the Capability Set Framework
3) Develop a Common Operating Environment (COE)



(U//FOUO) Figure 6: The Army Network Modernization Framework

LOE 1: Implement the Global Network Enterprise

(U//FOUO) The Global Network Enterprise (GNE) Implementation Plan is a strategy for transforming LandWarNet to deliver a globally accessible information capability to Army Soldiers and personnel across the Operating and Generating Forces at all echelons. Network access from any location requires an in-place network infrastructure or the network fails in its basic mission requirement. Three parallel efforts support operationalizing LandWarNet: (1) the development of Army Network Service Centers; (2) adopting EoIP for the tactical network architecture and Common Operating Environments; and (3) transparent global NetOps. The strategic backbone of this plan is the Network Service Centers (NSCs) and the Army Data Framework. This structural element will enable the force to access information, to provide C2, to maintain situational awareness and to collaborate through all phases of joint operations. NSCs give land forces a networked expeditionary capability regardless of where they are in the ARFORGEN cycle or their component.

LOE 2: LandWarNet Capability Sets

(U//FOUO) The LandWarNet Capability Set Framework allows the Army to incrementally deliver capability sets over time, aligned with the ARFORGEN process, which incrementally modernize the Army with both Network and Mission Command capabilities over time. This process allows the Army to manage delivery of network/mission command capabilities within resources, and provide the best possible

capabilities to deploying forces. The two-year increment process also provides for frequent technical insertions as technologies mature.

LOE 3: Develop a Common Operating Environment (COE)

(U//FOUO) The Common Operating Environment Architecture is a key part of the broader enterprise network architecture. Over time, the Army will make decisions that implement a single common environment, which will facilitate the overall enterprise from an acquisition and network operations perspective.

Current Army Network Modernization Strategy Impacts on Gaps

(U//FOUO) As written, the Army's Network Modernization Strategy will eventually mitigate the following gaps to an acceptable level: "Establish, Operate, and Maintain an Enterprise Network" (Gap 11), "Single System and User ID" (Gap 17), "Integrate CyNetOps with Mission Partners" (Gap 19), "Network Defense in Depth" (Gap 20), and "Access to Critical Network Information, Services, and Applications" (Gap 24).

Specific Recommended Modifications to GNE Implementation and LandWarNet Capability Sets

(U//FOUO) This solution further modifies the LandWarNet capability set framework to provide additional C/EM capabilities to the force. This will be accomplished by modifying the Network Enabled Mission Command ICD and the LandWarNet ICD. IEWS capabilities desired and as described in the Joint EW ICD, Annex K, will mitigate the gaps in the ANMS. Recommended modifications include:

- Develop applications to allow for the planning, integration, and synchronization of C/EM capabilities (02 C/EM Integrating Entity).

- Increase the number of sensors on the network to conduct dynamic information collection, asset management, and defensive and offensive C/EM. Establish an integrated (enterprise/ transport to host) intrusion detection/prevention sensor grid that extends from the maneuver battalions to USCYBERCOM, can be tailored based on the operational environment, and provide situational awareness in a JIIM environment when required. Provide sensors which are able to dynamically detect low powered jammers. This approach could include modifications to programs such as Prophet, Pistol/Stingray, RC-12 Guardrail and Counter Remote control improvised explosive device Electronic Warfare (CREW); and Joint programs such as Joint Tactical Radio System (JTRS), Prowler/Growler, and Compass Call. (20 Defense in Depth, 29 Organic BDE C/EM Collect and Exploit Intelligence, 32 Conduct Cyber attack, 37 EA Asset De-confliction, 45 Conduct Electronic Attack, and Gap 50 Detect Jamming).

- Provide for platforms and delivery systems (ground and air) to enable C/EM attack (32 Cyber Attack, 45 Conduct EA). This could include modification of existing programs such as Prophet, various unmanned aerial systems, and selected ground platforms).

- Display friendly and adversary C/EM sensor, tool, and device information on the COP This can be achieved though a modification of LandWarNet related applications on Command Post of the Future (CPOF), Battle Command Systems (BCS3), Distributed Common Ground System-Army (DCGS-A), Advanced Field Artillery Tactical Data System (AFATDS), and Force XXI Battle Command Brigade and Below (FBCB2). (40 C/EM Situational Awareness, Common Operational Picture).

- Provide spectrum management capability to dynamically and automatically manage, plan, and use the EMS. This can be achieved by modifying programs such as the Global Electromagnetic Spectrum Information System (GEMSIS) family, Coalition Joint Spectrum Management Planning Tool (CJSMPT), SPXXI Online, SPEED, S2AS, JTRS and JSDR. (51 Dynamic Spectrum Management, 53 EMS Use Plan Export, 54 Spectrum Use Prioritization).

- Posture the network to support individual and platform defense by enabling the rapid identification of C/EM threats to networks, systems, platforms (Ground, Air, and Space), and enabling effective collective and individual countermeasures. This gap can be mitigated by modifying CREW, Aircraft Survivability Equipment (ASE) IEWS capabilities to mitigate the gaps in the ANMS. (57 Defend/Protect Individuals and Platforms).

- Develop and install transport solutions that support bandwidth requirements IAW both GAO and RAND bandwidth studies. Provide aerial solutions in order to establish communications relays. This could include providing technology upgrades to existing programs such as Warfighter Information Network-Tactical (WIN-T); and providing air vehicles with aerial nodes to Shadow platoons (BCT networks) and Extended Range Multi-Purpose (ERMP) systems (Corps/Division networks) to provide more capable/scalable aerial extension and cross-linking capability (Gap 11).

- Develop an adaptive access framework that enables all communications devices to continually maintain connectivity across all required security levels without reconfiguration or continued authentication as the device moves through all phases of the operation and anywhere in the area of operations (Gap 11).

- Develop and implement an identity management solution that provides for universal credentialing, and secure authentication services for users and systems across all required classification levels (Gap 17).

- Develop and implement a solution to discover (reactively and proactively) information that can be tagged, filtered, verified, used, and rated (Gap 24).

- Develop and implement a solution that enables commanders to set priorities for information flow and network use in order to enable quality, dynamic, and flexible information sharing between authorized users, in accordance with enterprise and mission-specific policies (Gap 24).

- Develop and implement a cross-domain solution that enables the timely exchange of information across all security classifications and with mission partners (Gap 11).

- Establish integrity mechanisms from end-to-end that protect user/system data, system configuration information, cryptographic integrity on published information, and mechanisms to ensure integrity of metadata management infrastructure (Gap 20).

- Conduct follow on analysis of current Program Executive Officer / Program Manager (PEO/PM) structure to determine the most appropriate structure for C/EM. (Gap 61)

Rationale (U//FOUO) This solution integrates C/EM requirements into overall network requirement development, thus delivering the Army a truly integrated material approach to most facets of C/EM. The incremental network modernization approach must be broadly applied, in accordance with the 2010 Army Network Modernization Strategy, to ensure all future capabilities are brought to bear when needed.

Cost (U//FOUO) By leveraging the existing Network Modernization Strategy these improvements can be realized through existing funding. However, the delivery of these capabilities within the overall LandWarNet capability set framework must be carefully prioritized and sequenced. This recommended solution adds complexity to the existing network integration process.

M02 – Providing Cyber Attack unique delivery systems and payloads in a timely manner

Description (U//FOUO) This proposed solution leverages QRCs to provide delivery systems and payloads to Brigade and above units to quickly deny, disrupt, neutralize, or degrade enemy capabilities through cyber attacks. Current cyber attack capabilities are developed for specific missions and may not be sufficient to support future missions. Future tools will be mission specific due to the dynamic nature of cyber. Due to the highly specific nature of these tools, gaps will continue to require materiel solutions to mitigate new cyber threats. To mitigate future risks to an acceptable level the Army must develop delivery systems which may or may not be outside LandWarNet (personnel, World Wide Web, web pages) to provide cyber attack capabilities. By

creating QRCs in a timely manner to meet specific operational and tactical requirements the Army can mitigate threats. This can be achieved by developing QRCs that provide the payloads for conducting cyber attacks. INSCOM currently maintains QRC capabilities (see Classified Materiel Annex) which support INSCOMs cyber missions and thru ARCYBER the Army can gain access to these capabilities for operational and tactical unit use. This solution partially mitigates Gap 32 Cyber Attack.

Rationale (U//FOUO) Brigades/BCTs and above organizations require quick turnaround of Cyber War systems to enable the capability to execute C/EM offensive actions by operational units. Commanders require access to cyber war capabilities to effectively operate in the Cyber domain.

Cost (U//FOUO) Cost would be higher than current cost due to the need of potentially intensive software, hardware, and system modifications to expand current capabilities to meet future threats. RDTE and OMA funding to support development of Army offensive cyberspace operations capabilities will be derived from multiple sources including HQDA, COCOMS, Joint Staff, other services and other governmental agencies. Rationale: For clarity purposes, funds are derived from various agencies. No additional funds are required to implement already approved lifecycle upgrades.

M03 – Maintain currency of tools for threat hardware and software exploitation and vulnerability assessments

Description (U//FOUO) Maintain currency of the development and construction of QRC solutions to create systems and tools to perform adversary hardware and software exploitation and friendly network vulnerability assessments. These are niche solutions that will continue to evolve due to quickly adapting threats. This solution helps to solve Gap 33 Threat Hardware and Software Analysis and Gap 36 Cyber Vulnerability Assessment.

Rationale (U//FOUO) Brigades/BCTs and above organizations require the capability to quickly deconstruct and analyze threat hardware and software in a deployed/conflict environment before latest time information of value (LTIOV). The Army needs to maintain currency of QRC solutions in order to rapidly analyze threat hardware and software and vulnerability testing to minimize threats to C/EM systems and tools. The QRC process to develop these tools requires the capability to be adaptable and flexible to meet the necessary time, quality, and quantity needs of the operational force. QRC's which are developed to exploit threat hardware and software need to have the capability to be versatile and adaptable to future threats to provide adversary systems deconstruction. Units also require the capability to identify emerging vulnerabilities in order to provide friendly systems vulnerability assessments to the user. These QRCs require the capability to quickly and effectively analyze cyber threats to the network by dynamically identifying malicious and non-malicious actions. Current POR LandWarNet systems that conduct these functions cannot keep pace with the fast changing threat

Cost (U//FOUO) Cost would be equal to current cost to maintain the RDT&E and RDA processes in place to continue software, hardware, and system modifications to detect and meet current adversary capabilities and identify friendly vulnerabilities. No additional funds are required to implement already approved lifecycle upgrades.

M04 – C/EM Modeling and Simulation

Description (U//FOUO) This solution leverages the TRADOC Modeling and Simulation (M&S) strategy to fully incorporate C/EM considerations into Modeling and Simulations. The TRADOC M&S Strategic Plan will enable the proper replication of the C/EM environment and threats in models and simulations supporting training, leader development and education, analysis, and capability development efforts.

The TRADOC M&S Strategy includes:

- Identifying, integrating, and prioritizing key M&S requirements, gaps, and solutions
- Planning, programming and resourcing key M&S efforts and priorities
- Increasing interoperability, reuse, and efficiency of M&S tools, services, and data across TRADOC
- Fostering collaboration internal and external to the TRADOC M&S community
- Facilitating the development of TRADOC M&S standards, policies, and procedures

This solution modifies the TRADOC Strategy to address C/EM replication across all four categories of models (leader development and education, analysis, doctrine, and capabilities development). This will mitigate Gap 46 – C/EM Modeling and Simulation.

Rationale (U//FOUO) The Army faces several challenges in standardization and use of models and simulations. Army M&S was developed to recreate a Cold War adversary focused on the kinetic, force-on-force fight and does not adequately reflect the current or future operational environment.

- (U//FOUO) Training M&S must be modified to provide the appropriate C/EM aspects of the operational environment for both individual and collective training requirements. These C/EM aspects must be fully incorporated into M&S capabilities for Live, Virtual, and Constructive training including CTCs. Incorporating these M&S systems into the CTCs will effectively simulate FSO, better preparing Soldiers for known enemy TTPs they will encounter in the future. CTCs will need current systems (hardware) and software consistent with what is being used in the field and on deployments. For example, systems such as CENTRIX-I, DCGS-A, and radio systems must all be the same models (hardware) and same versions (software) in order for the training to be most effective. This operational data is required to train individual and collective tasks at all echelons.

- (U//FOUO) In a similar fashion, Leader Development & Education M&S must also be modified to increase leader cognizance and competence for C/EM aspects of the operational environment: Systems which model the network and the EMS need to provide a sufficient amount of C/EM related data to staff officers to enable commanders to make effective decisions.

- (U//FOUO) Analysis M&S requires adjustment to properly replicate both environmental and threat aspect of C/EM. This includes replication of highly networked human societies, and adaptive hybrid threats using C/EM in conjunction with other capabilities.

- (U//FOUO) Capability Development M&S also requires adjustment to properly replicate both environmental and threat aspect of C/EM. This includes replication of highly networked human societies, and adaptive hybrid threats using C/EM in conjunction with other capabilities. As new technologies and adversary TTPs are identified, an integrated M&S capability to accurately replicate them is essential for system and force design.

Cost (U//FOUO) Cost would be no higher than current cost of model and simulating process in place today. No additional funds are required to implement already approved lifecycle upgrades.

M05 – Defend and Protect Individuals and Platforms

Description: (U//FOUO) This solution leverages the current Army Network Modernization Strategy and the existing array of protection/survivability requirements documents to provide for adaptive and readily reconfigurable C/EM protection of individual Soldiers and platforms. This will be accomplished by modifying the Network Enabled Mission Command ICD and the LandWarNet ICD, and Soldier/platform specific requirements documents. Future IEWS CDDs will require networked EW capabilities which support this gap mitigation strategy. Recommended modifications include:

- Modifying individual Soldier and platform defensive suites to fully leverage C/EM capabilities for protection.
- Provide communication links to enable both situation awareness (itself a key contributor to survivability) and collective/cooperative defense
- Employ multi-function devices which perform both communication and protective functions while minimizing ‘size, weight, and power (SWaP)’ requirements
- Provide a readily re-configurable hardware ‘infrastructure’ that accommodates dynamic adaptation of software to counter newly identified C/EM threats

(U//FOUO) Protection is a combination of individual and collective measures; of technologies and TTPs. LandWarNet must be designed to provide a degree of cyber protection to individuals and platforms, but also to enable individual and collective

defensive suites. Threat warning systems need to cue systems which can detect and neutralize adversary capabilities. Data links must provide SA for the commanders and units using EW to limit EMS fratricide and facilitate cooperative defense between units.

(U//FOUO) This solution will ensure the proper integration of individual and collective protective systems leveraging network, IEWS, and platform-specific countermeasure suites. The solution addresses both cyber and EMS threats. In general, protective systems require the capability to communicate with other systems to provide situation awareness, de-conflict spectrum use, and provide protection. This solution, implemented over time, will allow defensive suites to effectively use the EMS, integrate with offensive systems, and meet size, weight, and power limitations. These defensive suites must cooperatively enable friendly communications and jam adversaries. This approach could include modifications to existing programs such as the emerging IEWS system, CREW, and Soldier/platform defensive suites (e.g. aircraft survivability equipment) to completely integrate with LandWarNet.

(U//FOUO) The Army requires systems which are dynamically adaptable to current and emerging C/EM threats. These systems require the capability to have independent peripherals to allow hardware and software exchange which provides communications and efficient, distributed, cooperative jamming depending on the threat. This will solve the Defend/Protect Individuals and Platforms (Ground, Air, and Space) (Gap 57).

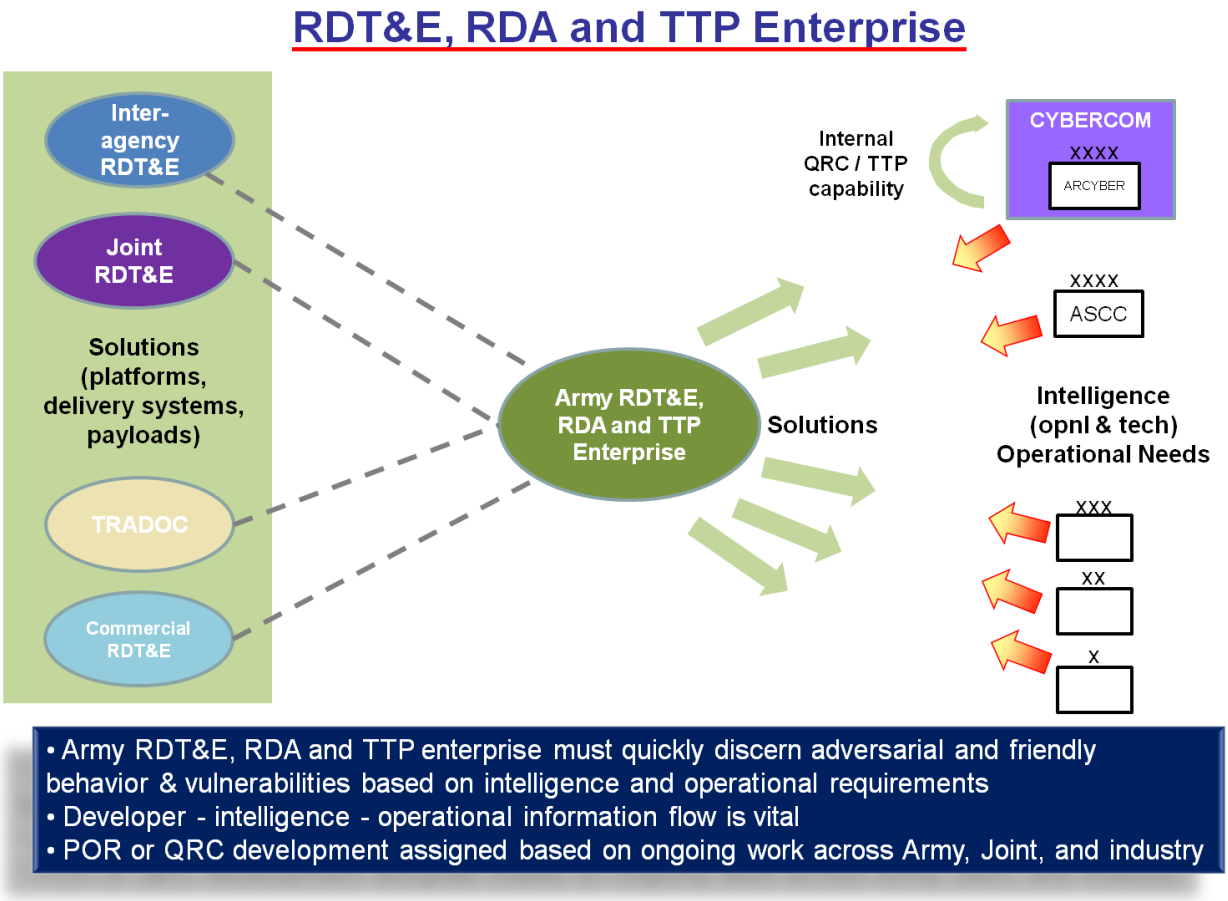
Rationale (U//FOUO) In recent conflicts personnel and platforms faced attacks initiated within the electromagnetic spectrum (remote controlled IEDs). The Army provided defensive electronic countermeasures in CREW systems as part of the response to these threats. In reaction, the threat adapted by changing its TTPs. Army systems meant to defeat one threat did not defeat another and the resources and manpower needed to develop these countermeasures were staggering but necessary to defend Soldiers. Therefore repeated fielding of new devices were necessary – a very expensive and slow process. Moreover, the future threat includes cyber threats, which a sophisticated adversary will employ in combination with more traditional EMS threats. An enabling capability within the LandWarNet ICD is survivability against threats; cyberspace, electromagnetic, and physical. In the Net Enabled Mission Command's ICD it identifies threats which must be overcome, by providing the ability to counter adaptive, hybrid enemies and adversaries as well as conventional enemies operating within all operational domains. Also to provide protection from threats to deny, degrade, and destroy U.S. communications in the EMS.

Cost (U//FOUO) By leveraging the existing Network Modernization Strategy and other existing programs of record, these improvements can be realized through existing funding. However, the delivery of these capabilities within the overall modernization framework must be carefully prioritized and sequenced. This recommended solution adds complexity to the existing network integration process.

M06 – C/EM Research, Development, Testing and Evaluation (RDT&E), Research, Development and Acquisition (RDA), and Tactics, Techniques, Procedures (TTP) Enterprise

Description (U//FOUO) This solution establishes an agile RDT&E and RDA enterprise with close links to the institutional and operational force that provides timely materiel POR and QRC solutions, with TTPs. This will be accomplished by improving existing communications between the operational force, the intelligence community, TRADOC, Army RDT&E organizations, Army RDA organizations, and external RDT&E and RDA organizations to better accounted for a converged C/EM environment and sophisticated threats. Recommended modifications include:

- Establishing shared awareness of ongoing development efforts inside and outside the Army
- Link the operational force (intelligence and operational needs) to developers and requirement managers (e.g. ARCYBER, TRADOC) in order to rapidly discern adversarial and friendly behaviors and vulnerabilities
- Rapidly incorporate emerging requirements into existing materiel requirements and strategies (e.g. existing network requirements and LANDWARNET capability sets)
- Provide clear points of entry for RDT&E, RDA and TTP support
- Establishing an acquisition process which provides a layered approach, maintaining the JCIDS process for larger development two years and up, rapid equipment fielding efforts for months to a year, and a QRC based rapid capability for days to week needs.
- Establish clear boundaries, priorities, and acquisition s authorizes to reduce duplicate efforts and bureaucracy.
- Limit the steps involved to provide tools in a timely manner.
- Provide a process which will link the Warfighter to the acquisition community to communicate the ground truth of the requirements.
- Incorporate academia, commercial, industry, inter governmental, and agencies in to the process and provide them with early engagement, CBA processes, up to date information, and field requirements.
- Link acquisition culture into the operational forces to ensure personnel understand the requirements. This will give GENFOR personnel a better understand of the timely need to provide solutions to the user.
- Provide a PEO and PM C/EM integration charter across the PEO elements with personnel who have the proper clearances to work in C/EM activities.



(U//FOUO) Figure 7: RDT&E and RDA Enterprise

(U//FOUO) C/EM operational requirements will occur in a very dynamic fashion across all echelons of the operational force (BCT thru ARCYBER). These requirements will emerge based on assessments coming from both intelligence and operations channels. In order to maintain the appropriate operational advantages, an intense collaboration between intelligence, operations, and GENFOR (e.g. CERDEC, TRADOC, PEO IEWS, PEO C3T) RDT&E and RDA agencies will be required. This collaboration of the operational force and GENFOR RDT&E and RDA organizations can assist in the deployment and fielding of materiel solutions in combination with effective TTPs. This will bring together the operating and generating forces to best respond to operational requirements.

(U//FOUO) Within the RDT&E and RDA community itself, collaboration must occur between Joint, interagency, academia, and commercial/industry agencies. Internal to the Army, ARCYBER has capability to conduct limited C/EM RDT&E and RDA and when needed, must request support from other organizations like RDA ASA ALT PEOs. By creating a database of C/EM QRC's the Army will reduce redundancy and provide a repository of solutions. The RDT&E and RDA Enterprise incorporating collaboration and solution databases will result in better responsiveness to a changing adversary.

This RDT&E and RDA community must be closely linked to the appropriate C/EM-related proponent organizations to generate TTPs for employment of said materiel solutions. This solution is linked to solutions M01, Pursue a modified Army Network Modernization Strategy (ANMS), M02 – Providing Cyber Attack unique delivery systems and payloads in a timely manner, M03 – Maintain currency of tools for threat hardware and software exploitation and vulnerability assessments, and M05 – Defend and Protect Individuals and Platforms. This solution most directly addresses Gap 61 Research, Development, Testing and Evaluation and Research, Development and Acquisition.

Rationale (U//FOUO) This RDT&E, RDA, and TTP enterprise will facilitate the flow of threat, TTP and adversary information from the operating force to the generating force. The enterprise must have a clear process and accessible points of entry for units to submit emerging threats. The enterprise must also allow for units to pass information on new emerging friendly capabilities and requirements e.g., network, sensors, or application limitations to higher. Through a system or tool in the enterprise network units will have the capability to pass the details of emerging threats and friendly requirements to higher organizations and have access to components of the generating force which could best address it.

This process should allow for units to identify the importance of the requirement and enable them to know if the requirements should be passed to higher echelons or taken directly to the generating force. This will facilitate the flow of information and enable collaboration of SME and development capabilities. Countermeasures developed in the field could also be passed to the generating force through this process to ensure quick RTD&E and RDA and distribution throughout the Army. The Rhino used as a CIED device during Operation Iraqi Freedom is an example of a materiel solution developed in the field which was effectively developed through RDT&E and RDA and then accepted throughout the Army.

Cost (U//FOUO) The primary costs associated with this solutions are those funds needed to improve the process of collaboration and generate shared awareness.

2-5 Leadership & Education

Introduction

(U//FOUO) Army leaders lack an in-depth understanding of how to integrate C/EM capabilities into FSO in order to create the desired effect. Leaders must be able to fight and win wars in and through cyberspace. They must be able to understand the C/EM contest and plan for the use of the C/EM dimension as a source of operational advantage. Leaders must be able to holistically and adequately understand the operational significance of the network to mission success; what roles/responsibilities exist in reference to the establishment, operation, and defense of the network; how to fight in and through a degraded network environment, and how to identify, attack, exploit, and defeat expanding C/EM threats. C/EM is not included in current funded and integrated Electronic Warfare Leadership and Education programs. These programs must be updated in order to create the training and education conditions that produce the leadership and education developmental outcomes required for the application of cyber capabilities in FSO.

FSA Methodology for Developing Leadership and Education Solutions

(U//FOUO) The FNA identified 17 gaps as having Leadership and Education aspects. The C/EM CBA Team conducted a series of working groups, teleconferences and workshops which culminated in FSA Workshop #3 where 20 SMEs discussed possible Leadership and Education solutions for the identified gaps.

FNA Gaps with Leadership & Education Aspects

C/EM Integrating Entity (Gap 02)
Establish, Operate, Manage Enterprise Network (Gap 11)
Transition Network C2 (Gap 15)
Integrate CyNetOps with Mission Partners (Gap 19)
Access Critical Network Info, Services, & Applications (Gap 24)
Non-Attributed Network (Gap 26)
Dynamic Cyber Defense (Gap 28)
Cyber Attack (Gap 32)
Threat Hardware & Software Analysis (Gap 33)
Cyber Vulnerability Assess & Operational Testing (Gap 36)
EA Asset Deconfliction (Gap 37)
Cyber Threat Investigation Information Sharing (Gap 38)
C/EM Situational Awareness, COP (Gap 40)
Conduct Electronic Attack (Gap 45)
C/EM Modeling and Simulation (Gap 46)
Spectrum Impact Analysis (Gap 52)
Defend / Protect Individuals and Platforms (Gap 57)

Identified Potential Solutions

L01 – Incorporate basic C/EM knowledge into the Officer Education System, Warrant Officer Education System, Noncommissioned Officer Education System, and Civilian Education System

Description (U//FOUO) Add a C/EM block of instruction in the common core section of every PME (Professional Military Education) course. TRADOC has already approved EW training for inclusion into BOLC-B and EW courses at ILE have been initiated. There are plans to integrate EW into the Senior Leader Courses, SAMS, OES, WOES, and NCOES schools. The Army should add C/EM objectives to the already approved and working EW Leadership and Education venues to include civilian education. (Gaps 02, 11, 15, 19, 24, 26, 28, 32, 33, 36, 37, 38, 40, 45, 46, 52, 57)

Rationale (U//FOUO) Soldiers, leaders and civilians provided basic C/EM knowledge will have the essential capabilities to execute required C/EM tasks. It is necessary for Soldiers, leaders, and civilians to have a fundamental understanding of available C/EM capabilities and effects. This solution is consistent with Army Leader Development Strategy (ALDS) Imperative 3: Prepare leaders for hybrid threats and full spectrum operations through outcomes-based training and education.

L02 – Incorporate additional specialized C/EM training into 14, 24, 25, 29, 30, 35, 40, and 53 series Professional Military Education (PME)

Description (U//FOUO) Provide 14, 24, 25, 29, 30, 35, 40, and 53 series Soldiers with basic, intermediate, and advanced C/EM training regarding how C/EM merge with their respective current roles and responsibilities. This will require a revision of the CMF 14, 24, 25, 29, 30, 35, 40, and 53 CATS and changes to current POIs. The 29-series training has already been enhanced to include spectrum management operations since there is a lack of 25Es (Spectrum Managers) in the Army. The Army should explore alternative methods to meet these requirements to provide more technical, hands on training during PME. Alternative methods could include civilian training venues (classroom and online) or combined training for Soldiers with different MOSs that perform similar C/EM missions. Another approach for C/EM PME enhancement is to develop a cross training method between cyber defense and cyber offense forces. Such modifications to current programs will enhance knowledge, skills, and abilities of the 14, 24, 25, 29, 30, 35, 40, and 53 series Soldier and better prepare them to integrate C/EM into FSO. (Gaps 02, 11, 15, 19, 24, 26, 28, 32, 33, 36, 37, 38, 40, 45, 46, 52, 57)

Rationale (U//FOUO) A robust C/EM training plan that covers friendly and adversary C/EM capabilities, applicable vulnerabilities, and concepts related to risk and employment decisions for 25, 29, and 35-series Soldiers will provide leaders with the essential decision-making capabilities to fully utilize and integrate C/EM capabilities into FSO.

Cost (U//FOUO) The addition of specialized training/tasks will cause a change in POIs that will generate costs.

L03 – Incorporate the C/EM Contest into leadership & education opportunities during training exercises

Description (U//FOUO) Integrate discussions and workshops on C/EM threats and countermeasures to leaders and staffs in BCTP seminars, MCTC Leader Training Programs, and in academic week prior to MRX execution. Commanders and Soldiers, especially G/S-6 Soldiers, need to understand mission command systems and the unit's portion of the network. Deployed units need to be able to perform critical functions in the absence of or with a decreased presence of civilian contractors and field support representatives. This is critical for mission command on the move or when operating on a tactical network removed from a FOB. In the past, EW MTTs have presented EW integration classes to unit leaders and staffs as part of MRX academics. These classes were delivered at Bde, Div, and Corps level exercises. The Army should continue to present these classes during MRX academics and include C/EM objectives in the presentations. (Gaps 02, 11, 15, 19, 24, 32, 33, 37, 38, 40, 45, 46, 52, 57)

Rationale (U//FOUO) Soldiers and leaders with the capability to adapt to and generate solutions for operational C/EM problem sets is an essential component to the successful application of the C/EM system. This solution is consistent with ALDS Imperative 6: Prepare our leaders by replicating the complexity of the operational environment in the classroom and at home station.

Residual Gap Assessment

(U//FOUO) The identified potential solutions will adequately mitigate C/EM leadership and education gaps; however these must be implemented in conjunction with other aspects of DOTMLPF to fully mitigate the gaps as a whole. Although GNEC addresses a range of gaps specifically related to an enterprise network, C/EM leadership and education developmental venues must account for the capabilities necessary for operations when these resources are not available such as operating in a degraded or denied networking environment. GNEC is not expected to be FOC until FY2018. Leadership and education represents the most feasible and suitable solution to address network related C/EM gaps until GNEC is FOC.

Cost

(U//FOUO) The cost of implementing the identified potential solutions is moderate and is comparable to the current approach.

2-6 Personnel

Introduction

(U//FOUO) The Cyber/Electromagnetic (C/EM) Contest is a "Total Force" matter, fully involving the generating force, the operational force, active component, reserve component, and government civilian personnel across Intelligence, Operational, and Signal specialties. In many cases, the Army lacks the right personnel, with the right knowledge, skills, and abilities to conduct the C/EM Contest. Currently the Army must adapt in order to acquire, develop, and sustain specific skill sets and expertise required to conduct C/EM activities. This also requires that the appropriate certifications and clearances are made available for specific billets in order to validate knowledge and share information.

FSA Methodology for Developing Personnel Solutions

(U//FOUO) During the FNA, 12 gaps were identified with personnel aspects. The C/EM CBA Team conducted a series of working groups, teleconferences and workshops which culminated in FSA Workshop #3 with 20 identified subject matter experts that assisted in the development of an 'expertise map' which describes critical expertise and skill requirements across echelons. This map consisted of a set of defined expertise levels (Common Soldier, Civilian, or Contractor; Apprentice; Journeyman; Master; and Guild) and skill sets with associated tasks to perform C/EM related activities related to echelons/formations. The personnel-related gaps were then applied by echelon/formation to develop an 'expertise gap map'. The C/EM community then assisted in identifying solutions which addressed these gaps across echelons.

FNA Gaps with Personnel Aspects

- (U//FOUO) Cyber/Electromagnetic Integrating Entity (Gap 02): The company level lacks sufficient expertise to request C/EM capabilities resident at higher echelons. For battalion level and above, staffs lack the full range of expertise to plan and integrate all aspects of the C/EM contest (situation awareness, offense, defense, and support), and the necessary 'practitioner' expertise to perform the C/EM tasks that they must execute. We expect companies to execute information security and operations security awareness; and tactical level planning and execution.
- (U//FOUO) Access (Gap 04): Functional Brigades lack sufficient practitioner expertise to respond to tactical level mission requirements.
- (U//FOUO) Network Defense in Depth (Gap 20): Army lacks NetOps personnel (officer/enlisted/civilian) with tracked cyber defense training, assignments that prevent the loss of perishable cyber defense skills (especially while in a garrison environment), and enduring cradle-to-grave cyber defense career path. Additionally, the Army lacks NetOps personnel with the right clearances/skill sets to effectively protect against, monitor for, detect, analyze, and respond to

unauthorized activity on Army networks, with the exception of the 255S Warrant Officers.

- (U//FOUO) Cyber War Network Support (Gap 26): ARCYBER lacks practitioners (C/EM savvy staff) to conduct C/EM operations.
- (U//FOUO) Organic Brigade C/EM Collect and Exploit Intelligence (Gap 29): Brigades lack the personnel required to plan, collect and develop C/EM intelligence for use in exploiting adversaries.
- (U//FOUO) Cyber Attack (Gap 32): Brigade and above lacks the specialized personnel to perform and conduct cyber warfare
- (U//FOUO) Threat Hardware and Software Analysis (Gap 33): The Army lacks experienced personnel that are sufficiently educated and trained to execute C/EM reverse engineering and forensic capabilities that can deconstruct and analyze threat hardware and software. Division and higher echelons lack personnel that know how to access Army and Joint reverse engineering and forensic support elements and cannot themselves execute digital media collection and limited analysis in a forensically sound manner.
- (U//FOUO) Cyber Vulnerability Assessment and Operational Testing (Gap 36): S2 and S6 personnel have limited expertise in analyzing Cyber threats and identifying threat specific vulnerabilities in the operational environment.
- (U//FOUO) EA Asset Deconfliction (Gap 37): Brigades lack trained personnel with the right skill sets to perform dynamic deconfliction. This process must consider: (1) Intelligence gain versus loss; (2) spectrum fratricide; (3) mission priorities; (4) risk management and risk acceptance; (5) mitigation strategies, all of which cut across EW, EM, EMSO and CyberOps.
- (U//FOUO) Dynamic Spectrum Management (Gap 51): Battalions lack 25E spectrum managers
- (U//FOUO) EMS Use Plan Export (Gap 53): Battalions lack 25E spectrum managers
- (U//FOUO) Research, Development and Acquisition and Research, Development and Acquisition (Gap 61): GENFOR lacks sufficient civilian or contractor personnel with the technical expertise necessary to conduct C/EM RDT&E and RDA.

C/EM Expertise Map

(U//FOUO) The study team developed the C/EM expertise map to identify both the type of skills and level of expertise required at each echelon. It was developed by defining each C/EM skill set, to include what tasks are associated with these skills, and then identifying at what echelons the skill sets and tasks should be performed. Any special requirements were identified as well. These expertise levels were then applied to the skill sets required by echelon resulting in the expertise map indicating tasks against specific experience levels are performed by echelon. The next two sections define the skill sets and expertise levels used to develop the expertise map.

Skill Sets, Associated Tasks & Duty Positions

(U//FOUO) This section outlines the 11 C/EM skill set areas for personnel. Each skill set area is defined and includes associated tasks. Some skill sets also include possible duty positions.

Establish and Operate the Network (U//FOUO) Establish and Operate the Network is the set of skills required install, secure, operate, manage, administer, optimize, and restore communications networks, information systems, and/or applicable applications that comprise the LWN. Currently all Signal personnel (25 officer/24A/53A/25X warrant/25 enlisted) perform the associated tasks related to establishing and operating the network. Additionally, 35T (MI Systems Maintainer/Integrator) establish and operate classified intelligence networks. The Army must also provide information services to assure warfighters' awareness of relevant, accurate information, access to newly revealed or recurring information, and timely and efficient delivery of information in a usable format.

- (U//FOUO) Plan, engineer, and establish network transport
- (U//FOUO) Install, operate, and provide network infrastructure
- (U//FOUO) Maintain the network
- (U//FOUO) Administer information systems and databases
- (U//FOUO) Collect and analyze friendly network C/EM data, capabilities, vulnerabilities, and intentions

Provide Information Services and Integrated NetOps Capabilities are subsets of Establish and Operate the Network.

Provide Information Services – Provide Information Services is the set of skills required to assure warfighters' awareness of relevant, accurate information; access to newly revealed or recurring information; and timely and efficient delivery of information in a usable format. Currently 53A, 255A, and many 25-series enlisted (B/C/M/R/U/V/Z) perform most of the associated tasks related to providing information services.

- Provide Technical Support to End User
- Manage Content
- Administer Database
- Develop Applications

Integrated NetOps Capabilities – Integrate NetOps Capabilities is the set of skills required to plan, engineer, and direct the operation, administration, maintenance, and provisioning, of communications networks and information services in order to assure network/system availability, information protection, and information delivery. Currently 25A, 24A, 53A, 255A, 255N, 255Z, and many 25-series enlisted (E/R/W/X/Z) perform most of the associated tasks related to defending the network.

- Manage Integrated Network Operations Activities

- Plan and Engineer Network and Services

Defend the Network (U//FOUO) Defend the Network is the set of skills required to protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication, and non-repudiation. Currently 25A/24A/53A/255S/25B/25N perform most of the associated tasks related to defending the network. Additionally, 35T (MI Systems Maintainer/Integrator) defend and sustain classified intelligence networks.

- (U//FOUO) Provide Network Defense Infrastructure
- (U//FOUO) Analyze Anomalous Network Activity
- (U//FOUO) Determine Response to Cyber Incidents
- (U//FOUO) Assess Security of Systems and Networks
- (U//FOUO) Oversee Network Defense Operations
- (U//FOUO) Conduct defensive C/EM capabilities and actions into the scheme of maneuver as part of the MC WfF

Vulnerability (U//FOUO) Vulnerability is the set of skills required to perform vulnerability testing on friendly, adversary and neutral actors in the C/EM contest. This includes actions such as identifying friendly vulnerabilities to improve defenses as well as identifying adversary vulnerabilities which may be exploited. Currently 25B (Information Technology Specialist) perform many of the associated tasks related to vulnerability testing. Additionally 35L (Counterintelligence Agent) in the Criminal Investigation Division provides electronic crime vulnerability assessments, IAVA step 3 support to network testing, as well as digital media collection, analysis and investigations. Also 35T (MI Systems Maintainer/Integrator) perform forensically sound digital media collection and limited analysis in support of site exploitation and subsequent investigations. Finally, 35N (Signals Intelligence Analyst) perform vulnerability analysis of threats via various reconnaissance and collection missions.

- (U//FOUO) Vulnerability assessment
- (U//FOUO) Vulnerability/security remediation
- (U//FOUO) Cyber aspects of site exploitation
- (U//FOUO) Counterintelligence

Forensics & Reverse Engineering Coordination (U//FOUO) Forensics is the set of skills related to collection and analytic investigation of an information system or network with the goal of illuminating hidden events, normally of a malicious nature, or to reveal the nature and manner that system or network operates. It encompasses any systematic analysis aimed at discovering features in, understanding aspects of, or revealing hidden parameters, and recovering evidence from digital media, electronic devices and computer networks. Duty positions for forensics include hardware/software reverse engineers and digital media forensic examiners. Currently 35N (SIGINT Analyst), 25B (Information Technology Specialist), 35T (MI Systems Maintainer/Integrator), and 35L (Counterintelligence Agent) perform coordination with forensics and reverse engineering

assets. Additionally, and in small numbers, these same MOSs perform various aspects of collection, analysis, or investigation commensurate with their organizational mission charter, authorities, and certified skill level.

- (U//FOUO) Access C/EM forensics investigations and reverse engineering to request assistance, provide and share data, and to ultimately determine malicious event attribution in the assistance of subsequent litigation, mitigation, and operational response decisions.

Spectrum Management (U//FOUO) Spectrum Management is the set of skills required to understand, plan, manage and deconflict the use of the electromagnetic spectrum. 25E currently perform spectrum management. Additionally, 35N (Signals Intelligence Analyst) provide to the spectrum manager the threat "red picture" portion of the spectrum.

- (U//FOUO) Determine spectrum requirements

Offensive C/EM and Dynamic Cyber Defense (U//FOUO) Offensive C/EM and Dynamic Cyber Defense is the set of skills required to conduct both offensive and dynamic defensive actions in and through cyberspace and the electromagnetic spectrum. Duty positions for Offensive C/EM and Dynamic Cyber Defense include attack and exploit positions. Offensive C/EM and Dynamic Cyber defense is performed by several MOSs including 25-series, 29-series, and 35-series.

- (U//FOUO) Conduct offensive C/EM actions into the scheme of maneuver as part of the MC WfF
- (U//FOUO) Plan C/EM responses
- (U//FOUO) Execute cyber exploitation (By law, these tasks cannot be performed by contractors)
- (U//FOUO) Execute cyber attack (By law, these tasks cannot be performed by contractors)
- (U//FOUO) Execute ES (Electronic Warfare Support)
- (U//FOUO) Execute EA (Electronic Attack)
- (U//FOUO) Execute EP (Electronic Protection)
- (U//FOUO) Plan and execute Dynamic Cyber Defense
- (U//FOUO) Engineer and install Cyber War Network
- (U//FOUO) Gain and maintain access to the enemy's network

C/EM Intelligence (U//FOUO) C/EM Intelligence is the set of skills required to collect, identify, assess and analyze adversary and neutral actors C/EM capabilities, threats, indications, warnings and trends. Duty positions for intelligence include C/EM threat analyst. Currently the 35-series and 352N (Traffic Analysis Technician) perform intelligence.

- (U//FOUO) Assess adversary and neutral C/EM capabilities, vulnerabilities, and intentions
- (U//FOUO) Collect and analyze adversary C/EM network systems and data
- (U//FOUO) Study the C/EM threat
- (U//FOUO) Provide C/EM trends, indications, and warnings

Cryptography (U//FOUO) Cryptography is the set of SIGINT and Counterintelligence skills and specific organizational charters and authorities required to properly construct and deconstruct highly technical encryption methods aimed at preventing the loss or transfer of data from information systems to unknown or unwanted parties. This is currently performed by 35N (SIGINT Analyst), 35G (Imagery Analyst) and 352N (Traffic Analysis Technician).

- (U//FOUO) Cryptography

Linguistics (U//FOUO) The linguist performs detection, acquisition, location, identification, and exploitation of foreign communications. Translates, transcribes, gists or produces summaries of foreign language transmissions in English/target languages. Linguistics is currently performed by 35P (Cryptologic Linguist).

- (U//FOUO) Linguistics

Synchronize and Integrate (U//FOUO) Integration is the set of skills required to staff, integrate, plan, synchronize, coordinate and facilitate C/EM capabilities to provide commanders a holistic view of the C/EM contest, through S/G2 and S/G3 channels. This includes the fusion of friendly, adversarial and other specified C/EM situational awareness into a single, coherent picture to support the commander's decision making process. This is currently partially being accomplished by disparate staff elements. Currently, portions of this skill set are being performed by series 25, 29, and 35 personnel.

- (U//FOUO) Understand relevant activity in and through cyberspace/EMS (C/EM SA)
- (U//FOUO) Understand information flow over network including purpose/criticality
- (U//FOUO) Understand effects and mission impact resulting from friendly and adversary C/EM operations
- (U//FOUO) Integrate and coordinate the employment of the full range of C/EM capabilities
- (U//FOUO) Plan, synchronize, request, and integrate offensive and defensive C/EM capabilities and actions into the scheme of maneuver as part of the MC WfF
- (U//FOUO) Enable C/EM vertical and horizontal integration and synchronization of operations across the WfF
- (U//FOUO) Synchronize operations with space, high altitude, cyber airborne and electromagnetic capabilities

- (U//FOUO) Support Inform & Influence Activities (IIA)
- (U//FOUO) Coordinate with forensics, law enforcement, counterintelligence and reverse engineering resources
- (U//FOUO) Collect, aggregate, and analyze; present analysis for Commander's decision making process

Acquisition (U//FOUO) Acquisition is the set of skills required to enable the right people to provide integrated products and services at the right time in response to requests that provides a new, improved, or continuing materiel, weapon or information system, or service capability in response to an approved need. This includes research, development, testing and experimentation. Currently this is provided by a wide variety of military personnel, civilians, and contractors.

- (U//FOUO) C/EM Research, Development, Test, and Evaluation (RDT&E)
- (U//FOUO) C/EM Research, Development and Acquisition (RDA)
- (U//FOUO) C/EM Combat Development and Acquisition
- (U//FOUO) Develop and field material solutions to mitigate and defeat new and evolving capabilities

Expertise Levels Definitions

(U//FOUO) This section defines Expertise Levels. The levels include the Common Soldier, Civilian, or Contractor; Apprentice; Journeyman; Master; and Guild. The Level descriptions include training and skills personnel at each level should possess and suggested associated ranks.

Common Soldier/Civilian/Contractor

- (U//FOUO) General understanding of Cyberspace, the electromagnetic spectrum, and C/EM activities.
- (U//FOUO) Performs assigned duties, which may contribute to C/EM activities at times.
- (U//FOUO) Includes Soldiers with Additional Skill Identifiers (ASI) or special training e.g., master gunner.

Apprentice

- (U//FOUO) First assignment and specialty training that allows development of proficiency, up to three years of accumulative experience in related field
- (U//FOUO) Possible Equivalent Experience: E1-E4, 2LT-1LT, GS5-GS6, Industry junior level; to include those transitions that do not fit normal career progression
- (U//FOUO) Basic knowledge of concepts, practice, and procedures
- (U//FOUO) Certified at appropriate level

Journeyman

- (U//FOUO) Equivalent Experience: E5-E7, WO1-CW3, CPT-MAJ, GS7-GS11, Industry experienced professional, between three and seven years of accumulative experience in related field
- (U//FOUO) Two plus assignments in specialty, intermediate specialty training, current operational experience, up to date certifications and demonstrated qualifications
- (U//FOUO) Can perform staff work
- (U//FOUO) Conducts routine planning and integration in support of FSO
- (U//FOUO) Received basic and intermediate specialized training and basic leader development
- (U//FOUO) Mastery of Apprentice function; intermediate knowledge of concepts, practice, and procedures

Master

- (U//FOUO) Equivalent Experience: E7-E9, CW3-CW5, MAJ-COL, GS12-GS15, Industry highly skilled; seven years or more of accumulative experience in related field
- (U//FOUO) Expert in advanced knowledge concepts, practices and procedures
- (U//FOUO) Three plus assignments in specialty, advanced specialty training, current operational experience, up to date certifications and demonstrated qualifications
- (U//FOUO) Able to operate autonomously or lead planning and execution supporting FSO
- (U//FOUO) Can fully integrate, plan, and lead tasks within their area of specialty
- (U//FOUO) Received intermediate and advanced specialized training and leader development (JPME/ILE or higher level education)
- (U//FOUO) Certified at appropriate level

Guild

- (U//FOUO) Highly technical, specialized skilled individual; ten or more years of accumulative experience in related field
- (U//FOUO) Special management
- (U//FOUO) Broad range of knowledge; fully conversant in ‘cutting edge’ technologies and their innovative application
- (U//FOUO) Technical leader/opportunities vice traditional leader roles
- (U//FOUO) High demand/low density with perishable skills
- (U//FOUO) Can remain within strategic and national level organizations for life of career

- (U//FOUO) Professional with in-depth knowledge of C/EM, planning and execution of national strategy requirements
- (U//FOUO) Educated and certified at a level to be recognized as an expert in their field

How to Read the C/EM Expertise Map and C/EM Expertise Gap Map

(U//FOUO) The C/EM Expertise Map aligns skill sets by echelons. Within each cell, statements are made to indicate the required expertise level for that skill set for that particular echelon. Where appropriate, notes are used to highlight specific requirements. Color shading is used to denote the feasibility of military, civilian, or contractor sourcing of the expertise. As an example of how to read the C/EM Expertise Map; the skill set of defend the network requires an apprentice level expert at the battalion level.

(U//FOUO) The C/EM Expertise Gap Map also aligns skill sets by echelons, but focuses on 'missing' expertise. Within each cell, statements are made to indicate the 'missing' expertise level for that skill set for that particular echelon. Where appropriate, notes are used to highlight specific aspects of the requirements. Color shading is used to denote the feasibility of military, civilian, or contractor sourcing of the expertise. An example of how to read the C/EM Expertise Gap Map; the skill set of spectrum management requires and lacks an apprentice level expert at the battalion level.

C/EM EXPERTISE MAP

Skills	Company	BN	Bde/ BCT	DIV	Corps	ASCC	ARCYBER	GENFOR
Establish & Operate the Network	A	A	J	J, M	J, M	J, M	J, M, G	J, M, G
Defend the Network	A	A	J*	J*	J*, M*	J*, M*	J*, M*, G*	J, M, G
Vulnerability		A	J	J, M	J, M	J, M	J, M, G	M, G
Forensics & Reverse Engineering Coord			A, J	J, M	J, M	J, M	J, M, G	M, G
Spectrum Management	S	A	J	J, M	J, M	J, M	J, M	J, M
Offensive C/EM & Dynamic Cyber Defense	S	A	A, J	J, M	J, M	J, M	A*,J*, M*, G*	M, G
C/EM Intelligence	S, A	A	J	J, M	J, M	J, M	J, M	J, M
Cryptography			A, J	J	J, M	J, M	M, G	J, M
Linguistics**			A, J	J	J, M	J, M	J, M	
Synchronize & Integrate	S	A, J	J, M	J, M	J, M	J, M	M	J, M
Acquisition						J, M	J, M	J, M, G

(U//FOUO) Table 5: C/EM Expertise Map

**** These personnel require special career management and development through multiple progressively more difficult positions remaining within their specialty. These personnel have highly developed skills and are required to maintain strenuous proficiency and currency due to these skills being highly perishable.***
*****Personnel used to fill linguistics positions will most normally be civilian or contractor personnel with highly specialized language skills.***

S = Soldier
A = Apprentice
J = Journeyman
M = Master
G = Guild

Color Code	
White	Requires Military due to tactical level operations and deployment (Company thru Brigade) and/or Title X Offensive C/EM Operations (ARCYBER)
Yellow	Military or DA Civilians due to probably deployments
Green	Military, DA Civilians or Contractors

C/EM EXPERTISE GAP MAP

<table>
<tr><th>Skills</th><th>Company</th><th>BN</th><th>BDE/BCT</th><th>DIV</th><th>Corps</th><th>ASCC</th><th>ARCYBER</th><th>GENFOR</th></tr>
<tr><td>Defend the Network</td><td colspan="6"></td><td>J*, M*, G*</td><td></td></tr>
<tr><td></td><td colspan="8">At all echelons, the Army requires NetOps personnel (officer/enlisted/civilian) with cyber defense training, assignments that prevent loss of perishable cyber defense skills, proper clearance, and an enduring career path. Defense personnel must effectively protect against, monitor for, detect, analyze, and respond to unauthorized activity on Army networks.</td></tr>
<tr><td>Vulnerability</td><td colspan="2"></td><td colspan="6">S2 and S6 Personnel have limited expertise in analyzing cyber threats and identifying threat vulnerabilities.</td></tr>
<tr><td>Forensics & Reverse Engineering Coord</td><td colspan="2"></td><td colspan="6">Staff personnel have limited expertise in coordinating and interacting with forensics and reverse engineering resources.</td></tr>
<tr><td>Spectrum Management</td><td colspan="2">A</td><td colspan="6"></td></tr>
<tr><td>Offensive C/EM & Dynamic Cyber Defense</td><td colspan="7"></td><td>A*,J*, M*, G*</td><td></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="6">Brigade and above Cyber War expertise</td></tr>
<tr><td>C/EM Intelligence</td><td colspan="2"></td><td>J</td><td colspan="5"></td></tr>
<tr><td>Linguistics**</td><td colspan="8">The Army must recognize the need to have linguists and cultural experts (not necessarily resident in the active duty / reserve Army) to guide C/EM efforts as needed. The Army may also consider efforts conducted by other agencies to fill linguistic and cultural expertise requirements.</td></tr>
<tr><td>Synchronize & Integrate</td><td></td><td>A,J</td><td>J, M</td><td>J, M</td><td>J, M</td><td>J, M</td><td>M</td><td>J, M</td></tr>
<tr><td>Acquisition</td><td colspan="7"></td><td>J, M</td></tr>
</table>

(U//FOUO) Table 6: C/EM Expertise Gap Map

**** These personnel require special career management and development through multiple progressively more difficult positions remaining within their specialty. These personnel have highly developed skills and are required to maintain strenuous proficiency and currency due to these skills being highly perishable.***
*****Personnel used to fill linguistics positions will most normally be civilian or contractor personnel with highly specialized language skills.***

S = Soldier
A = Apprentice
J = Journeyman
M = Master
G = Guild

Color Code	
White	Requires Military due to tactical level operations and deployment (Company thru Brigade) and/or Title X Offensive C/EM Operations (ARCYBER)
Yellow	Military or DA Civilians due to probably deployments
Green	Military, DA Civilians or Contractors

Identified Potential Solutions

P01 – Create C/EM Integration Specialists for battalion through ASCC C/EM Elements (Bundled solution with O01, P02, and P03)

Description (U//FOUO) This solution provides a 'no growth' creation of C/EM Integration Specialists for C/EM Elements, battalion through ASCC, to provide operational planning, synchronization, coordination and integration of C/EM capabilities into full spectrum operations. This solution can be instituted relatively quickly by transforming the 29-series to holistically incorporate all aspects of C/EM and provide operational C/EM expertise.

(U//FOUO This solution utilizes the 29-series, assigned from battalion through ASCC, to provide expertise for incorporating all aspects of cyber/electromagnetic activities, using a combined arms approach, into the unit's overall operation. This recommended solution effectively integrates C/EM capabilities into the operations process. This solution will transform the existing 29-series EW officer to a skilled C/EM planner/integrator that has the acumen to effectively incorporate all aspects of the C/EM contest (cyberspace and EMS) into the commanders' decision making process. Specific transformation recommendations include:

- (U//FOUO) At appropriate times in the new C/EM 29-series professional progression, attendance in additional courses may be required, such as the Joint Network Attack Course and select National Cryptologic School Courses, such as the Network Warfare Planner.
- (U//FOUO) Modify the FA29 EWO Qualification Course to address combined arms C/EM integration and planning.
- (U//FOUO) Modify the 290A Electronic Warfare Technician Course to address specific C/EM targeting requirements.
- (U//FOUO) Modify the 29E Electronic Warfare Specialist Course to address C/EM integration and planning.
- (U//FOUO) All C/EM Integration Specialists require a Top Secret clearance with Special Compartmented Information access (TS/SCI)

(U//FOUO) This solution is integrated with the following solutions: O01, Create the C/EM Staff Element and Working Group, Battalion through ASCC, and O02, Add required C/EM personnel/skill sets to the C/EM Element, Battalion through ASCC.

Rationale (U//FOUO) The 29-series is the most logical and least impact solution for C/EM integration and planning gaps because the 29-series personnel are currently focused on the operational integration of electronic warfare into the combined arms fight. Given convergence, by default they are already working simultaneously in areas of import from both a cyberspace operations and electronic warfare perspective. Furthermore, the Army has expended resources to develop doctrine, organizational structure, training, leader development and education, and personnel to build the 29-

series and is in the process of fielding this capability. The 29-series is easily adapted and transformed to encompass the additional duties that C/EM integration requires. Therefore, transforming 29-series personnel leverages the Army's investment and provides the Army with the capability to operationalize C/EM capabilities in a combined arms fashion supporting FSO.

(U//FOUO) Other career fields and functional areas were considered for this solution. The 25-series was considered but not selected because they are focused primarily on operation and defense of the network. The 35-series was also considered but not selected as a solution because of their orientation on full spectrum intelligence. FA30 was considered but not selected because of their impending orientation on the new Inform and Influence responsibilities defined in the Mission Command Army Functional Concept. FA40 was considered but not selected because the numbers in this Functional Area are small; they're focused at division and above and would not provide the numbers expected to be needed for this solution. FA53 was considered but not selected due to the technical nature of their functional area to integrate diverse forms of enterprise systems technologies rather than the required operational integration focus needed for the C/EM element. All of these career fields and functional areas require more adaptation to handle the C/EM integration tasks than the proposed FA29 solution. ASI solutions were considered but not selected because they would not provide the Army with the institutional capability over time to conduct C/EM planning and integration through progressively more challenging assignments.

(U//FUOU) This solution helps to resolve the personnel gaps identified for Gap 02 - C/EM Integrating Entity, Gap 04 - Access, Gap 26 - Cyber War Network Support, Gap 32 - Cyber Attack, and Gap 37 - EA Asset Deconfliction.

Costs (U//FOUO) This solution requires appropriate level NSA approved Network Warfare Planner training, modification of existing 29-series EW training, and could increase course load at selected other courses as noted above. HQDA resourcing of the EW FDU to date will place a limited number of 29-series personnel on battalion through ASCC staffs. Additional resourcing of the EW FDU over time will produce additional C/EM integration expertise capacity in the Army's formations, particularly at lower echelons.

P02 – Provide Cyber Warfare Expertise (Develop new 35A Cryptologic Cyber Analyst and 35-Series C/EM Offensive Technical Analyst from existing 35-series specialties) (Bundled solution with O01, O02, P01, and P03)

Description (U//FOUO) For ARCYBER requirements, create a new CyberWar Offensive 35A MOS, Cryptologic Cyber Analyst, from existing 35-series specialties for technical planning, coordination, and synchronization pertaining to specific CyberWar related missions (e.g., cyber attack, cyber exploit, dynamic cyber defense; target identification, tracking, and pattern of life analysis; facilitates intelligence distribution and information exchange; provides reach-back to Cryptologic support, access to various SIGINT and intelligence databases, gain/loss analysis, legal review, and de-confliction approval

process). The 35A MOS is trained in specialized SIGINT-enabled CyberWar-centric functions and is required to support C/EM missions. The Cryptologic Cyber Analyst will complete 35-series formal and sustainment training. The 35A Soldiers will be assigned specifically to ARCYBER with expeditionary and staff support roles to tactical and operational units. This MOS will require uniquely managed and developed practitioners at ARCYBER in order to provide the Army with the level of expertise needed to conduct CyberWar C/EM operations. Joint Cyber Analysis Course (JCAC) (6 months) will serve as the AIT for this new cyber warfare MOS along with required follow-on job specific training ranging from two months to over a year to fully train a cyber warfare technician to perform their assigned duties. Total time to train a novice analyst/operator ranges from 8-24 months (which includes JCAC and work role related training).

Description (U//FOUO) For operational echelons requirements (ASCC to BCT), create a new 35-series C/EM Offensive Technical Analyst from existing 35-series specialties, who is the technical integrator for offensive C/EM capabilities to include technical planning, coordination, and synchronization pertaining to CyberWar related mission aspects (e.g., cyber attack, cyber exploit, dynamic cyber defense; target identification, facilitates intelligence inclusion and information exchange; understands the specific requirement to request reach-back to Cryptologic support, access to various SIGINT and intelligence databases, and supports the de-confliction approval process. The 35-series Offensive C/EM Technical Analyst is trained in specialized, SIGINT-enabled CyberWar-centric functions and is required to support C/EM operational missions. The Offensive C/EM Technical Analyst will complete 35-series formal and sustainment training. This function does not replace any current G/S2 functions but builds on the technical expertise of the 35-series Soldier and provides the organic technical expert in the operational planning process that has offensive C/EM expertise.

Rationale (U//FOUO) The Army must have sufficient practitioner and technical expertise to gain access, seize and secure network critical infrastructure to enable tactical level unit's network freedom of action, information collection and mission execution, and the capability to effectively identify and analyze cyber threats, provide vulnerability assessment, and assist threat mitigation. The Army requires practitioners and technicians to conduct offensive, intelligence, and Dynamic Cyber Defense C/EM operations. C/EM access ability at brigade and higher operational organizations is critical to the C/EM contest and will be provided by the 35-series Soldiers. Brigades require organic personnel capability to plan, collect and develop C/EM intelligence for use in exploiting the adversary. The Army requires practitioners to perform and integrate EA and CNA. This solution helps to resolve the personnel gaps identified for Gap 04 - Access, Gap 26 - Cyber War Network Support, Gap 32 - Cyber Attack, Gap 37 - EA Asset Deconfliction, Gap 36 - Cyber Vulnerability Assess and Operational Testing, and Gap 29 - Organic C/EM Collect and Exploit. This Solution is integrated with solutions O02 - Add required C/EM skill sets, O01 – Create the C/EM Staff Element and Working Group, Battalion through ASCC.

Costs (U//FOUO) This is a repurposing of some specific 35-series Soldiers. There will be associated training costs. For the 35A, the Army has 108 fully funded seats for

FY11, 110 for FY12 and 120 for FY13 in the proposed NSA funded course in Pensacola, FL.

P03 – Develop new 25-series enlisted Cyber Defense MOS, officer cyber defense ASI, and cyber defense specialty within Civilian Career Program 34 from existing 25-series specialties (Bundled solution with O01, O02, P01, and P02)

Description (U//FOUO) Establish a cyber defense ASI for Signal Areas of Concentration (25A, 24A, and 53A), a new cyber defense enlisted MOS (25x) that is accessed at the mid-grade level (E6 and above) from primarily 25-series MOSs (e.g. 25B and 25N), and a new cyber defense specialty within Career Program 34. Ensure these personnel are granted the proper clearance. All solutions will offer assignments/positions that prevent the loss of perishable cyber defense skills (especially while in a garrison environment) and provide an enduring cyber defense career path. (Gaps 20, 33, 36). This is tied to Solution O02, Add required C/EM personnel/skill sets to the C/EM Element, Battalion through ASCC.

Rationale (U//FOUO) The Army requires personnel with the required knowledge, skills, abilities, experiences, and security clearance to effectively establish network defense-in-depth, through the implementation of best business practices, utilization of threat assessment data (to include deconstructing and analyzing threat hardware and software), and information gained from vulnerability assessments. This will provide the Army with defensive measures to protect and defend information, information systems, and networks from disruption, denial, degradation, or destruction by incorporating actions specifically conducted to protect against, monitor for, detect, analyze, and respond to unauthorized network activity.

Costs (U//FOUO) A minimal increase in cost for the enlisted solution given the fact any new courses will replace the current 25-series Advanced Leader and Senior Leader Courses. The major increase in cost would come from the establishment of a functional (ASI producing) course, which would cost approximately $41K per year/per student and with approximately an initial throughput of 40 PAX per year, the yearly cost total would be $1.64M per year. It is believed that civilian personnel who work in the NECs, TNOSCs, or ARCYBER can and should attend the enlisted and/or ASI producing courses and thus they would be included in the student throughput noted above – in the end, providing overall cost savings.

P04 – Institute special management procedures for specific ARCYBER experts

Description (U//FOUO) The Army must specially manage (identify, assess, recruit, assign and retain) ARCYBER designated offensive and dynamic network defensive experts predominantly within ARCYBER, INSCOM and 1st Cyber Brigade. These experts are uniquely qualified, highly skilled and specially trained to conduct cyber warfare operations.

These specialized 25 and 35-series MOSs have low density populations located in a limited number of organizations. These MOSs will serve at a variety of NSA/CSS (DoD Central Security Service) extended enterprise locations (NSA Washington – Ft Meade, NSA Georgia – Ft Gordon, NSA Texas – Medina AFB, and NSA Hawaii – Kunia, HI) in addition to the INSCOM Cyber Brigade and will rotate between these organizations. There will most likely be future requirements for cyber warfare Soldiers within Army network defense efforts at the AGNOSC/ACERT/A2TOC (ARCYBER ACOIC) as well as the TNOSCs. The majority of these Soldiers will serve in INSCOM's Cyber Brigade supporting Army, ARCYBER, CYBERCOM, Combatant Commanders, and National cyber requirements.

DA HRC will provide sequentially more difficult assignments resulting in consistently certified personnel who can also continue to progress throughout their career. HRC will send these specialized Soldiers to training to obtain the required skills/certifications that have been identified by position. Once the Soldiers complete training, they will be assigned to a 5 year utilization tour serving in the documented positions. Each headquarters will manage their assigned Soldiers in order to assure they have professional development opportunities commensurate with the rest of the Army and MOS. The special positions will be coded indicating the special training, certifications, and utilization these Soldiers will be assigned to. HRC will also add a special management expert to select promotion boards to ensure these Soldiers are not disadvantaged.

Rationale (U//FOUO) This solution is required in order to specially manage these specialially designated 25 and 35-series experts who have advanced technical skills, high cost training, and significant training time invested in them to produce qualified and certified offensive and dynamic network defensive experts. They must be specially managed in order to maintain and scale nascent cyber warfare subject matter expertise, meet ever increasing demands for cyber warfare operations, increase cyber warfare capability, and provide qualified cyber warfare technicians over the long-term. This solution would provide ARCYBER and INSCOM with uniquely qualified dynamic defensive and cyber warfare personnel in a stable assignment pattern that allows for reinvestment back into cyber warfare operations.

This model does not follow the traditional Army career progression model. This management system should also address recruitment and retention of C/EM personnel.

It takes years of job experience as well as formal training to build this cyber tactical and technical competency. This solution would provide ARCYBER with the uniquely qualified personnel in a stable assignment pattern. These MOSs will require uniquely managed and developed practitioners at ARCYBER in order to provide the Army with the level of expertise needed to conduct C/EM operations for the Army. This solution partially helps to solve Gaps: Gap 04 Access, Gap 26 Cyber War Network Support, Gap 32 Cyber Attack, Gap 37 EA Asset Deconfliction, Gap 36 Cyber Vulnerability Assess and Operational Testing, and Gap 29 Organic C/EM Collect and Exploit. Gap 20

Network Defense in Depth, Gap 36 Cyber Vulnerability Assess and Operational Testing, and Gap 33 Threat Hardware and Software Analysis.

Cost (U//FOUO) Relatively low cost to specially manage a relatively small number of 25 and 35-series personnel.

P05 – 25E Electromagnetic Spectrum Manager (Grade E6-E9)

Description (U//FOUO) Resource Battalion 25E positions which cause this echelon to lack the ability to conduct spectrum management in the C/EM contest and the ability to integrate with EW and cyber.

Rationale (U//FOUO) Army C/EM operations demand dynamic management of available EMS resources and the ability to develop and export EMS use plans in the DoD format due to the increasing reliance on the EMS, as networks and telecommunication infrastructures increasingly make use of wireless means. Our sensors (as part of the network) require the EMS in order to collect information and then to disseminate it. The Army therefore must have the ability to dynamically manage and utilize the Electromagnetic Spectrum (EMS), to include with joint partners along with developing and exporting EMS use plans. The 25E (Electromagnetic Spectrum Managers) at grades E6-E9 perform the electromagnetic spectrum requirements. This solution addresses the personnel-related aspects of Gap 51 – Dynamic Spectrum Management and Gap 53 – EMS Use Plan Export.

Costs (U//FOUO) This solution requires additional resourcing of the EW FDU to provide these positions. Partial resourcing of EW FDU provides for inadequate 25E support. This is currently estimated to be 312 25E30 additional personnel. VCSA validated the EW FDU and directed unresourced positions be resourced in FMR 13-17 and TAA 14-18. EW FDU is competing for unresourced positions from FMR 13-17 in TAA 14-18. 25E resourced MTOE shortages filled by 2012.

P06 – Generating Force C/EM DA Civilians

Description (U//FOUO) Provide the necessary development path for DA Civilian within the Generating Force to maintain a competitive edge in RDT&E and RDA. Ensure these personnel have the appropriate clearances.

Rationale (U//FOUO) The GENFOR requires the capacity to develop and field materiel solutions to mitigate/defeat new and evolving capabilities of technical savvy adversaries. The GENFOR requires the technical expertise necessary to conduct C/EM RDT&E and RDA. This expertise can be made up of military, civilians and/or contractors. This solution addresses the personnel aspect of Gap 61 – Research, Development, and Acquisition and Research, Development and Acquisition.

Costs (U//FOUO) This solution requires sufficient resourcing to place the necessary developmental assignments, education, and training.

2-7 Facilities

Introduction

(U//FOUO) The Army lacks the required facilities to properly conduct the C/EM Contest. Sensitive compartmented information facilities (SCIFs) that can adequately store classified information and holistically integrate the "Observe," "Defend," "Attack," and "Exploit" elements of the C/EM Contest are required. Currently the Army shares joint and national facilities to accomplish portions of its C/EM missions. In addition to facilities required to conduct the C/EM Contest, the Army lacks the facilities to properly test and train C/EM objectives (per training solutions section). To meet these testing and training objectives, C/EM ranges are required to simulate the cyberspace and electromagnetic spectrum domains. The Army's IO Range provides one of the key tools for battle staff to exercise integrated planned and effects in a training environment, but not all leaders and staffs have access.

FSA Methodology for Developing Facilities Solutions

(U//FOUO) The FNA identified 12 gaps as having Facilities aspects. During the first FSA Workshop, Facilities was examined by 45 SMEs. The SMEs broke into 3 working groups to collaborate about potential Facilities solutions.

FNA Gaps with Facilities Aspects

C/EM Integrating Entity (Gap 02)
Access (Gap 04)
Establish, Operate, Manage Enterprise Network (Gap 11)
Single System and User ID (Gap 17)
Network Defense in Depth (Gap 20)
Access to Critical Network Information, Services and Applications (Gap 24)
Non-Attributed Networks (Gap 26)
Dynamic Cyber Defense (Gap 28)
Threat Hardware and Software Analysis (Gap 33)
C/EM Modeling and Simulation (Gap 46)
Defend / Protect Individuals and Platforms (Gap 57)
Research, Development and Acquisition (Gap 61)

Identified Potential Solutions

F01 – Ensure adequate facilities are available at the strategic, operational, and tactical levels in order to conduct C/EM activities

Description (U//FOUO) Proper facilities, operational centers, TOCs, and SCIFs are required to plan and execute C/EM missions to include defense, exploitation, and attack functions. Proper facilities must be built to support Cyber and EW training at the CTCs.

The Army must identify new facilities and expand existing facilities to meet these needs. (Gaps 02, 04, 11, 17, 20, 24, 26, 28, 33, 46, 57, 61)

Rationale (U//FOUO) Enhanced infrastructure is necessary to meet EW and C/EM requirements at CTCs and home stations. Access to JWICS and NSA networks, for which the access points must be secured in SCIFs, will improve Intelligence support to the Network Operations and Security Centers (NOSCs) at each echelon by providing timely intelligence estimates that accurately identify adversary intentions, support defense operations, and predict adversary future COAs in sufficient detail as to be actionable. Intelligence will provide NOSC leaders with reach-back to Intelligence tool suites such as the Threat Incident Database (TID) and the Threat Intelligence Portal (TIP). The objective of Intelligence support is to share intelligence information and events in support of CND to enable rapid, near-real time cross-cueing of threat activity and fusion of all-sources of information on foreign threats to the LandWarNet. Additional secure facilities will be needed to plan and execute cyber war tasks at all applicable echelons.

Costs (U//FOUO) The cost of providing the Army with an adequate number of SCIFs will rely on many factors set forth in Director of Central Intelligence Directive (DCID) Manual 6/9 - Physical Security Standards for Sensitive Compartmented Information Facilities (Nov 2002). Each facility will have greatly varied cost estimates based on the following security layer considerations:

- (U//FOUO) Type of SCIF – closed storage, open storage, continuous operations, or secure working area
- (U//FOUO) CONUS or OCONUS location
- (U//FOUO) Located on or off a controlled government installation
- (U//FOUO) Security/response force available
- (U//FOUO) New building or existing building
- (U//FOUO) Controlled access or open access of building
- (U//FOUO) Number of doors to the building
- (U//FOUO) Construction and type of building, doors, windows, vents, ducts, and pipes
- (U//FOUO) Sound attenuation factors

F02 – Ensure adequate facilities and C/EM ranges are available to execute C/EM experimentation, testing and training

Description (U//FOUO) The Ft. Sill EW facility has been upgraded to accommodate training; Ft. Huachuca TS/SCI classrooms currently seat 1,357; and the Ft. Gordon TS/SCI classroom should be operational by Feb 11 to support the 255S training. As training requirements increase, ensure that classroom space can handle the increased demand. Ranges (current or new) must be able to incorporate the C/EM Contest and support requirements at all levels of integration. These ranges must support training, experimentation, and RDT&E and RDA. This requires Authority to Operate and FCC

clearance for spectrum control. Currently the IO Range is available at many, but not all, Army installations. Minimal live fire C/EM opportunities exist and are currently available at White Sands Missile Range, the Intelligence Electronic Warfare Test Directorate, and at Yuma Proving Grounds. The DARPA Cyber Range advancements should also be leveraged to incorporate new technologies as they emerge. The Army should support Ft. Sill's efforts for an EW range survey, work with FORSCOM and CTCs to determine training infrastructure needs, and utilize Joint IO Range Sites. Facility requirements for the RDT&E and RDA communities are needed in order for the PEO/PM, testing and evaluation communities to develop integrated C/EM solutions, potentially different facilities rated to the appropriate clearance level. This is required in order to conduct C/EM software development and testing. (Gaps 02, 04, 28, 46, 57, 61)

Rationale (U//FOUO) The Army has limited facilities to properly test and train C/EM objectives. C/EM ranges are required to simulate the cyberspace and electromagnetic spectrum domains.

Residual Gap Assessment

(U//FOUO) The identified potential solutions will adequately mitigate C/EM Facilities gaps; however these must be implemented in conjunction with other aspects of DOTMLPF to fully mitigate the gaps as a whole.

2-8 Policy

Introduction

(U//FOUO) The Army and DoD lack definitive policy to conduct the C/EM Contest. The Army requires the appropriate policy and authorities to coordinate with interagencies and conduct actions in and through cyberspace and the electromagnetic spectrum. Currently policy addresses parts of the C/EM contest separately and does not holistically address actions in FSO. The Army must set forth policies to be able to deter, prevent, detect, defend against, respond to, and remediate hostile actions in the C/EM Contest.

The top five Policy implication priorities identified during UQ11 were the need to provide ARCYBER the authorities to ensure it is responsive the national, Service, combatant commander (CCDR) and interagency cyberspace operational requirements; implement policies that facilitate effective and timely sharing of information about cyber threats, operations and capabilities; a coordinated revision of current policies relating to cyberspace to make them relevant and effective in supporting cyberspace operations; clearly define terms such as "use of force," "hostile intent," and "hostile act" as related to cyberspace; and authorities to conduct cyberspace operations should continue to use the same authority process, such as EXORDS, for offensive and defensive cyberspace activities.

FSA Methodology for Developing Policy Solutions

(U//FOUO) The FNA identified 27 gaps as having Policy aspects. During the first FSA Workshop, Policy was examined by 45 SMEs. The SMEs broke into 3 working groups to collaborate about what Policy needed updating to mitigate C/EM gaps.

FNA Gaps with Policy Aspects

C/EM Integrating Entity (Gap 02)
Access (Gap 04)
Legal Advisement for C/EM (Gap 06)
Establish, Operate, Manage Enterprise Network (Gap 11)
Transition Network C2 (Gap 15)
Single System and User ID (Gap 17)
Integrate CyNetOps with Mission Partners (Gap 19)
Network Defense in Depth (Gap 20)
Access Critical Network Info, Services, & Applications (Gap 24)
Non-Attributed Networks (Gap 26)
Dynamic Cyber Defense (Gap 28)
Organic BDE C/EM Collect and Exploit Intelligence (Gap 29)
Cyber Attack (Gap 32)
Threat Hardware & Software Analysis (Gap 33)

Cyber Vulnerability Assess & Operational Testing (Gap 36)
EA Asset Deconfliction (Gap 37)
Cyber Threat Investigation and Information Sharing (Gap 38)
Conduct Electronic Attack (Gap 45)
C/EM Modeling and Simulation (Gap 46)
Detect Jamming (Gap 50)
Dynamic Spectrum Management (Gap 51)
EMS Use Plan Export (Gap 53)
Spectrum Use Prioritization (Gap 54)
Defend/Protect Individuals and Platforms (Gap 57)
Research, Development, and Acquisition (Gap 61)

Identified Potential Solutions

Policy01 – Update Army Regulations, DA PAMS, DoD Instructions, CJCS Instructions, and US Codes

Description (U//FOUO) Adding C/EM considerations to Army Regulations, DoD Instructions, CJCS Instructions, and US Codes will allow the Army to execute the C/EM Contest quickly and legally.

Rationale (U//FOUO) Most of these publications currently do not adequately address C/EM activities, present an obstacle to performing the required C/EM activities, or use antiquated verbiage to describe C/EM activities. (2, 4, 6, 11, 15, 17, 19, 20, 24, 26, 28, 29, 32, 33, 36, 37, 38, 45, 46, 50, 51, 52, 53, 54, 57, 61)

- (U//FOUO) AR 25-series, including AR 5-22 & AR 10-87 (Chapters 1, 14, and 16): Changes in mission roles and responsibilities for ARCYBER, 9th SC (A), INSCOM, and 1st IO CMD

- (U//FOUO) AR 70 Series, DoD 5000 Series, and AFAR/DFAR to integrate quick reaction and technical insertion acquisition capabilities into programs of record

- (U//FOUO) DA PAM 600-3 – Develop and implement an integrated C/EM Career Force development model describing apprentice, journeyman, and master skill set levels

- (U//FOUO) DoD 8110.1 Multinational Information Sharing Networks Implementation

- (U//FOUO) DoD 8530.2 Support to Computer Network Defense (CND)

- (U//FOUO) CJCSI 6510 Information Assurance (IA) and Computer Network Defense (CND); AR 380-53 Information Systems Security Monitoring

- (U//FOUO) UJTL – Universal Joint Task List

- (U//FOUO) US Code Title 6 – Domestic Security, Title 18 – Crimes & Criminal Procedures, Title 32 – National Guard, Title 40 – Public Buildings, Property and Works, Title 50 – War & National Defense

Policy02 – Update US Code Title 10

Description (U//FOUO) Title 10 – Armed Forces currently only allows active duty personnel to execute cyber war operations. Recommend that Title 10 be changed to allow Department of the Army civilians (DAC) to also have authorization to execute cyber war. (Gaps 28, 32, 45)

Rationale (U//FOUO) Allowing DACs to fully execute cyber war tasks will ease the staffing strain to execute C/EM missions.

Residual Gap Assessment

(U//FOUO) The identified potential solutions will adequately mitigate C/EM policy gaps; however these must be implemented in conjunction with other aspects of DOTMLPF to fully mitigate the gaps as a whole.

Cost – Benefit and/or Trade – Off Analysis

(U//FOUO) The cost of implementing the identified potential solutions is moderate and is comparable to the current approach.

Policy03 – Create New Network Policies

Description (U//FOUO) Develop policies related to network architectures, authentication, information assurance, network command and control, and acquisition of network technologies, for which none currently exist. (Gaps 11, 15, 17, 20, 24)

Rationale (U//FOUO) Most of the following policies do not exist at all and thus impact operational readiness and the ability for units to quickly transition in FSO:

- Policy that ensures the interoperability of LandWarNet assets, in accordance with approved requirements documents, and compliant with the operational, system, and technical views of the LandWarNet architecture.

- Policy that universally enables all approved systems/devices to connect to any portion of the network without need for recertification or determination of net worthiness.

- Support policy that enables a single systems/device to operate at all classification levels.

- Policy that provides a common, or enterprise-level, communications, and computing architecture for the LandWarNet to provide a full range of information services at all major security classifications and information handling caveats consistent with NSTISSP No. 11.

- Policy and C2 structure for exercising authority and direction by a properly designated commander during all phases of an operation; and determine which entities can designate authority.

- Security policy that addresses all aspects of identity management/ authentication and provides for realistic opportunities to enforce the greater IA policy requirements.

- Policy which provides guidance for information sharing in a net-centric environment through collaborative forums (Communities of Interest (COIs)), provides a set of activities that members of COIs and associated leadership can use to implement key policies of DoDD 8320.02, and addresses the sharing of information across domains.

- Army enterprise network acquisition policy that ensures network technologies will be planned, resourced, acquired, and implemented at a pace required to make them operationally relevant.

Cost – Benefit and/or Trade – Off Analysis

(U//FOUO) The cost of implementing the identified potential solution is low and is comparable to the current approach.

Section III – RSA Prioritization

(U//FOUO) The FSA identified 38 solutions to mitigate the FNA gaps. These solutions were aligned to the gaps in the Recommended Solution Analysis worksheet (Appendix A) using a matrix focusing on the Technical Risk, Supportability, Feasibility, Affordability, and DOTMLPF Implications. The solutions were then prioritized by the gap priority and by the number of gaps the solution addressed. Some solutions were grouped if they were interdependent. For example, Leader Development and Education and Training are inter-related as is Personnel and Organizations. Doctrinal and Policy implementation is considered mandatory. These solutions are required to fully integrate the C/EM contest into the Army at all echelons and were not prioritized against the remaining solutions. Solutions were grouped into mandatory, first and second priority. Within each priority are bundles of interdependent solutions that support each other and need to be implemented on a similar timeline.

Mandatory
(U//FOUO) Update Capstone and supporting doctrine Solution Group. These doctrine and policy solutions are mandatory because the Army must have doctrine in order to execute all other solutions.

D01 – Army Capstone Doctrine – Modify FM 3-0 Operations
D02 – Army Warfighting Functional Doctrinal Publications – Modify FM 2-0 Intelligence, FM 4-0 Sustainment, FM 6-0 Mission Command and Control, FM 3-09 Fire Support, FM 3-30 Protection, and FM 6-02 Signal Operations
D03 – Elements of Army Combat Power Doctrinal Publications – Rewrite FM 3-13 as the Inform and Influence Activities FM
D04 – Rewrite FM 3-36 as the Cyber/Electromagnetic Activities FM
D05 – Other & Supporting Doctrine Solutions
Policy01 – Update Army Regulations, DA PAMS, DoD Instructions, CJCS Instructions, and US Codes
Policy02 – Update US Code Title 10
Policy03 – Create New Network Policies

First Priority
(U//FOUO) The prioritization process revealed the following solutions are all considered priority one because they solve the highest priority gaps, affect the most gaps, and are already strategies which can be modified with minimal cost.

(U//FOUO) Update Organizations and Personnel Solution Group. These solutions were bundled together because they are mutually supportive and interdependent in order to develop structure there must be personnel to fill the skill sets.

O01 – Create the C/EM Staff Element and Working Group, Battalion through ASCC

O02 – Add required C/EM personnel/skill sets to the C/EM Element, Battalion through ASCC
P01 – Create C/EM Specialists for battalion through ASCC C/EM Elements
P02 – Develop new 35A Cryptologic Cyber Analyst MOS
P03 – Develop new 25-series enlisted Cyber Defense MOS, officer cyber defense ASI, and cyber defense specialty within Civilian Career Program 34
P05 – 25E Electromagnetic Spectrum Manager (Grade E6-E9)
P06 – Generating Force C/EM DA Civilians

(U//FOUO) Update the ANMS. This solution is an already approved strategy and will mitigate many gaps at an acceptable operational risk.

M01 – Pursue a modified Army Network Modernization Strategy (ANMS)

(U//FOUO) Update Leader Development & Education and Training Solution Group. These solutions were bundled together because they address generic standard training and leader development that affects all Army Soldiers and leaders (e.g. Warrior Skills, WLC, and CCC).

T01 – Incorporate basic C/EM Contest knowledge into individual
T02 – Incorporate C/EM into home station training
T03 – Incorporate basic tasks that test C/EM knowledge into collective training and CTC events
L01 – Incorporate basic C/EM knowledge into the Officer Education System, Warrant Officer Education System and Noncommissioned Officer System
L03 – Incorporate the C/EM Contest into leadership & education opportunities during training exercises

Second Priority
(U//FOUO) The prioritization process revealed the following solutions are all prioritized according to the gaps they address after the mandatory and priority solutions were addressed. They affect moderately high priority gaps, affect numerous gaps, and can be modified with minimal cost.

(U//FOUO) Materiel Requirements to Integrate the C/EM contest Group. These solutions were bundled together because they are the processes and tools the Army requires to effectively operate. These materiel solutions address fewer gaps overall, however rank higher because their impacts on the C/EM contest are significant.

M05 – Defend and Protect Individuals and Platforms
M02 – Providing Cyber Attack unique delivery systems and payloads in a timely manner
M03 – Maintain currency of tools for threat hardware and software exploitation and vulnerability assessments
M04 – C/EM Modeling and Simulation

M06 – C/EM Research, Development, Testing and Evaluation (RDT&E), Research, Development and Acquisition (RDA), and Tactics, Techniques, Procedures (TTP) Enterprise

(U//FOUO) Specialized Training and Management Group. These solutions were bundled together because they address specialized training, leader development, and personnel that affect a small amount of Soldiers and leaders (e.g. JCAC, NCC, and NWP).

T04 – Specialized Training and Certification
L02 – Incorporate additional specialized C/EM training into 14, 24, 25, 29, 30, 35, 40, and 53 series Professional Military Education (PME)
P04 – Institute special management procedures for specific ARCYBER experts

(U//FOUO) Update Network Organizations and Training Solutions Group. These solutions were bundled together because they support the establishment of network organizations, training, and facilities. These solutions address fewer gaps and are moderately important to enable organizations to effectively operate in the future.

O04 – Designate a NETCOM element to coordinate network C2 transition
O03 – Modify Expeditionary Signal Battalion (ESB) structure to a Joint Communications Support Element (JCSE) like organization to provide network connectivity and defense capabilities.
O05 – Reorganize Brigade/BCT S6 structure IAW the NetOps Construct
O07 – NetOps Positions in Cyber Brigades
T06 – Establish NetOps Training Program
T05 – Propose a Joint Cyber Training Enterprise
T07 – Support IA Certification Requirements
O06 – Franchise Theater Network Operations and Security Centers and Network Enterprise Centers
F01 – Ensure adequate facilities are available at the strategic, operational, and tactical levels in order to conduct C/EM activities
F02 – Ensure adequate facilities and C/EM ranges are available to execute C/EM experimentation, testing and training

Appendix A RSA Worksheet

Recommended DOTMLPF Solution Approaches (RSA) Worksheet

0

Gap Type (JCIDS Manual A-6) = A: proficiency; B: sufficiency; C. no capability; D: replace current; E: policy limitations
Gap Timeframe = N. near-term (BY); M. mid-term (POM); L. long-term (EPP); A. All timeframes
Materiel Types:
RECAP/SLEP – no significant improvement in operational capability
Evolutionary – a significant (or incremental) improvement to an existing materiel capability
Transformational – an approach considered so significant (and needed) that potential cost and technical risk, etc should be considered
Information Systems – generally used synonymously with IT systems

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
2	D; A	7	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
2	D; A	7	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
2	D; A	7	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										to mitigate the gap
2	D; A	7	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
2	D; A	7	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
2	D; A	7	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
2	C;N&M	7	Organization O01 Rewrite EW Element to C/EM element, BN-ASCC and Rewrite EW WG to C/EM WG	N/A	N/A	Likely	M	Doctrine – C/EM element, Personnel (29-series), training – additional training required	1	Major
2	C;M&L	7	Organization O02 Add required C/EM skill sets to the Rewrited EW	N/A	N/A	Likely	H	Doctrine – C/EM element, Personnel (29, 25 and 35-series), training –	1	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Element					additional training required		
2	C; A	7	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
2	C; A	7	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
2	C; A	7	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Moderate
2	C; A	7	Training T04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	2	Moderate
2	D; A	7	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
2	D; A	7	Leadership L02 Incorporate C/EM into 25, 29, & 35	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	3	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Courses							
2	D; A	7	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
2	C; A	7	Materiel M01 Informational Systems: Application or set of applications to allow for the planning, integration, and synchronization of C/EM capabilities	L	M	Likely	M	Y, requires Training of new system(s)	1	Major, Materiel solutions will facilitate the integration of the C/EM contest and mitigate the gap
2	C;N&M	7	Personnel P01 Adapt 29A EW, 290A EW Tech, 29E EW Specialist	N/A	N/A	Likely	M	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major
2	C; A	7	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	4	Minimal
2	D; A	7	Facilities F02 C/EM Ranges	N/A	N/A	Likely	H	Personnel – to execute C/EM experimentation, testing, and training	5	Minimal
4	D; A	10	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
4	D; A	10	Doctrine D01 Modify	N/A	N/A	Likely	M	Must incorporate	Mandatory	Major,

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Army Capstone Doctrine					doctrine changes into Training and Leadership courses		however all doctrine approaches must be implemented to mitigate the gap
4	D; A	10	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
4	D; A	10	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
4	D; A	10	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
4	D; A	10	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										implemented to mitigate the gap
4	C;N&M	10	Personnel P01 Adapt 29A EW, 290A EW Tech, 29E EW Specialist	N/A	N/A	Likely	M	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major, required to ensure access capability's at the functional Bde
4	C;N&M	10	Personnel P02 Develop new 35A Cryptologic Cyber Analyst MOS	N/A	N/A	Likely	H	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major, required to ensure access capability's at the functional Bde
4	C;N&M	10	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	2	Major, required to ensure access capability's at the functional Bde
4	C; A	10	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	3	Moderate, must be completed with other solutions to completely mitigate the gap
4	D; A	10	Facilities F02 C/EM Ranges	N/A	N/A	Likely	H	Personnel – to execute C/EM experimentation, testing, and training	4	Moderate, must be completed with other solutions to completely mitigate the gap

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
6	D; A	19	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
6	D; A	19	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
6	D; A	19	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
6	D; A	19	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
6	D; A	19	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
6	D; A	19	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
6	C; A	19	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate, training must be addresses to completely mitigate the gap
11	D; A	8	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
11	D; A	8	Policy03 – Create New Network Policies	N/A	N/A	Likely	M	N	Mandatory	Major
11	D; A	8	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
11	D; A	8	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										to mitigate the gap
11	D; A	8	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
11	D; A	8	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
11	D; A	8	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
11	B; M&L	8	Organization O03 Modify Expeditionary Signal Battalion structure to JCSE	N/A	N/A	Likely	H	Training – will increase number requiring training	2	Major
11	C; A	8	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
11	C; A	8	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
11	C; A	8	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Moderate
11	C; A	8	Training T04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	3	Moderate
11	C; L	8	Training T05 Purpose a Joint Cyber Training Enterprise	N/A	N/A	Likely	M	Doctrine Possible changes to joint doctrine. Possible changes to LDT&E for joint operations	5	Moderate
11	C; L	8	Training 06 Establish NetOps Training Program	N/A	N/A	Likely	M	Organization- Must designate who is responsible for NetOps training program; material for training; LDT&E for effective training; personnel to train; facilities	4	Moderate
11	D; A	8	Leadership L01 Incorporate C/EM	N/A	N/A	Likely	M	Personnel – must have personnel to	1	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			into PME					train C/EM; Facilities – potential need of SCIFs at training venues		
11	D; A	8	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	6	Moderate
11	D; A	8	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
11	A B; A	8	Materiel M01 Evolutional: Implement a Global Network Enterprise Implementation Strategy	L	L	Likely	M	Y, requires Organizational changes, new Training, new Materiel, may require more Personnel to man, updated and new Facilities and Policy changes	1	Major
11	C; A	8	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	7	Minimal
15	D; A	23	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
15	D; A	23	Policy03 – Create New Network Policies	N/A	N/A	Likely	M	N	Mandatory	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
15	D; A	23	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
15	D; A	23	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
15	D; A	23	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
15	D; A	23	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
15	D; A	23	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										must be implemented to mitigate the gap
15	C; N&M	23	Organization O04 Designate a NETCOM element to coordinate network C2 transition	N/A	N/A	Likely	M	Doctrine & Policy – designate C2 transition authorities	2	Moderate, coordinated entity must be identified to allow other gap solutions to be effective
15	C; A	23	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate, required for effective application of Materiel to reduce gap to an acceptable operational level
15	C; L	23	Training 06 Establish NetOps Training Program	N/A	N/A	Likely	M	Organization- Must designate who is responsible for NetOps training program; material for training; LDT&E for effective training; personnel to train; facilities	3	Moderate, required for effective application of Materiel to reduce gap to an acceptable operational level
~~15~~	~~A B; A~~	~~23~~	~~Materiel M01 Evolutional: Implement a Global Network Enterprise Implementation Strategy~~	~~L~~	~~L~~	~~Likely~~	~~M~~	~~Y, requires Organizational changes, new Training, new Materiel, may require more Personnel to man,~~	~~1~~	~~Major, Gap mitigated congruent with operational risk~~

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								~~updated and new Facilities and Policy changes~~		
15	D; A	23	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate, required for effective transition of network C2
15	D; A	23	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	4	Moderate, required for effective transition of network C2
15	D; A	23	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate, required for effective transition of network C2
17	D; A	18	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major impact on closing the gap
17	D; A	18	Policy03 – Create New Network Policies	N/A	N/A	Likely	M	N	Mandatory	Major
17	A B; A	18	Materiel M01 Evolutional: Implement a Global Network Enterprise Implementation Strategy	L	L	Likely	M	Y, requires Organizational changes, new Training, new Materiel, may require more Personnel to man, updated and new	1	Closes the Gap

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								Facilities and Policy changes		
17	C; A	18	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	2	Major, but must be done together with materiel solution M01
19	D; A	17	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
19	D; A	17	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
19	D; A	17	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
19	D; A	17	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
19	D; A	17	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
19	D; A	17	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
19	C; A	17	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
19	C; A	17	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
19	C; A	17	Training T04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	3	Moderate
19	C; L	17	Training 05 Purpose a Joint Cyber Training Enterprise	N/A	N/A	Likely	M	Doctrine Possible changes to joint doctrine. Possible changes to LDT&E for joint operations	2	Moderate
19	C; L	17	Training 06	N/A	N/A	Likely	M	Organization- Must	4	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Establish NetOps Training Program					designate who is responsible for NetOps training program; material for training; LDT&E for effective training; personnel to train; facilities		
19	D; A	17	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
19	D; A	17	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	5	Moderate
19	D; A	17	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
19	A B; A	17	Materiel M01 Evolutional: Implement a Global Network Enterprise Implementation Strategy	L	L	Likely	M	Y, requires Organizational changes, new Training, new Materiel, may require more Personnel to man, updated and new Facilities and Policy changes	1	Major
20	D; A	1	Policy01 Incorporate	N/A	N/A	Likely	M	Must incorporate	Mandatory	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			C/EM into Policy					policy changes into Training and Leadership courses		
20	D; A	1	Policy03 – Create New Network Policies	N/A	N/A	Likely	M	N	Mandatory	Major
20	D; A	1	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
20	D; A	1	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
20	D; A	1	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
20	D; A	1	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										to mitigate the gap
20	D; A	1	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
20	C; M&L	1	Organization O05 Reorganize brigade/BCT S6 structure IAW the Netops construct	N/A	N/A	Likely	H	Training – will increase number requiring training	3	Moderate
20	A B; L	1	Organization O06 Franchise Theater Network Operations and Security Centers and Network Enterprise Centers	N/A	N/A	Likely	M	Possible Organizational changes, new Training, updates to Facilities	2	Moderate
20	A B; L	1	Organization O07 NetOps Positions in Cyber Brigades	N/A	N/A	Likely	M	Possible Organizational changes, new Training, updates to Facilities	4	Moderate
20	C; A	1	Training T04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	6	Moderate
20	C; L	1	Training 05 Purpose a Joint Cyber Training Enterprise	N/A	N/A	Likely	M	Doctrine Possible changes to joint doctrine. Possible changes to LDT&E for joint operations	8	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
20	C; L	1	Training 06 Establish NetOps Training Program	N/A	N/A	Likely	M	Organization- Must designate who is responsible for NetOps training program; material for training; LDT&E for effective training; personnel to train; facilities	5	Moderate
20	C; L	1	Training T07 Support IA Certification Requirements	N/A	N/A	Likely	M	N	7	Moderate
20	A B; A	1	Materiel M01 Evolutional: Implement a Global Network Enterprise Implementation Strategy	L	L	Likely	M	Y, requires Organizational changes, new Training, new Materiel, may require more Personnel to man, updated and new Facilities and Policy changes	1	Major
20	A;N&M	1	Personnel P03 Revise 25B IT Spec and integrate 255S Info Protection Tech network defense MOSs	N/A	N/A	Likely	M	Training – will change	1	Major
20	C;N&M	1	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	10	Major
20	C; A	1	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security	9	Minimal

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								manager & appropriate clearances		
24	D; A	12	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Training, Leadership	Mandatory	Major
24	D; A	12	Policy03 – Create New Network Policies	N/A	N/A	Likely	M	N	Mandatory	Major
24	D; A	12	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
24	D; A	12	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
24	D; A	12	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
24	D; A	12	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and	Mandatory	Major, however all doctrine

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			FM					Leadership courses		approaches must be implemented to mitigate the gap
24	D; A	12	Doctrine D05 Modify Other & Supporting	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
24	B; M&L	12	Organization O03 Modify Expeditionary Signal Battalion structure to JCSE	N/A	N/A	Likely	H	Training – will increase number requiring training	2	Minimal
24	C; A	12	Training T04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	3	Moderate
24	C; L	12	Training 05 Purpose a Joint Cyber Training Enterprise	N/A	N/A	Likely	M	Doctrine Possible changes to joint doctrine. Possible changes to LDT&E for joint operations	7	Moderate
24	C; L	12	Training 06 Establish NetOps Training Program	N/A	N/A	Likely	M	Organization- Must designate who is responsible for NetOps training program; material for training; LDT&E for effective training; personnel to train; facilities	4	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
24	D; A	12	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
24	D; A	12	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	5	Moderate
24	D; A	12	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
24	A B; A	12	Materiel M01 Evolutional: Implement a Global Network Enterprise Implementation Strategy	L	L	Likely	M	Y, requires Organizational changes, new Training, new Materiel, may require more Personnel to man, updated and new Facilities and Policy changes	1	Major
24	C; A	12	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	6	Minimal
26	D; A	3	Policy 01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
26	D; A	3	Doctrine D01 Modify	N/A	N/A	Likely	M	Must incorporate	Mandatory	Major,

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Army Capstone Doctrine					doctrine changes into Training and Leadership courses		however all doctrine approaches must be implemented to mitigate the gap
26	D; A	3	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
26	D; A	3	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
26	D; A	3	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
26	D; A	3	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										implemented to mitigate the gap
26	C; A	3	Training T04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	4	Major
26	D; A	3	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Minimal
26	D; A	3	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	5	Minimal
26	C;N&M	3	Personnel P01 Adapt 29A EW, 290A EW Tech, 29E EW Specialist	N/A	N/A	Likely	M	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major
26	C;N&M	3	Personnel P02 Develop new 35A Cryptologic Cyber Analyst MOS	N/A	N/A	Likely	H	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major
26	C;N&M	3	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	3	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
26	C; A	3	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	2	Minimal
28	D; A	6	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
28	A; A	6	Policy02 Update Title 10	N/A	N/A	Likely	M	Organization – might affect numbers of active duty required if DACs can execute cyber attack. Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
28	D; A	6	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
28	D; A	6	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
28	D; A	6	Doctrine D03 Modify	N/A	N/A	Likely	M	Must incorporate	Mandatory	Major,

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Element of Army Combat Power Doctrine					doctrine changes into Training and Leadership courses		however all doctrine approaches must be implemented to mitigate the gap
28	D; A	6	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
28	D; A	6	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
28	D; A	6	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Major
28	D; A	6	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	2	Major
28	C; A	6	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate	3	Minimal

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								clearances		
28	D; A	6	Facilities F02 C/EM Ranges	N/A	N/A	Likely	H	Personnel – to execute C/EM experimentation, testing, and training	4	Minimal
29	D; A	11	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
29	C; A	11	Training T04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	2	Major, required to mitigate operational risk to acceptable level
29	C; L	11	Training 05 Purpose a Joint Cyber Training Enterprise	N/A	N/A	Likely	M	Doctrine Possible changes to joint doctrine. Possible changes to LDT&E for joint operations	3	Major, required to mitigate operational risk to acceptable level
29	A B; A	11	Materiel M01 Evolutionary: Modify LandWarNet to allow increased sensors and sensor bandwidth for effective use the EMS to conduct dynamic information collection asset management and defensive and offensive EA. Modify Prophet, pistol/ stingray, CREW, JTRS Prowler/	M	M	Likely	M	Y, requires Organizational changes, new Materiel, may require more Personnel to man, updated and new Facilities	1	Closes the Gap

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Growler, compass call and RC-12 Guardrail							
29	C;N&M	11	Personnel P02 Develop new 35A Cryptologic Cyber Analyst MOS	N/A	N/A	Likely	H	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major, however must be congruent with other approaches to effectively use new capabilities in M01
29	C;N&M	11	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	4	Major, however must be congruent with other approaches to effectively use new capabilities in M01
32	D; A	9	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
32	A; A	9	Policy02 Update Title 10	N/A	N/A	Likely	M	Organization – might affect numbers of active duty required if DACs can execute cyber attack. Must incorporate policy changes into Training and Leadership courses	Mandatory	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
32	D; A	9	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
32	D; A	9	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
32	D; A	9	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
32	D; A	9	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
32	D; A	9	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										must be implemented to mitigate the gap
32	C; A	9	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Major
32	C; A	9	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Major
32	C; A	9	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Major
32	C; A	9	Training 04 Specialized Training	N/A	N/A	Likely	M	Leadership – leaders must know what their Soldiers are being trained on; Facilities – must have adequate SCIFs at training venues	3	Major
32	C; L	9	Training 05 Purpose a Joint Cyber Training Enterprise	N/A	N/A	Likely	M	Doctrine Possible changes to joint doctrine. Possible changes to LDT&E	6	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								for joint operations		
32	D; A	9	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
32	D; A	9	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	5	Moderate
32	D; A	9	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
32	A B; A	9	Materiel M02 Transformational: Providing Cyber Attack unique delivery systems and payloads in a timely manner.	H	M	Likely	H	Y, requires Organizational changes, new Materiel, may require more Personnel to man	2	Major
32	C;N&M	9	Personnel P01 Adapt 29A EW, 290A EW Tech, 29E EW Specialist	N/A	N/A	Likely	M	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major
32	C;N&M	9	Personnel P02 Develop new 35A Cryptologic Cyber Analyst MOS	N/A	N/A	Likely	H	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
32	C;N&M	9	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	4	Major
33	D; A	16	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
33	D; A	16	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
33	D; A	16	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
33	D; A	16	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
33	D; A	16	Doctrine D04	N/A	N/A	Likely	H	Must incorporate	Mandatory	Major,

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Rewrite FM 3-36 as the C/EM Activities FM					doctrine changes into Training and Leadership courses		however all doctrine approaches must be implemented to mitigate the gap
33	D; A	16	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
33	C; A	16	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
33	D; A	16	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
33	D; A	16	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Moderate
33	D; A	16	Leadership L01	N/A	N/A	Likely	M	Personnel – must	1	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Incorporate C/EM into PME					have personnel to train C/EM; Facilities – potential need of SCIFs at training venues		
33	D; A	16	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	4	Moderate
33	D; A	16	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
33	A B; A	16	Materiel Approach M03 Evolutionary: Maintain currency of tools for threat hardware and software exploitation and vulnerability assessments	L	L	Likely	M	Y, requires Training of new systems and materiel	2	Major
33	A;N&M	16	Personnel P03 Revise 25B IT Spec and integrate 255S Info Protection Tech network defense MOSs	N/A	N/A	Likely	M	Training – will change	1	Major
33	C;N&M	16	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	5	Major
33	C; A	16	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security	3	Minimal

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								manager & appropriate clearances		
36	D; A	2	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
36	D; A	2	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
36	D; A	2	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
36	D; A	2	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
36	D; A	2	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										must be implemented to mitigate the gap
36	D; A	2	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
36	C; A	2	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
36	C; A	2	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
36	C; L	2	Training 05 Purpose a Joint Cyber Training Enterprise	N/A	N/A	Likely	M	Doctrine Possible changes to joint doctrine. Possible changes to LDT&E for joint operations	4	Moderate
36	D; A	2	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Minimal
36	D; A	2	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	3	Minimal

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
33	A B; A	16	Materiel Approach M03 Evolutionary: Maintain currency of tools for threat hardware and software exploitation and vulnerability assessments	L	L	Likely	M	Y, requires Training of new systems and materiel	2	Major
36	C;N&M	2	Personnel P02 Develop new 35A Cryptologic Cyber Analyst MOS	N/A	N/A	Likely	H	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Moderate
36	A;N&M	2	Personnel P03 Revise 25B IT Spec and integrate 255S Info Protection Tech network defense MOSs	N/A	N/A	Likely	M	Training – will change	1	Moderate
36	C;N&M	2	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	5	Moderate
37	D; A	15	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
37	D; A	15	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										implemented to mitigate the gap
37	D; A	15	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
37	D; A	15	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
37	D; A	15	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
37	D; A	15	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
37	C; A	15	Training T02	N/A	N/A	Likely	M	Leadership –	1	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Incorporate C/EM into Home Station Training					leaders must know what their solider are being trained on		
37	C; A	15	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Moderate
37	D; A	15	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Minimal
37	D; A	15	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	2	Minimal
37	D; A	15	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Minimal
37	C;N&M	15	Personnel P01 Adapt 29A EW, 290A EW Tech, 29E EW Specialist	N/A	N/A	Likely	M	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
37	C;N&M	15	Personnel P02 Develop new 35A Cryptologic Cyber Analyst MOS	N/A	N/A	Likely	H	Doctrine – C/EM element, Organization (EW Element), training – additional training required	1	Major
37	C;N&M	15	Personnel P04 Institute special management procedures for specific ARCYBER experts	N/A	N/A	Likely	M	Policy – change policy for special management	3	Major
38	D; A	21	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
38	C; A	21	Training T04 Specialized Training	N/A	N/A	Likely	M	Facilities – must have adequate SCIFs at training venues; Leadership – leaders must know what their Soldiers are being trained on	3	Major, to ensure interoperability of information sharing
38	D; A	21	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate, however must be complete with other approaches to mitigate to acceptable operational risk
38	D; A	21	Leadership L02 Incorporate C/EM into 25, 29, & 35	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	2	Moderate, however must be complete

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Courses							with other approaches to mitigate to acceptable operational risk
38	D; A	21	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate, however must be complete with other approaches to mitigate to acceptable operational risk
40	D; A	13	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
40	D; A	13	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
40	D; A	13	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										to mitigate the gap
40	D; A	13	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
40	D; A	13	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
40	C; A	13	Materiel M01 Informational Systems: Application or set of applications to allow for the planning, integration, and synchronization of C/EM capabilities	L	M	Likely	M	Y, requires Training of new system(s)	1	Major, Materiel solutions will facilitate the integration of the C/EM contest and mitigate the gap
40	C; A	13	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
40	C; A	13	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
40	C; A	13	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Moderate
40	D; A	13	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
40	D; A	13	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	2	Moderate
40	D; A	13	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
45	D; A	22	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
45	A;A	22	Policy02 Update Title 10	N/A	N/A	Likely	M	Organization – might affect numbers of active duty required if	Mandatory	Major

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								DACs can execute cyber attack. Must incorporate policy changes into Training and Leadership courses		
45	D; A	22	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
45	D; A	22	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
45	D; A	22	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
45	D; A	22	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										to mitigate the gap
45	D; A	22	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
45	C; A	22	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
45	C; A	22	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
45	C; A	22	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Moderate
45	C; A	22	Training T04 Specialized Training	N/A	N/A	Likely	M	Facilities – must have adequate SCIFs at training venues; Leadership – leaders must know what their	2	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								Soldiers are being trained on		
45	D; A	22	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
45	D; A	22	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	3	Moderate
45	D; A	22	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Moderate
46	D; A	24	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
46	D; A	24	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
46	D; A	24	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										implemented to mitigate the gap
46	D; A	24	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
46	D; A	24	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
46	D; A	24	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
46	C; A	24	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
46	C; A	24	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
46	C; A	24	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel – must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on	1	Moderate
46	C; A	24	Training T04 Specialized Training	N/A	N/A	Likely	M	Facilities – must have adequate SCIFs at training venues; Leadership – leaders must know what their Soldiers are being trained on	4	Moderate
46	A B; A	24	Materiel M04 Evolutionary: C/EM modeling and simulation	L	L	Likely	M	Materiel- Must develop responsive C/EM M&S tools; Personnel to conduct M&S; and appropriate facilities	2	Moderate
46	C; A	24	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	5	Minimal
46	C; A	24	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	6	Minimal
46	C; A	24	Leadership L02	N/A	N/A	Likely	H	Personnel – must	6	Minimal

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Incorporate C/EM into 25, 29, & 35 Courses					have personnel to train C/EM		
46	C; A	24	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	6	Minimal
46	D; A	24	Facilities F02 C/EM Ranges	N/A	N/A	Likely	H	Personnel – to execute C/EM experimentation, testing, and training	3	Minimal
50	D; A	14	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
50	D; A	14	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
50	D; A	14	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
50	D; A	14	Doctrine D03 Modify	N/A	N/A	Likely	M	Must incorporate	Mandatory	Major,

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			Element of Army Combat Power Doctrine					doctrine changes into Training and Leadership courses		however all doctrine approaches must be implemented to mitigate the gap
50	D; A	14	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
50	D; A	14	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
50	C; A	14	Training T01 Incorporate C/EM into Individual Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
50	C; A	14	Training T02 Incorporate C/EM into Home Station Training	N/A	N/A	Likely	M	Leadership – leaders must know what their solider are being trained on	1	Moderate
50	C; A	14	Training T03 Incorporate C/EM into Collective Training	N/A	N/A	Likely	H	Facilities – must have adequate SCIFs at training venues; Personnel	1	Moderate

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
								– must have personnel to train C/EM; Leadership – leaders must know what their Soldiers are being trained on		
51	D; A	25	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
51	B;N&M	25	Personnel P05 25E EMSO	N/A	N/A	Likely	M	Training – would increase the number needing to be trained	Mandatory	Closes the Gap
52	D; A	20	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
52	D; A	20	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
52	D; A	20	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										gap
52	D; A	20	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
52	D; A	20	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
52	D; A	20	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
52	D; A	20	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Major, Required to ensure effective operational use of other approaches
52	D; A	20	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	2	Major, Required to ensure effective

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										operational use of other approaches
52	D; A	20	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Major, Required to ensure effective operational use of other approaches
53	D; A	26	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
53	B;N&M	20	Personnel P05 25E EMSO	N/A	N/A	Likely	M	Training – would increase the number needing to be trained	Mandatory	Closes the Gap
54	D; A	27	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Training, Leadership	Mandatory	Major
54	D; A	27	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
54	D; A	27	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										to mitigate the gap
54	D; A	27	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
54	D; A	27	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
54	D; A	27	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, however all doctrine approaches must be implemented to mitigate the gap
57	D; A	4	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
57	D; A	4	Doctrine D01 Modify Army Capstone Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, changes in doctrine facilitate implementation

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										of other approaches
57	D; A	4	Doctrine D02 Modify Army Warfighting Functional Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, changes in doctrine facilitate implementation of other approaches
57	D; A	4	Doctrine D03 Modify Element of Army Combat Power Doctrine	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, changes in doctrine facilitate implementation of other approaches
57	D; A	4	Doctrine D04 Rewrite FM 3-36 as the C/EM Activities FM	N/A	N/A	Likely	H	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, changes in doctrine facilitate implementation of other approaches
57	D; A	4	Doctrine D05 Modify Other & Supporting Doctrine Solutions	N/A	N/A	Likely	M	Must incorporate doctrine changes into Training and Leadership courses	Mandatory	Major, changes in doctrine facilitate implementation of other approaches
57	D; A	4	Leadership L01 Incorporate C/EM into PME	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Major, Required to ensure effective operational use of other

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
										approaches
57	D; A	4	Leadership L02 Incorporate C/EM into 25, 29, & 35 Courses	N/A	N/A	Likely	M	Personnel – must have personnel to train C/EM	2	Major, Required to ensure effective operational use of other approaches
57	D; A	4	Leadership L03 Incorporate C/EM into Exercises	N/A	N/A	Likely	H	Personnel – must have personnel to train C/EM; Facilities – potential need of SCIFs at training venues	1	Major, Required to ensure effective operational use of other approaches
57	A B; A	4	Materiel Approach M05 Evolutionary: Defend and Protect Individuals and Platforms	L	L	Likely	H	N	1	Major, but unlikely to mitigate operational risk without all other approaches
57	C; A	4	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	4	Moderate
57	D; A	4	Facilities F02 C/EM Ranges	N/A	N/A	Likely	H	Personnel – to execute C/EM experimentation, testing, and training	3	Moderate
61	D; A	5	Policy01 Incorporate C/EM into Policy	N/A	N/A	Likely	M	Must incorporate policy changes into Training and Leadership courses	Mandatory	Major
61	C; A	5	Materiel Approach	M	M	Likely	H	Y, requires	1	Closes the

Gap #	Gap type & time-frame[1]	Gap Priority	Materiel[2] or non-Materiel Approach	METRICS					Priority of Approach	Impact on Gap
				Technical Risk	Support-ability	Feasibility	Affordability	DOTMLPF Implications		
			M06 Evolutionary: C/EM Research, Development, Testing, and Evaluation (RDT&E) and Research, Development, and Acquisition (RDA) Enterprise					Organizational changes, new Training, new RDT&E and RDA Materiel, may require new personnel and new testing and evaluation Facilities.		Gap
61	C;M&L	5	Personnel P06 GENFOR C/EM DA Civilians	N/A	N/A	Likely	H	Organization – would add DACs, Training – would increase the number needing to be trained, Leader Development – would need to be developed	2	Major, however requires M06 to be effective
61	C; A	5	Facilities F01 SCIFs	N/A	N/A	Likely	H	Personnel – security manager & appropriate clearances	3	Moderate, must be completed with M06 to mitigate congruent with operational risk
61	D; A	5	Facilities F02 C/EM Ranges	N/A	N/A	Likely	H	Personnel – to execute C/EM experimentation, testing, and training	4	Moderate, must be completed with M06 to mitigate congruent with operational risk

1