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

Final Report

DRAFT V 0.9

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) WITHOUT ANNEXES C & D

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

For Official Use Only
Distribution authorized to U.S. Department of Defense elements and their contractors (operational information). This determination was made on **24 October, 2010**. Other requests for this document shall be referred to the U.S. Combined Arms Center.

Table of Contents

Table of Figures

Table of Tables

Cyber/Electromagnetic Contest Capabilities Based Assessment Executive Summary

Introduction

(U//FOUO) Trends in the operational environment continue to indicate that cyberspace and the electromagnetic spectrum (EMS) will remain important entities within the operational environment for the foreseeable future. The Army understands the importance of cyberspace and the electromagnetic spectrum to human societies in general, and to military operations specifically. Army leaders and Soldiers must possess an in-depth understanding of this contest, and how to gain, maintain, and leverage advantages in this contest. To this end, the Army Concept Framework recognizes an increasingly important aspect to military operations: the "cyber/electromagnetic contest (C/EM contest)".

(U//FOUO) Understanding how to posture the Army to fight the C/EM contest is critical to success on the future battlefield. The Commanding General, Training and Doctrine Command directed the Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA) to gain a holistic review of the Army's required capabilities. The study's objective was to identify C/EM requirements across Full Spectrum Operations, then assess capability gaps and potential solutions.

Scope

(U//FOUO) This study considered Army echelons that include BCT to Army and Joint echelons. It considered all phases of Joint operations and the ARFORGEN cycle from reset and pre-deployment to deployment through power projection platforms to the theater of operations and addresses requirements from the 2016-2028 timeframe.

The Cyber/Electromagnetic Contest

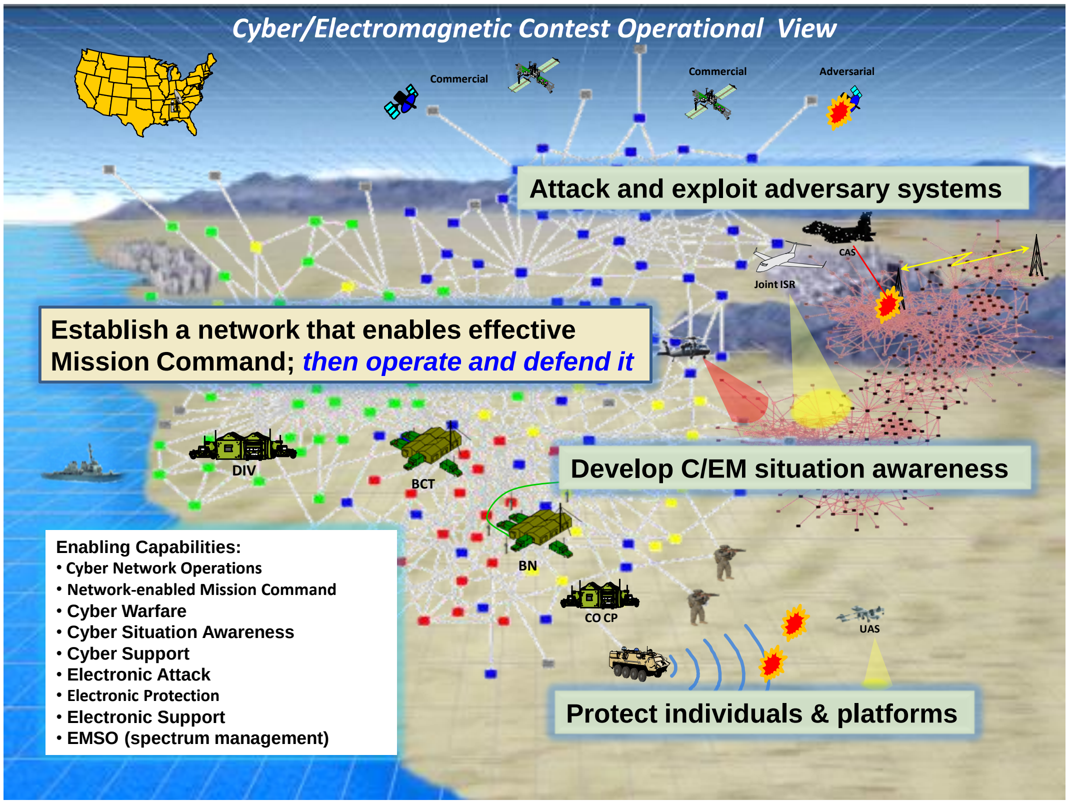
(U//FOUO) The C/EM Contest is defined as "That dimension of full spectrum operations which aims to gain advantage, maintain that advantage, and place adversaries at a disadvantage in the increasingly contested and congested cyberspace domain and electromagnetic spectrum". The C/EM Contest is a holistic, combined arms approach that offers five key ideas:

- (U//FOUO) Cyberspace and the EMS are 'commander's business' and activities in these mediums must be fully integrated within the overall operation.
- (U//FOUO) Today's environment requires an expanded notion of combined arms operations. Commanders must think broadly and employ the full range of their capabilities to win the contest.
- (U//FOUO) The Cyberspace domain and the EMS must be thought of as maneuver space where positional advantage can be gained or lost.

- (U//FOUO) Cyberspace operations and EMS operations have converged in technology and must converge operationally; many times drawing on the same capabilities to meet objectives in either.

- (U//FOUO) Winning the contest (maintaining our freedom of action in the cyberspace domain and the EMS while denying our adversaries the same) greatly facilitates our efforts; and if not, our operations can be severely degraded.

(U//FOUO) The fundamental objective of the C/EM contest is to establish a network that enables effective Mission Command; then operate and defend it. In conjunction with this primary effort, commanders seek to develop C/EM situational awareness, which enables all aspects of the C/EM Contest. Operations are directed to attack and exploit adversary systems, and to protect friendly individuals and platforms. Support activities underpin these efforts to gain and maintain advantages.



Cyber/Electromagnetic Contest Operational View

Attack and exploit adversary systems

Establish a network that enables effective Mission Command; ***then operate and defend it***

Develop C/EM situation awareness

Protect individuals & platforms

Enabling Capabilities:
- Cyber Network Operations
- Network-enabled Mission Command
- Cyber Warfare
- Cyber Situation Awareness
- Cyber Support
- Electronic Attack
- Electronic Protection
- Electronic Support
- EMSO (spectrum management)

(U) Figure 1: C/EM Contest Operational View

Methodology

(U//FOUO) The C/EM CBA used a collaborative and multidisciplinary approach within a JCIDs framework and took a joint perspective. The effort began with an extensive literature search, concurrent with the building of the study team. The second step was a Functional Area Analysis (FAA) that identified and defined the tasks, conditions, and standards for C/EM capabilities. The third step was a Functional Needs Assessment (FNA), which assessed the ability of current and programmed capabilities to accomplish the tasks identified in the FAA. The final step was a Functional Solution Assessment (FSA), which developed and assessed potential doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) approaches to solving gaps.

The Study Team

(U//FOUO) The C/EM CBA leveraged not only the Army community but also Joint, Industry and academia expertise. Its analytic team included subject matter experts, force developers, concept writers, PEOs and PMs, leaders of cyber units, and analysts. Membership included ARCIC, CAC, CADD, IPO, EWPO, TRAC, TRISA, HQDA G-3/5/7, HQDA ACTF, 1ST IO Command, 704TH MI BDE, 744 MI BN, ARCYBER, ARL, FIRES COE, DIAP, Intelligence CoE, I2WD, INSCOM, National Simulations Center, NETCOM, NGB ARNG, MS CoE, RAND Corporation, SMDC ARSTRAT, SOCOM, Signal CoE, USAR ARIOC, USASOC, and USCYBERCOM.

The Future Operational Environment and CBA Scenarios

(U//FOUO) In order to fully reflect the future operational environment, the study used a total of eight vignettes drawn from scenarios illustrating threats operating conventionally and unconventionally employing adaptive and asymmetric combinations of traditional, irregular and criminal tactics. These threats challenged US access – directly and indirectly, and employed very sophisticated information campaigns combined with attacks on the US homeland. Finally, these vignettes included an omnipresent media potentially giving local events global significance.

Overall Conclusions and Implications

(U//FOUO) The study team’s examination of the future environment, concepts, previous studies, and scenarios led to implications regarding the Army’s requirements for the C/EM contest. These conclusions and implications follow.

Requirements for Commanders and Units

(U//FOUO) Understanding how the EMS and cyber influences the operational environment is an essential responsibility for leaders – it is commander’s business. Leaders must grasp how they can leverage C/EM capabilities to their advantage and how to ensure that misuse of the EMS and cyberspace will not debilitate their operations. This implies that commanders must be able to create the necessary C/EM conditions throughout their area of operations. This also implies that staffs must possess analytic tools and processes to adequately address the C/EM contest as their bosses apply the art of command. Units will require sufficient capacity to adeptly apply multiple capabilities. The dynamic nature of the C/EM contest highlights the importance of synchronization and close collaboration among all mission elements. Staying ahead requires timely, high quality, continuous C/EM situation awareness to enable high quality decisions. This awareness combines the latest intelligence with real-time awareness of the status of networks to facilitate command and control at all echelons, and rapidly respond to early warning of C/EM attack.

Implications for the Network

(U//FOUO) The study used the LandWarNet (LWN) definition of network, which consists of five layers: platforms and sensors, applications, services, transport infrastructure, and standards. The 'five layer' perspective helped illustrate the linkage between larger networks and individual systems within the overall C/EM contest. Future adversaries will be able to employ sophisticated C/EM techniques over time to gain ability to disrupt or degrade key nodes/sensors and portions of our networks. Therefore, the Army's network strategy needs to address specific design features that provide resiliency as well as enable mission command. These attributes include:

- (U//FOUO) C/EM infrastructure with the technological diversity and capacity to enable Army forces to respond to, bypass, and fight through network intrusions, and allow Army forces to continue to operate even when systems are degraded or disrupted.
- (U//FOUO) Redundant methods of transmitting, receiving, and storing information.
- (U//FOUO) Features that allow commanders to train and prepare to operate networks under suboptimal conditions.
- (U//FOUO) Create the necessary foundation for offensive and defensive C/EM capabilities by equipping selected systems to be C/EM platforms and delivery systems.

Maintaining Technical Advantage

(U//FOUO) In order to gain and maintain an advantage in the C/EM Contest, the Army must pursue a framework of materiel (tools, weapons) and tactics, techniques, and procedures (TTPs). Most devices today, down to the individual Soldier level, possess "IP components" which leverage cyberspace, and "electronic apertures" which leverage the electromagnetic spectrum. Networks and systems use cyberspace/EMS in an integrated way – the attendant tools, weapons and TTPs must also be integrated. These components and apertures allow our devices/systems to function yet also represent vulnerabilities.

(U//FOUO) A focused dialogue between intelligence, operations, and materiel developers is required to develop the best possible combinations of tools, weapons, and TTP. Given the agile and innovative nature of our adversaries, this interaction must be very dynamic. The tools, weapons, and TTP are not limited to C/EM capabilities but are dictated by the capabilities available to the commander. Maintaining a technical edge in the C/EM Contest requires dynamic discernment of both adversarial and friendly requirements, capabilities, & vulnerabilities, combined with innovative development of tools, weapons, and TTPs.

(U//FOUO) In order to have the best possible infrastructure for the C/EM contest, Army formations will need the best combination of platforms, delivery systems, and payloads. Materiel development must provide the best possible combination of programs of record and quick reaction capabilities.

The Implications of Convergence

(U//FOUO) This study carefully studied the current state and future trends of convergence between cyber and EMS capabilities. There is overwhelming evidence of convergence, but not to the point of absorption. Technological advances are increasingly dictating the interrelatedness and interdependence of cyber and EMS capabilities in order to maximize the full potential of both. Cyber is reliant on the EMS, as networks and telecommunication infrastructures expand their use of wireless means. Our sensors (also part of the network) require the EMS in order to collect and disseminate information. Conversely, integrated electronic warfare and electromagnetic spectrum operations systems generate requirements for a viable network, and, therefore, a dependence on cyber. This is particularly important for collaborative systems, such as the proposed Integrated Electronic Warfare System, which require a network to operate effectively. Our analysis indicates that future capabilities will increasingly be unified single solutions with both cyber and EW aspects.

FAA: Overall Conclusions

(U//FOUO) The FAA is the most critical portion of any CBA, as it examines the future environment, defines the conditions under which our forces will fight, and establishes the required capabilities for success. The study team reached the following conclusions regarding the Army's requirements for the C/EM contest.

- (U//FOUO) Cyberspace and the EMS are deeply inter-related with physical domains (air, land, sea, space). The entities (soldiers, devices, systems) that leverage cyberspace and the EMS all reside in the physical domains. C/EM capabilities are able to create effects in the physical, and conversely conventional capabilities are able to contribute to effects in cyberspace and the EMS. Therefore, C/EM activities blend all capabilities together for a combined arms approach to desired objectives.

- (U//FOUO) C/EM is an integral part of every operation – at every echelon. Since the 2006-2007 timeframe, there is growing evidence that governments, militaries, and non-state actors utilize cyberspace and the electromagnetic spectrum for military and political objectives. Moreover, they are using C/EM capabilities in a sophisticated and highly integrated fashion with conventional capabilities. At the same time our forces rely on C/EM for communication, navigation, lethality, and survivability.

- (U//FOUO) Cyberspace and the electromagnetic spectrum have 'echelon-independent' characteristics. A global context is needed, yet each echelon must be enabled to be part of the overall enterprise. Provision must be made for capabilities resident at one echelon to be available and responsive to needs at other echelons.

- (U//FOUO) The complexion of the C/EM contest changes across echelons. At lower echelons the focus is more on individuals and specific systems (e.g.

counter-IED or tracking key adversaries). At higher echelons the focus is more on networks and groups of targets. Although the 'target set' changes across echelons, the constant is that the systems involved all have IP components and electronic apertures.

- (U//FOUO) Sophisticated adversaries will seek to fragment and isolate our formations and their supporting networks. Provisions must be made to 'compartmentalize' the network, and allow units to be able to operate in isolation and under degraded conditions.

- (U//FOUO) New and innovative acquisition processes are necessary. Current acquisition processes, and management of those processes, do not ensure a commander's ability to win the C/EM contest.

FAA: Organic Capabilities

(U//FOUO) While the FAA conducted thorough analysis across all Army formation and echelons, it focused on those units that most clearly needed C/EM performed as part of their mission set. In general terms, organic capability is needed when units require immediate and highly responsive and complex C/EM capabilities to perform their mission. Based on subject matter expert input, workshops, other studies' conclusions, and the full range of scenarios and vignettes, capabilities were placed into two categories: "organic" versus "access to". Organic capability is defined as that capability which must reside with an echelon, included on their associated table of organization and equipment. Access is defined by the ability of an echelon to request and employ additional support that is not resident in the organization on a permanent basis. Specific organic required capabilities include:

- (U//FOUO) All echelons require the ability to have C/EM situation awareness and to integrate C/EM activities as part of their overall mission.

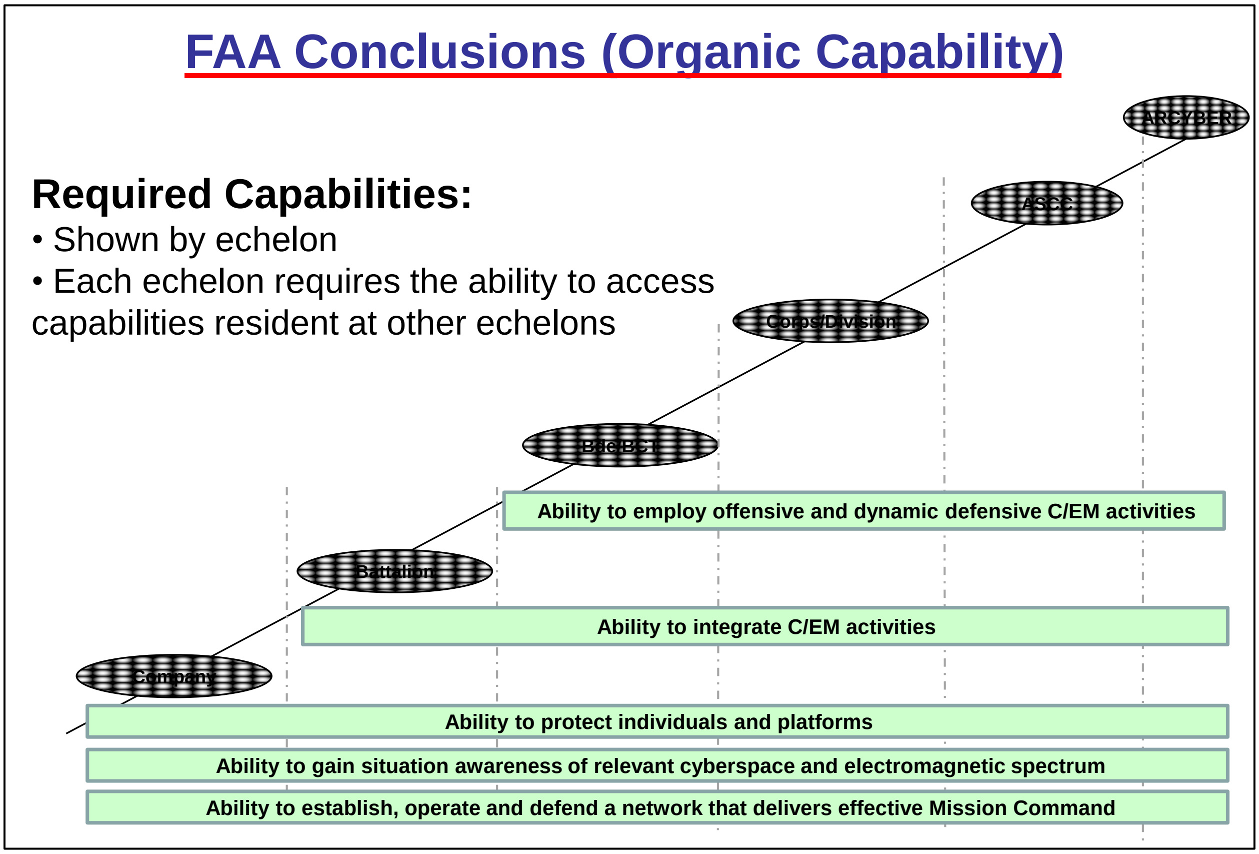
- (U//FOUO) All echelons require the ability to leverage the overall network enterprise and require Mission Command essential capabilities.

- (U//FOUO) BCT/Brigade and above echelons require the ability to employ offensive C/EM capabilities and dynamic defense capabilities within their area of operations. This includes air and ground, organic and supporting capabilities.

- (U//FOUO) All echelons require capability to protect individuals and platforms.

- (U//FOUO) Select functional and multifunctional brigades require capabilities that provide access to adversaries' networks for exploitation and attack purposes. These brigades will support corps and divisions with this capability.

- (U//FOUO) BCT/Brigade requires capability to collect and exploit adversary capabilities and responsively support the operation.



FAA Conclusions (Organic Capability)

Required Capabilities:

- Shown by echelon
- Each echelon requires the ability to access capabilities resident at other echelons

Ability to employ offensive and dynamic defensive C/EM activities

Ability to integrate C/EM activities

Ability to protect individuals and platforms

Ability to gain situation awareness of relevant cyberspace and electromagnetic spectrum

Ability to establish, operate and defend a network that delivers effective Mission Command

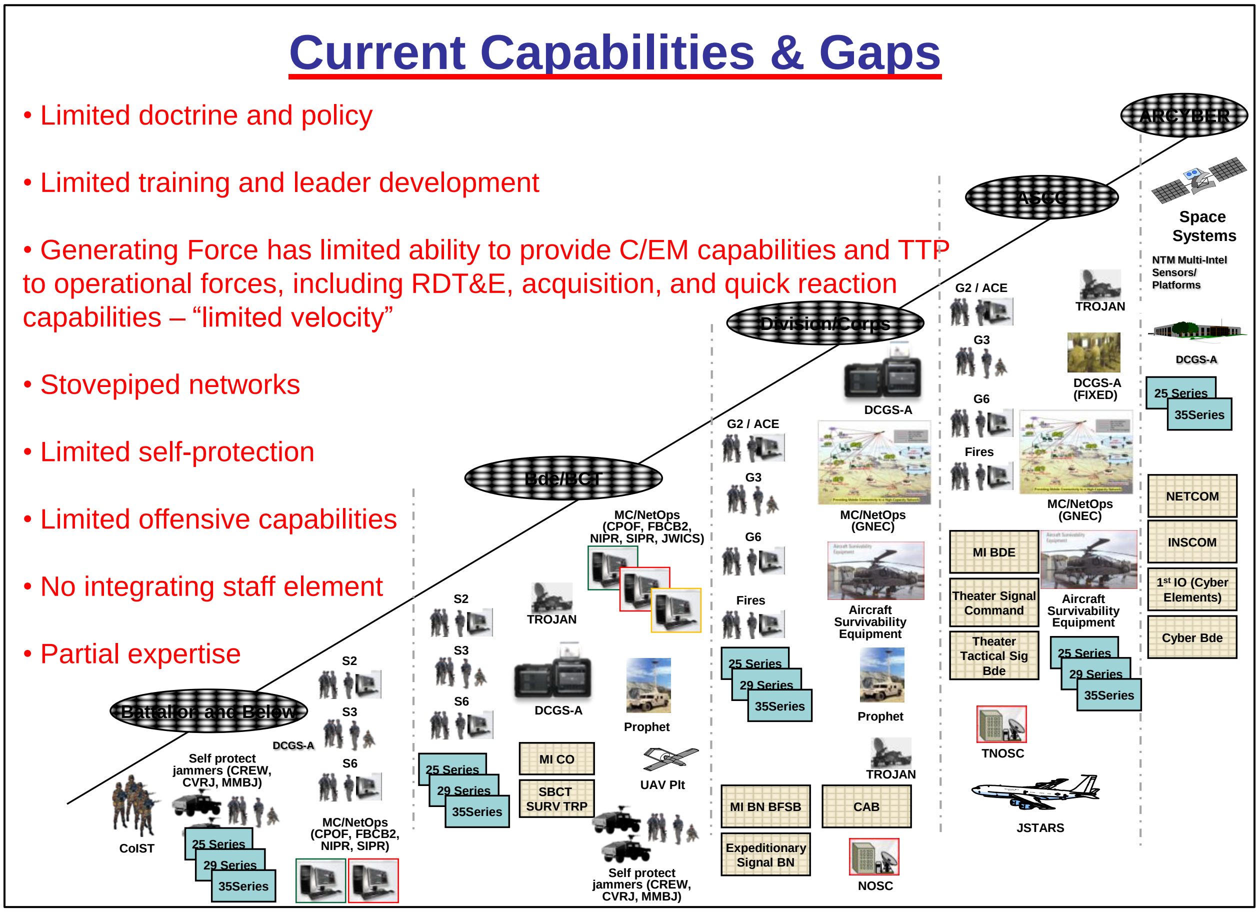
(U//FOUO) Figure 2: FAA Conclusions

Functional Needs Analysis Results
(U//FOUO) The FNA identified 27 capability gaps which fell within five broad categories. The Army has limited ability to:

- Integrate C/EM activities and generate C/EM situational awareness
- Establish, operate, and defend networks which provide Network-enabled Mission Command
- Develop and field materiel solutions to mitigate and defeat new and evolving capabilities.
- Conduct offensive C/EM and dynamic defense actions
- Defend and protect individuals and platforms

(U//FOUO) Gaps were prioritized by carefully selected C/EM subject matter experts from across the Army. Gaps were assessed by probability and severity, in accordance with the methodology from FM 5-19. The overall critical areas were (in priority order) #1

Operate and defend the network and network enabled Mission Command; #2 Defending individuals and platforms; #3 Assessing current and potential threats; #4 Operational Integration; and #5 Offensive capabilities.



Current Capabilities & Gaps

- Limited doctrine and policy
- Limited training and leader development
- Generating Force has limited ability to provide C/EM capabilities and TTP to operational forces, including RDT&E, acquisition, and quick reaction capabilities – "limited velocity"
- Stovepiped networks
- Limited self-protection
- Limited offensive capabilities
- No integrating staff element
- Partial expertise

(U//FOUO) Figure 3: FNA Conclusions

FSA Conclusions and Recommendations

(U//FOUO) To prevail in the C/EM contest will require significant advancements in doctrine, organization, training and leader development, personnel, facilities, and materiel. There are also numerous policies which will require change to increase the synergistic effects. Optimizing these capabilities will require us to inculcate a mindset within the Army that appreciates and understands the implication of the C/EM contest, builds a professional force with the requisite skills to operate effectively within the C/EM contest and provide the tools needed to best apply those skills. CBA recommendations in priority order include:

- (U//FOUO) Modify Capstone and supporting doctrine to internalize the C/EM Contest from both an institutional and operational perspective. These changes are low cost, feasible, and will generate the necessary mindset within the force.

Pursue policy changes to increase the Army's flexibility to pursue the C/EM contest.

- (U//FOUO) Create a C/EM Integration Staff Element, and a corresponding Cyber/Electromagnetic Working Group, Battalion through ASCC. Leverage the existing EW staff element and Working Group as the foundation for this element and Working Group. If additional resources are available add additional C/EM-related personnel to this new element for additional capacity.

- Add and adapt 25, 29, and 35 series career fields to the C/EM Element to provide necessary C/EM integration and technical expertise and additional capacity.

- (U//FOUO) Reconfigure elements within Expeditionary Signal Brigades, NETCOM, TNOSCs, NECs, and unit G6/S6 staff elements to better support Cyber NETOPS. These are no growth changes

- (U//FOUO) Modify and leverage the Army Network Modernization Strategy Framework by modifying the Network Enabled Mission Command (NeMC) ICD, future Integrated Electronic Warfare System (IEWS) Initial Capability Document (ICD) and LWN ICD in order to achieve the desired network enterprise, fully equip units for Network-enabled Mission Command, and provide the means for units to be effective across cyberspace and electromagnetic spectrum. Incrementally field capabilities using the LANDWARNET capability set framework.

- (U//FOUO) Incorporate C/EM challenges into Leader Development, Education and Training. Examples include individual training, collective training, and specialty training for C/EM professionals. These changes build on existing EW training initiatives.

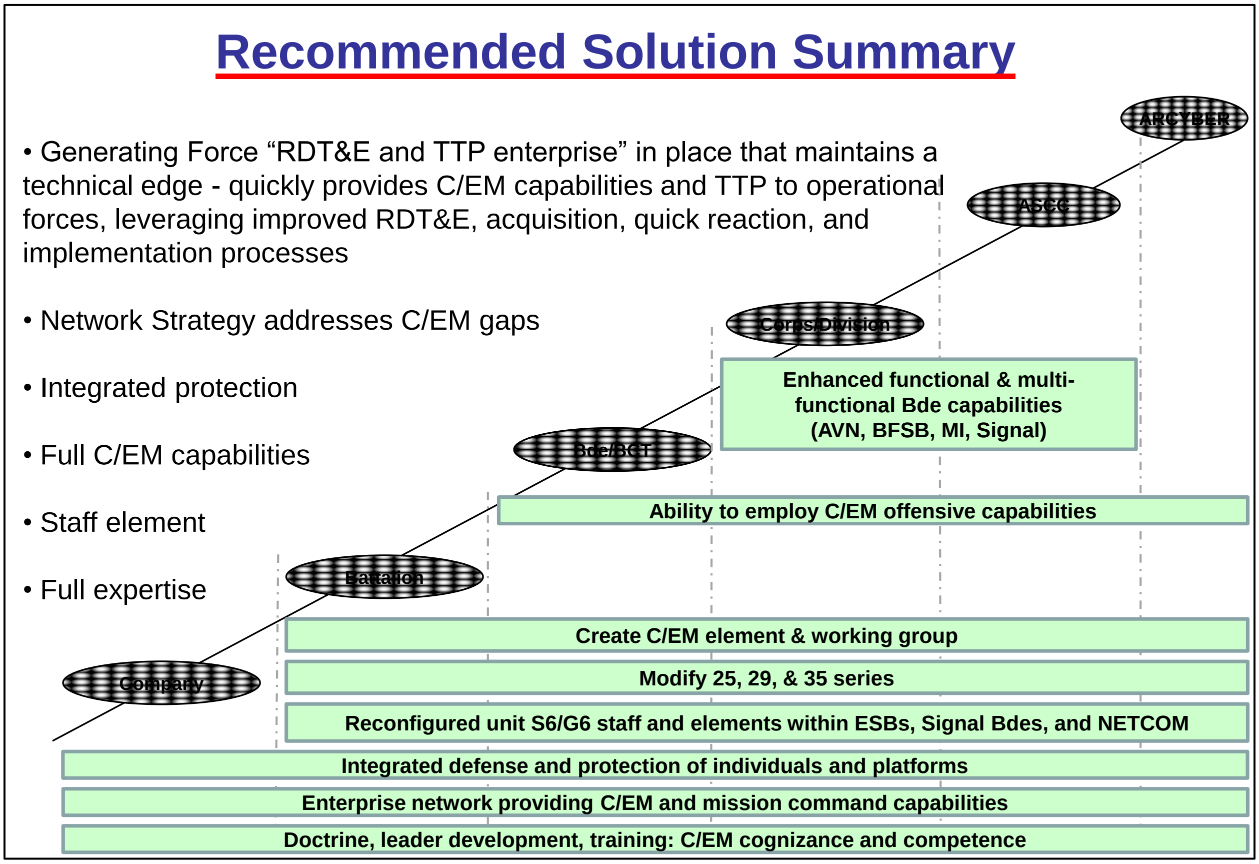
- (U//FOUO) Modify the LWN ICD, NeMC ICD, IEWS ICD, and platform specific defensive suites to integrate defense and protection of individuals and platforms efforts. This will ensure the proper integration of individual and collective protective systems leveraging network, IEWS, and platform-specific countermeasure suites.

- (U//FOUO) Rely on Quick Reaction Capability programs to providing C/EM unique delivery systems and payloads in a timely manner and maintain currency of tools for threat hardware and software exploitation and vulnerability assessments.

- (U//FOUO) Modify the Army's Modeling and Simulation Strategy to provide C/EM modeling and simulation capabilities for analytic, experimentation, operational, and training purposes.

- (U//FOUO) Develop a C/EM RDT&E, RDA and TTP Enterprise to satisfy the Army's need for a responsive means to provide timely materiel solutions to the operational force.

- (U//FOUO) Ensure adequate facilities are available at the strategic, operational, and tactical levels in order to conduct C/EM activities.



Recommended Solution Summary

• Generating Force "RDT&E and TTP enterprise" in place that maintains a technical edge - quickly provides C/EM capabilities and TTP to operational forces, leveraging improved RDT&E, acquisition, quick reaction, and implementation processes

• Network Strategy addresses C/EM gaps

• Integrated protection

• Full C/EM capabilities

• Staff element

• Full expertise

Enhanced functional & multi-functional Bde capabilities (AVN, BFSB, MI, Signal)

Ability to employ C/EM offensive capabilities

Create C/EM element & working group

Modify 25, 29, & 35 series

Reconfigured unit S6/G6 staff and elements within ESBs, Signal Bdes, and NETCOM

Integrated defense and protection of individuals and platforms

Enterprise network providing C/EM and mission command capabilities

Doctrine, leader development, training: C/EM cognizance and competence

(U//FOUO) Figure 4: Solution Summary

Section I: Introduction to the Full Report

1-1 Point of Contact For C/EM CBA Report

Mr. Malcolm W. Martin
Senior Analyst for Cyber Concepts
CAC/CDID Concepts Determination Division
806 Harrison Drive, Pope Hall
Ft. Leavenworth, KS 66027
(913)684-4600 office
(312)552-4600 DSN
(913)991-3505 mobile
SIPR: malcolm.w.martin@us.army.smil.mil
JWICS: malcolm.w.martin@army.ic.gov

1-2 Acknowledgements

(U) This CBA succeeded due to dedication and sustained involvement by numerous organizations as well as many subject matter experts. While there have been many participants there have been several "stalwart" individuals who are directly responsible for the successful completion of the CBA. We would like to acknowledge their support. Mr. Russ Fenton, Mr. Les Caster, Mr. Jeff Hoing, Mr. Jac Shipp, LTC Jenn Easterly, Mr. Mike Fox, Mr. Joe Thompkins, COL Tim Chafos, LTC Eric Toler, Mr. Giorgio Bertoli, Mr. Frank Silva, MAJ Brady Stout, CPT Brian Olsen, Mr. Steve Swartwood, MAJ Tom Addyman and Ms. Carol Parks.

The individuals and agencies listed below are recognized for their significant contributions to this Cyber/Electromagnetic Capabilities Based Assessment Study. Many other individuals at these named agencies and other agencies contributed to this effort as well.

Agencies	Role	Individuals
CAC Study Leadership	Study Director	COL Jeffrey Witsken
	Study Lead	Mr. Malcolm Martin
	Study Analysis	Mr. Jim Richter
		Mr. John Slater
		Ms. Carol Parks
		Mr. Ian Edmonston
		Ms. Jennifer Hollock
		Mr. Dan Arthur
		Mr. Paul Layman
ARCIC		COL Jet Bibler
		MAJ Buddy Janovsky
		Mr. Steve Swartwood

	Mr. Lowell Asher Mr. Larry Jennings
CAC, CDID CDD	Mr. Steve Edwards Mr. Wesley Farmer Mr. Jeff Hoing
CAC, CDID RDD	COL Michael Armstead
CAC, IPO	COL Mike Dominique Mr. Cameron Wesson
CAC, EWPO	COL Joe Howard LTC Kevin Romano Mr. Tony McNeill Mr. Greg Buehler Mr. Chester Wilson Mr. Wade Melton Mr. Brian Gerling
CAC, CADD	LTC Jeffrey LaFace Mr. Clint Ancker Mr. Michael Flynn
CAC G-3	Mr. Howard Brewington
TRAC	Mr. Duane Riddle Mr. Cody Beck
TRISA	Mr. Gregory Lee
HQDA G-3/5/7 DAMO-ODE	Mr. Jeffrey Edgell Mr. Rhon Say
HQDA G3/5/7 DAMO-ODI	LTC Chris Reichart
HQDA ACTF	COL Dawnlee Deyoung
1ST IO Command	COL Michael Miller LTC Bryant Glando Mr. Richard Simon
704TH MI Brigade	MAJ Brady Stout MAJ Rebekah Barnes CW4 Mark Mollenkoph

744th MI Battalion	LTC Eric Toler LTC Jennifer Easterly CPT Brian Olson
ARCYBER	COL Timothy Chafos
ARL	Mr. Chuck Smith
Fires Center of Excellence	LTC James Looney 1SG David Howard Mr. John Caudill Mr. Tom Arnold
DIAP	Mr. Steven Busch
Intelligence Center of Excellence	COL Brian Moore MR. Roy Fox MSG Theresa Robinson Mr. Leslie Caster Mr. Reginald Story Mr. Anthony Riggio Mr. Lou Frere
I2WD	Mr. Giorgio Bertoli Mr. Jeffery D'Arcy Mr. Frank Silva
INSCOM	COL Alex Cochran LTC Ralph Taylor CW2 Keisha Moss Mr. Bill McNeill Mr. Greg Platt Mr. Tom Wetzel Mr. Joe Thompkins Mr. Robert Trantin Ms. Gwendolyn King
National Simulations Center	Mr. Kurtis Ritchey
NETCOM	Ms. Elizabeth Patten Mr. Rod Trevino Mr. Byron McNeill Mr. Norman Mims Mr. Aaron O'Hara Mr. Jim Fegler Mr. Wayne Trader

NGB ARNG	COL Fred Bolton
	LTC Robert Quinker
	MAJ Gordon Matthews
MS Center of Excellence	Mr. Frank Chapman
RAND	Dr. Elliot Axelband
	Dr. Isaac Porche
SMDC ARSTRAT	Mr. David Carrithers
	Mr. Jac Shipp
	Mr. Jon Millner
	Mr. Michael Muatafago
	Ms. Sue Randles
	Mr. Pete Dykman
SOCOM	Mr. Joseph Primosch
Signal Center of Excellence	COL Michael Kell
	LTC Maureen O'Connor
	MAJ Thomas Addyman
	CW5 Todd Bodreau
	SFC Neftali Diaz
	Mr. Russell Fenton
USAR ARIOC	COL John Diaz
	LTC Mike Holland
	LTC John Garnsey
	LTC Gail Owen
USASOC	COL William Lee
	MAJ Michael Ignacio
	Ms. Mia Kelly
USCYBERCOM	Mr. Paul Schuh

(U) The development of the Cyberspace Operations Concept to Capability Plan (CCP), and the completion of the Cyber/Electromagnetic CBA by the Combined Arms Center was a two year effort. This marathon effort was not possible without the continued support of the Army, Navy, Marine Corps, and Air Force. Industry and Academia also participated, providing support, insight and analysis.

1-3 Participants of the C/EM CBA

(U//FOUO) Throughout this study, CAC has leveraged not only the Army community but also Joint, Industry and academia. Starting with the Information & Cyberspace and Electronic Warfare ICDTs, numerous organizations have been added to the study team. Participants of the C/EM Contest CBA include (but were not limited to): CAC, ARCIC, SMDC/ARSTRAT ARCYBER, ACTF (HQDA, G-6, G-8), DA G3/5/7 DAMO-ODE (EW), INSCOM, NETCOM/9th SC(A), TRADOC, Army War College, CGSC, USA JFK SWC, HQDA G3/5/7 DAMO-ODI (IO), HQDA G3/5/7 DAMO FM (Force Mgmt), DCS G-3/5/7, HQDA G2, 1st IO CMD (Land), SOCOM, CENTCOM, USASOC, USAR/ARIOC, ARNGB, CERDEC/I2WD, TRAC, JFCOM, MARCYBER, USMC/MCCDC, USMC/MCIOC (IO Cmd), USMC/HQMCPLI (IO & Space Integration), USN/10th NAVFLEET (NAVFORCYBER), USN SPAWAR, USAF, USSTRATCOM, Kansas University, RAND Corporation and MITRE.

(U) To the Army and Joint community, thank you for the patience, continued support and desire to do what is best for the Army. We look forward to continuing to work with you all in the future efforts as we look to build capability and capacity within the world's greatest Army.

1-4 Introduction

(U//FOUO) The Cyber/Electromagnetic Contest (C/EM) is defined as "that dimension of full spectrum operations which requires military forces to gain an advantage, protect that advantage and place adversaries at a disadvantage, across both cyberspace and the electromagnetic spectrum." This definition acknowledges the ever-increasing convergence of cyberspace and the electromagnetic spectrum (EMS).

(U//FOUO) The continued growth of cyberspace and convergence of cyberspace and the EMS requires analysis to a determination if the Army is optimally organized and manned to address the C/EM dimension of full spectrum operations. The C/EM CBA is that analysis to identify required Army cyberspace and electromagnetic spectrum capabilities for Army echelons, to include BCT, to Army and Joint echelons.

(U//FOUO) The CBA conforms to the Joint Capabilities Integration and Development System (JCIDS) process as outlined in Chairman of the Joint Chiefs of Staff Instruction 3170.01G, *Joint Capabilities Integration and Development* and identifies capability gaps and potential solutions with regard to cyber/electromagnetic contest required capabilities. This final report provides an overview of the study and is maintained at the Unclassified//For Official Use Only (U//FOUO) classification level. Each major part of the CBA (FAA, FNA & FSA) is included in the overall report as annexes (FAA is Appendix C, FNA is Appendix D, FSA is Appendix E). Each Annex has additional sections due to classification requirements of the information and resides on the appropriate classified system:

- Classified FAA: Appendix C on SIPR and on JWICS
- Classified FNA: Appendix D on SIPR and on JWICS
- U//FOUO FSA: On Nipr and SIPR
- Classified FSA: Appendix E on SIPR and on JWICS

1-5 Purpose

(U//FOUO) The C/EM CBA is 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). The objective is to identify outcomes-based, integration-focused, and resource-informed solutions which will enable the U.S. Army to prevail in the cyber-electromagnetic contest.

1-6 Problem Statement

(U//FOUO) The Army lacks sufficient capabilities and capacity to fully leverage the cyberspace domain and the EMS in order to prevail in the Cyber/Electromagnetic contest. Army cyber and electromagnetic spectrum capabilities are not fully integrated in the right combination, both internally and with joint/interagency capabilities, to gain the advantage, protect that advantage and place adversaries at a disadvantage within specified authorities.

1-7 Background

(U//FOUO) This report documents the Cyber/Electromagnetic (C/EM) Contest Capabilities Based Assessment (CBA) and is the culmination of over two years of conceptual developments, analytic rigor, cooperation and collaboration. On 16 October, 2009, TRADOC CG provided, to the Chief of Staff of the Army (CSA), a recommended way forward regarding Cyberspace, Electronic Warfare (EW) and Information Operations (IO) in terms of concepts, force modernization and implications across Army DOTMLPF. TRADOC recommended conducting a CBA to determine how the Army should provide the necessary capabilities in the cyber/electromagnetic dimension of full spectrum operations (FSO). In conjunction, the Army Capabilities Integrating Center (ARCIC) directed the C/EM CBA in order to conduct a holistic review of the Army's required capabilities necessary to operate in and through both the cyberspace domain and the electromagnetic spectrum as a holistic and integrated part of FSO. The objective was to identify outcomes-based, integration-focused, and resource-informed solutions which can enable the U.S. Army to prevail in the Cyber/Electromagnetic Contest.

Section II Overview

2-1 Scope of the C/EM CBA

(U//FOUO) This study considered Army echelons that include BCT to Army and Joint echelons. It considered all phases of Joint operations and the ARFORGEN cycle from reset and pre-deployment to deployment through power projection platforms to the theater of operations.

2-2 Study Issues

(U//FOUO) Study Issue A: What C/EM capabilities are needed by a warfighter, by echelon, in order to accomplish assigned missions? Essential Elements of Analysis (EEA)

- EEA A.1: What is the most advantageous way to gain situational awareness of cyberspace and the EMS, while our adversary's awareness is degraded?
- EEA A.2: What is the most advantageous way to operate our networks and network sensors (all) while mitigating adversary attacks and the impacts of the environment (contested & congested)?
- EEA A.3: What is the most advantageous way to attack and exploit adversary individuals, facilities, platforms, sensors, systems, and networks?
- EEA A.4: What is the most advantageous way to protect individuals, facilities, platforms, sensors, systems, and networks?

(U//FOUO) Study Issue B: Which of the identified C/EM capabilities do warfighters by echelon lack?

- EEA B.1: What C/EM resolutions are presently fielded by echelon? What C/EM solutions are programmed?
- EEA B.2: Which of the C/EM tasks can the warfighter, by echelon, not perform to standard under the given conditions with currently fielded DOTLMPF solutions? These are gaps.
- EEA B.3: Using FM 5-19, what are the high risk C/EM shortfalls (i.e. gaps)?

(U//FOUO) Study Issue C: What C/EM DOTMLPF solution approaches may DOD implement in order to mitigate the gaps?

- EEA C.1: What C/EM non-material solution approaches mitigate the identified gaps?
- EEA C.2: What C/EM material solution approaches mitigate the identified gaps?
- EEA C.3: Using FM 5-19, what is the residual risk, given the application of the identified C/EM solution approaches?

- EEA C.4: What C/EM DOTLMPF solutions are currently available to units that can be redistributed or eliminated that do not increase the operational risk, as per FM 5-19?
- How should the Army command and control (C2) organize, by echelon, to effectively integrate C/EM operations?
- Where must the Army improve their investment of planners and liaisons in order to maintain situational awareness of national-level cyberspace operations and leverage national capability, when required, for the Army?

(U//FOUO) Constraints: A constraint is a restriction imposed by the study sponsor that limits the study team‘s options in conducting the study. The projected CBA completion date will be 180 days from the study plan approval date, but is dependent upon additional support requirements and subject matter expert availability. Funding will constrain the number of subject matter experts available for the study.

(U//FOUO) Limitations: A limitation is an inability of the study team to fully meet the study objectives or fully investigate the study issues. A certified modeling and simulation (M&S) tool capable of fully modeling cyberspace and electromagnetic spectrum effects does not exist. This will limit the analysis to subject matter experts (SME), professional military judgment (PMJ), and qualitative analysis (QA). It may be difficult to obtain critical SME support due to multiple or parallel CBAs in related and supporting areas. There is a limited historical knowledge foundation of cyberspace and electromagnetic spectrum operations.

(U//FOUO) Assumptions: An assumption is a statement related to the study that is taken as true in the absence of facts, often to accommodate a limitation. The following are assumptions of the C/EM CBA.

- (U//FOUO) The United States will have a declaratory cyber policy that communicates to potential adversaries the likely responsive action in the event of a cyber attack on US cyber networks and related components. This policy is apt to include greater specifications regarding law enforcement involvement and legal repercussions. Responsive action will likely incorporate the use of force, as necessary. (“Letter Report from the Committee on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy”, March 25, 2010)
- (U//FOUO) USSTRATCOM will be responsible for synchronizing planning for cyberspace operations, and will do so in coordination with other combatant commands, the Services, and as directed, appropriate U.S. government agencies. (Unified Command Plan 2008).
- (U//FOUO) The Army will increasingly be tasked to provide cyberspace capabilities and capacity to support homeland defense through NORTHCOM and cyber operations for USCYBERCOM.
- (U//FOUO) DoD will collaborate with other U.S. departments and agencies and international partners both to support their efforts and to ensure our ability to operate in cyberspace. This mutual assistance includes information sharing,

support for law enforcement, defense support to civil authorities, and homeland defense. In particular, DoD will strengthen its cooperation with DHS, which leads the national effort to protect federal information systems. (Quadrennial Defense Review Report, FEB2010)

- (U//FOUO) DoD will continue to lease certain space capabilities that enhance C2.
- (U//FOUO) Secretary of the Army will release memorandum aligning Army NetOps to the operational maneuver chain of command enabling theater commanders to make risk-based decisions synchronized with the Global NETOPS Commander's directed actions. (Army CIO/G6 NETOPS Update, COL John Shrader ,18 Mar 10)
- (U//FOUO) Operational and Tactical commanders in the Joint Battlespace who are delegated authority from COCOM Commanders, will be responsible for the operation and defense of the network. This will provide a single Joint NETOPS authority supporting the operational maneuver commander. This approach to NETOPS will improve unity of effort that focuses on transparent reporting and problem solving. (Army CIO/G6 NETOPS Update, COL John Shrader, 18 Mar 10)
- (U//FOUO) Uncertainty in the future operational environment will continue to increase as political, economic, informational, and cultural systems become more complex and interconnected. (TRADOC Pam 525-3-1 The United States Army Operating Concept 19 Aug 2010)
- (U//FOUO) Adversaries will be able to achieve tactical, operational, and strategic surprise based on rapid application of available and emerging technologies in both manned and unmanned systems. (TRADOC Pam 525-3-1 The United States Army Operating Concept 19 Aug 2010)
- (U//FOUO) U.S. forces will operate in environments where land, air, space, maritime and cyberspace superiority is increasingly contested by an ever widening set of state and nonstate actors with sophisticated capabilities. (TRADOC Pam 525-3-1 The United States Army Operating Concept 19 Aug 2010)
- (U//FOUO) U.S. forces will face increasing antiaccess and area denial challenges due to strategic preclusion, operational denial, and tactical overmatch. (TRADOC Pam 525-3-1 The United States Army Operating Concept 19 Aug 2010)
- (U//FOUO) U.S. forces will have limited ability to overcome antiaccess and area denial capabilities, deploy into austere locations, and sustain operations in immature theaters. (TRADOC Pam 525-3-1 The United States Army Operating Concept 19 Aug 2010)
- (U//FOUO) The Army will continue to employ the Army National Guard and Army Reserve on a routine basis as part of its operational forces. (TRADOC Pam 525-3-1 The United States Army Operating Concept 19 Aug 2010)
- (U//FOUO) The Army will continue to use a force management model that relies on unit replacement and cyclical readiness to govern the training, deployment, and reset of its operational forces. (TRADOC Pam 525-3-1 The United States Army Operating Concept 19 Aug 2010)

- (U//FOUO) Army modernization efforts will provide incremental, brigade-based capability improvements to the force. (TRADOC Pam 525-3-1 The Unided States Army Operating Concept 19 Aug 2010)
- (U//FOUO) The FA29 will be responsible for STO planning at the Bde/BCT.
- (U//FOUO) The FA29 will continue to be the EW expert battalion throught ASCC.
- (U//FOUO) No MOSs will be changed, but some will be adapted to include C/EM skills.

Section III Study Approach

3-1 Analytic Methodology

(U) This study was conducted using a collaborative and multidisciplinary approach within a JCIDs framework and took a joint perspective. “JCIDS provides a deliberative methodology to assess force concepts or concepts of the operations (CONOPS), identify gaps in required capabilities, and identify DOTMLPF solutions to mitigate gaps with unacceptable risk.”[1] In executing this methodology the study team ensured a defined and defensible JCIDS process by following the steps, principles, and tenets contained within the TRADOC CBA Guide.

Study Process

(U//FOUO) Following the JCIDS methodology, the C/EM Contest CBA was conducted in four Phases as depicted in Figure 5 below.

> (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.
>
> (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).
>
> (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

[1] TRADOC Regulation 71-20, *Concept Development, Experimentation, and Requirements Determination*. 6 May 2009. p.11

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.

(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.

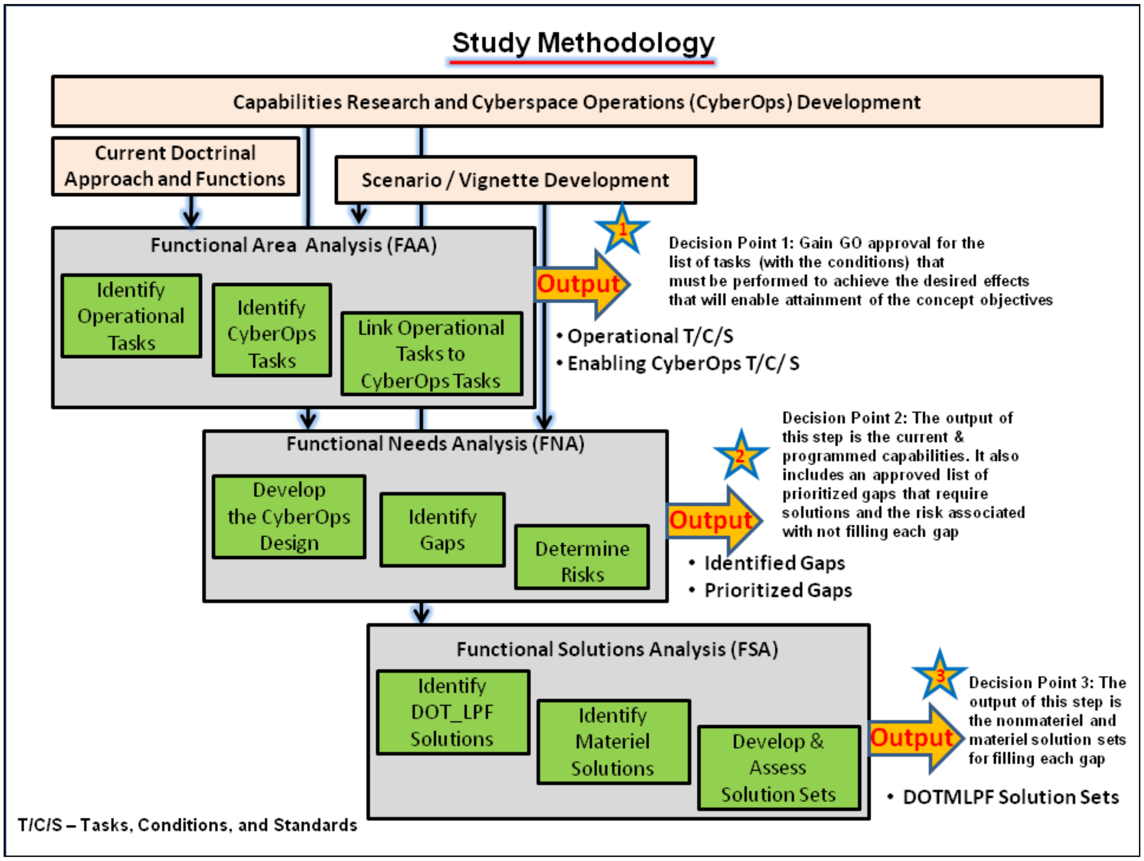
(U//FOUO) The FSA is normally composed of three sub steps, the DOTLMPF Analysis, the Ideas for Materiel Approaches (IMA); and the Analysis of Materiel Approaches (AMA). Because of the nature of this particular C/EM CBA, the analysis team focused on the first sub-step.

(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) 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.

(U) Specific methodology is articulated to greater detail in the Appendixes of the FAA, FNA and FSA.


Study Methodology
Capabilities Research and Cyberspace Operations (CyberOps) Development
Current Doctrinal Approach and Functions
Scenario / Vignette Development
Functional Area Analysis (FAA)
Identify Operational Tasks
Identify CyberOps Tasks
Link Operational Tasks to CyberOps Tasks
1
Output
Decision Point 1: Gain GO approval for the list of tasks (with the conditions) that must be performed to achieve the desired effects that will enable attainment of the concept objectives
• Operational T/C/S
• Enabling CyberOps T/C/S
Functional Needs Analysis (FNA)
Develop the CyberOps Design
Identify Gaps
Determine Risks
2
Output
Decision Point 2: The output of this step is the current & programmed capabilities. It also includes an approved list of prioritized gaps that require solutions and the risk associated with not filling each gap
• Identified Gaps
• Prioritized Gaps
Functional Solutions Analysis (FSA)
Identify DOT_LPF Solutions
Identify Materiel Solutions
Develop & Assess Solution Sets
3
Output
Decision Point 3: The output of this step is the nonmateriel and materiel solution sets for filling each gap
• DOTMLPF Solution Sets
T/C/S – Tasks, Conditions, and Standards

(U//FOUO) Figure 5: JCIDS Analytical Process
(TRADOC CBA Guide Version 3, dated 28 September 2009)

Section IV: Literature Review

4-1 Army Concept Framework

(U) The purpose of TRADOC Pam 525-3-0, *The Army Capstone Concept Operational Adaptability—Operating Under Conditions of Uncertainty and Complexity in an Era of Persistent Conflict* (ACC), is to describe the broad capabilities the Army will require in 2016-2028. It provides a guide to how the Army will apply available resources to overcome adaptive enemies and accomplish challenging missions and articulates how to think about future armed conflict within an uncertain and complex environment. It provides a foundation for a campaign of learning and analysis that will evaluate and refine the concept's major ideas and required capabilities. Ultimately, prioritized capabilities that emerge from this concept and subordinate, more detailed concepts will guide changes in doctrine, organization, training, materiel, leader development and programs related to the human dimension for our Army.

> *"Because Army forces are increasingly dependent on electro-magnetic, computer network and space-based capabilities and because those conduits of information are converging, exerting technical influence will require forces that are prepared to fight and win on an emerging "cyber-electromagnetic battleground."*

(U) TRADOC Pam 525-3-1, *The Army Operating Concept* (AOC) describes how Army forces conduct operations as part of the joint force to deter conflict, prevail in war, and succeed in a wide range of contingencies in the future operational environment. It expands on ideas presented in TRADOC Pam 525-3-0 (referred to as the ACC). The AOC describes the employment of forces to guide Army force development and identifies capabilities required for future success. The ideas introduced in the ACC and discussed further in the AOC are central to the way the future Army will fight and win and guide the integration of Army forces with a wide array of domestic and international partners.

> *"The cyber/electromagnetic contest involves gaining advantages in the cyberspace domain and electromagnetic spectrum, maintaining those advantages, and denying the same to enemies. In the cyber/electromagnetic contest, significant advantage will go to the side that is able to gain, protect, and exploit advantages in the highly contested cyberspace domain and electromagnetic spectrum. As Army forces increase demand for cyber capabilities to support precision guidance, navigation, and communications, they must learn to operate information systems at peak capacities and when degraded or disrupted."*

(U) TRADOC Pam 525-3-3*, The United States Army Functional Concept for Mission Command 2016-2028,* (MC AFC) expands on the ideas presented in TRADOC Pam 525-3-0, the ACC, and TRADOC Pam 525-3-1, the AOC, and introduces mission command as a warfighting function. Confronted by decentralized, networked, and adaptive enemies in complex environments, the Army must redefine its approach to the exercise of authority and direction over its forces. The application of mission command enables commanders to decentralize authority and prevail in three increasingly important dimensions of military operations: the contest of wills, strategic engagement, and the cyber/electromagnetic contest.

> *"The aim of the third dimension—cyber/electromagnetic contest—is to gain advantage, maintain that advantage, and place adversaries at a disadvantage in the increasingly contested and congested cyberspace domain and the electromagnetic spectrum (EMS). Staffs conduct cyber/electromagnetic activities. Cyber/electromagnetic activities focus on seizing, retaining, and exploiting advantages in cyberspace and the electromagnetic spectrum. These activities include cyberspace operations, electronic warfare, and electromagnetic spectrum operations."*

4-2 Other Army Works

(U//FOUO) The study team began with a significant body of work, reaching back over the last ten years of operations, explored current and future operational environments that included the cyber/electromagnetic contest and full spectrum operations. This provided a solid foundation of knowledge relevant to the study. During the CAC Hosted Cyberspace Symposium, 27-30 October 2009, one of the working groups was dedicated to conducting a literature review to support analysis. This working group captured potential tasks and then refined these into the initial task list. Documents used for analysis included previous analytic studies, approved task lists, network references, related efforts, lessons learned and various briefs. Some examples reviewed were BPP 03-EC-0-0001, Acquiring Secret Internet Protocol Router Network (SIPRNET); Homeland Defense and Civil Support CBA (JCD); Operational Environment Assessment: Afghanistan; TPO NETOPS/CDID, "NETOPS Conference Issues Update (U)",30 Sept 2009, Fort Gordon GA, 30 Sep 09, PowerPoint Brief.

(U//FOUO) Other key documents referenced were joint and Army concepts and doctrine such as TRADOC Pamphlet 525-7-8 Cyberspace Operations Concept Capability Plan 2016-2028, the Army Network Modernization Strategy Framework (version 1.0 XX June 2010), Army Network Architecture Strategy – Tactical v1, Army Enterprise Network Execution Framework – LandWarNet, LandWarNet ICD, Mission Command Essential Capabilities White Paper, Network Enabled Mission Command ICD, Army Training Concept Draft, Field Manual 3-0 Operations, and Field Manual 3-36 Electronic Warfare Operations. Additional documents are referenced in Appendix A.

Section V: Understanding the C/EM Contest and Implications

5-1 Impacts to the Army

(U) To understand the capabilities adversaries can now command, below is a synopsis of some major C/EM events that demonstrate the willingness of threat actors to use cyber effects as a means to achieve political or military objectives:

- (U) May 2007: Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, most likely at the behest of the Russian government. Some government online services were temporarily disrupted and online banking was halted.
- (U) September 2007: Israeli forces conducted an aerial attack on a Syrian nuclear facility. Prior to the attack, the Syrian radar and anti-missile batteries were paralyzed by a suspected computer virus which allowed Israeli planes to pass undetected by radar into Syria and attack the nuclear plant unimpeded. This is one of the first large scale effects caused by the convergence of cyberspace and the EMS, blinding an integrated air defense/electronic warfare capability through a computer network system.
- (U) August 2008: Russian troops crossed into South Ossetia vowing to defend what they called "Russian compatriots". As this was taking place, a multi-faceted cyber attack began against the Georgian infrastructure and key government web sites. The attack modalities included: Defacing of Web Sites (Hacktivism), Web-based Psychological Operations (Psyc-Ops), a fierce propaganda campaign (PC) and of course a Distributed Denial of Service Attack (DDoS).
- (U) January 2009: Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip which briefly paralyzed government sites. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah. Historically, every time the conflict between Israel and the Palestinians flares up, Israeli web sites suffer a barrage of virtual assaults. During the fighting in Gaza, however, the attack was unusually severe and complex.

(U) In response to the growing threat from new and advanced adversary capabilities, the DoD and Army in particular have taken steps to prepare for countering these threats.

- (U) 23 June, 2009: The Secretary of Defense (SecDef) signed a memorandum establishing USCYBERCOM as a subordinate unified command under USSTRATCOM, with responsibility for military cyberspace operations. This directive was the culmination of multiple efforts to define the optimal Department of Defense (DoD) response to the significant cyber challenges confronting the nation.
- (U//FOUO) 20 October 2009: US Central Command (USCENTCOM) established a CENTCOM Cyberspace Warfare Cell (CWC) to counter

adversaries' use of cyberspace and to counter their use of the CENTCOM Theater Information Grid (TIG). The mission of this cell is to provide a proactive, operational capability which synchronizes exploitation, attack and defense to regain control of their networks and take action against enemy networks. The CWC is responsible for integrating all aspects of cyberspace support to USCENTCOM Commander, staff and components. They conduct direct liaison with various elements to include Intelligence, Communications and Operations Communities.

- (U) 1 February, 2010: Army G-3/5/7 directed the establishment of ARCYBER as the Army Service Component Command (ASCC) to plan, coordinate, integrate, synchronize, direct, and conduct network operations and defense of all Army Networks. It is also charged, when directed, to conduct cyberspace operations in support of full spectrum operations to ensure US/Allied freedom of action in cyberspace and to deny the same to our adversaries.

(U//FOUO) All of these DoD organizations have been developed and stood up to grow capacity and capability to counter our adversaries in cyberspace. As recognized in JP 3-0, Cyber and the EMS are increasingly inter-related or "meshed‟ with each other, with many parallels in the use of capabilities. Cyber is reliant on the EMS, as networks and telecommunication infrastructures increasingly make use of wireless means. Smart devices (e.g. iPhone, PDAs) are simultaneously computers, cell phones, cameras, and wireless devices. Our sensors (also part of the network) require the EMS in order to collect information and then to disseminate it. For this reason, cyber operations must include the employment of capabilities that manage and ensure our access to those portions of the EMS needed for the functioning of the network and related sensors.

(U//FOUO) The Bottom Line: The Army conducts cyberspace operations, Electronic Warfare and Electromagnetic Spectrum Operations to support the combatant commanders and conduct Army operations in support of commanders' objectives. The most prolific issue facing the Army today is the inability for Army forces to holistically include C/EM activities, as an integrated part of full spectrum operations (the commanders' decision making process), and the ability to leverage all available resources and capabilities. In addition, Commanders must have the understanding, capability, capacity and authorities to integrate, plan and employ C/EM capabilities in a combined arms fashion to conduct full spectrum operations. This is no longer a "nice to have" but is now a documented requirement if we are to ensure we can gain and maintain an advantage in the cyber domain and EMS while countering our adversaries' capabilities.

5-2 The Cyber/Electromagnetic Contest

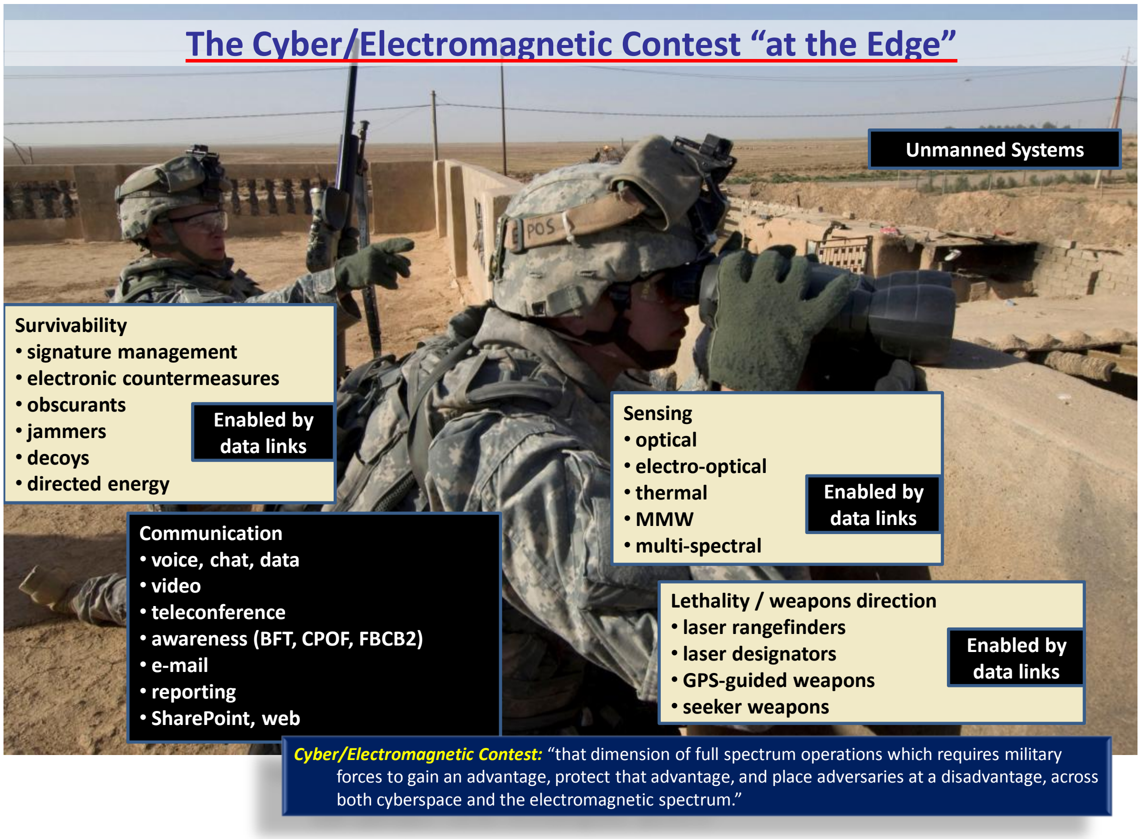
(U//FOUO) *"The conflict started with massive cyber attacks on government web sites and commercial operations. Distributed attacks using botnets, denial-of-service attacks, logic bombs and other cyber weapons overwhelmed many of the targeted sites and servers, fully disrupting the economy and the government. The government was unable* *to communicate with the rest of the world – radio and television stations could not function. Previously reliable Internet service providers were 'bought out' and refused to provide service. The banking system effectively collapsed for several days. Friendly websites were hijacked to distribute enemy propaganda. Soon enemy airstrikes and ground attacks began. Commercial and military communications systems were disrupted by continuous cyber attacks and electronic jamming. Remaining communications systems were clearly being exploited by the aggressor – particularly phone conversations between civilian and military leaders. Friendly military forces found themselves isolated and unable to communicate. Attempts to communicate using radios resulted in very precise artillery and air attacks by the enemy. False orders and reports came across cell phones, increasing the confusion.*[2]

(U//FOUO) The above vignette, drawn from Georgia-Russia 2008 South Ossetia war illustrates a "new normal" for commanders: combined arms warfare now includes seeking advantage in cyberspace and the electromagnetic spectrum. Information and communication technology has created an environment of pervasive inter-relationship and convergence between the cyberspace domain and the electromagnetic spectrum (EMS). Effectively, this creates a new "maneuver space" for operations. Commanders must now think and act holistically regarding an increasingly important dimension of full spectrum operations: the "cyber/electromagnetic contest".

(U//FOUO) The C/EM Contest is a holistic, combined arms approach that recognizes a cyber/electromagnetic dimension to operations. It is defined as "That 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". The C/EM Contest offers five key ideas:

1. (U//FOUO) Cyberspace and the EMS are 'commander's business' and activities in these mediums must be fully integrated within the overall operation.
2. (U//FOUO) Today's environment requires an expanded notion of combined arms operations. Commanders must think broadly and employ the full range of their capabilities to win the contest.
3. (U//FOUO) The Cyberspace domain and the EMS must be thought of as maneuver space where positional advantage can be gained or lost.
4. (U//FOUO) Cyberspace operations and EMS operations have converged in technology and must converge operationally; many times drawing on the same capabilities to meet objectives in either.
5. (U//FOUO) Winning the contest (maintaining our freedom of action in the cyberspace domain and the EMS while denying our adversaries the same) greatly facilitates our efforts; and if not, our operations can be severely degraded.

[2] This vignette is largely drawn from events described in "Lessons from the Russia-Georgia Cyberwar" by Kenneth Corbin, www.internetnews.com, March 12, 2009.



The Cyber/Electromagnetic Contest "at the Edge"

Unmanned Systems

Survivability
- signature management
- electronic countermeasures
- obscurants
- jammers
- decoys
- directed energy

Enabled by data links

Sensing
- optical
- electro-optical
- thermal
- MMW
- multi-spectral

Enabled by data links

Communication
- voice, chat, data
- video
- teleconference
- awareness (BFT, CPOF, FBCB2)
- e-mail
- reporting
- SharePoint, web

Lethality / weapons direction
- laser rangefinders
- laser designators
- GPS-guided weapons
- seeker weapons

Enabled by data links

Cyber/Electromagnetic Contest: "that dimension of full spectrum operations which requires military forces to gain an advantage, protect that advantage, and place adversaries at a disadvantage, across both cyberspace and the electromagnetic spectrum."

(U) Figure 6: The C/EM Contest at the Lowest Tactical Level

(U//FOUO) At the small unit level, the C/EM Contest is not an ethereal struggle, but a very necessary element of shoot, move, and communicate. The ability to communicate, see the battlefield and have situational awareness depends on access to cyber and the EMS for data links and sensors. Counter-IED devices proliferate on the battlefield here and are a great example of adversary cyber/EMS denial capabilities that supports soldier and vehicle survivability. The significance of C/EM activities is magnified as we provide small units increased data, networking capability, protective systems, and robotics. In a very inter-related fashion, the cyberspace domain and the EMS enable communication, lethality, and survivability.

(U//FOUO) At echelons above the small unit level, the focus of C/EM activities shifts from attack and protection of individual entities and platforms, more to the operation and defense of the network. The network essentially functions as a central nervous system (back bone) connecting the sensory organs to the brain. It connects our forces and allows the commander to command those forces. However, as we connect the network, this also connects us to other friendly, neutral, and adversarial audiences and actors. Therefore, the network is a key portion of our ability to engage in the contest of wills with adversaries and conduct strategic engagement with friends and neutrals.

Ends: Success in Cyber/Electromagnetic Contest

(U//FOUO) The commander's mission objectives define overall success. This is achieved by the integration of operations to gain and protect advantage while placing adversaries at a disadvantage. Given adaptive and innovative adversaries, such advantages and disadvantages are likely to be localized and transient - our ability to recognize change and adapt will be crucial. We 'win' the C/EM Contest if our operations are fully enabled, and adversary operations are hindered at the desired points in time and space. Our adversaries will continually adapt and react, so relative advantages must be created and sustained over time. Commanders will need to continually ensure they are meeting four criteria:

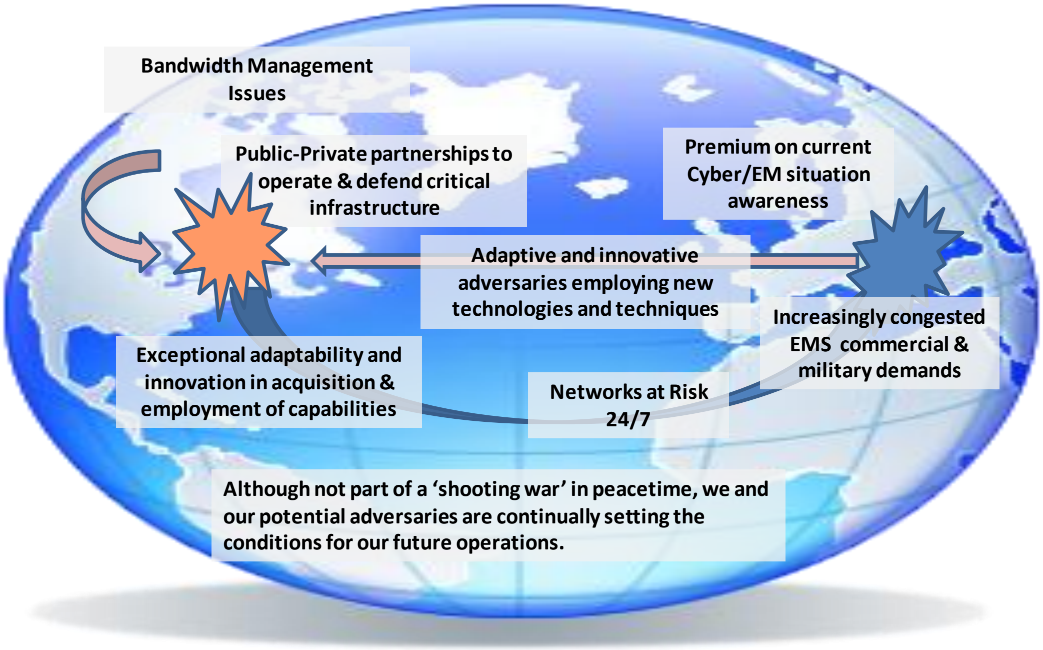
- We have situational awareness of cyberspace and the EMS, while our adversary's awareness is degraded.
- We operate our networks (mitigating adversary attacks and environmental impacts), while attacking and exploiting adversary networks.
- We can attack/exploit adversary individuals, facilities, platforms, and systems.
- We can protect individuals, facilities, platforms, and systems.

Ways: A Cyber/Electromagnetic Contest Operational View

(U//FOUO) The C/EM Contest is an ongoing commercial-military phenomenon, establishing conditions for both current and potential future operations. Networks are at risk 24 hours a day, 7 days a week as nation-states and other adversaries attempt to penetrate friendly networks. The EMS is congested with multiple users. Government and military agencies operate and defend the network, related infrastructures, and maintain access to critical portions of the EMS. Public-private partnerships are often required. The predominant challenge in maintaining awareness and preparedness is keeping pace with new technologies (usually new commercial technologies) and potential adversary's use of these new capabilities. This requires exceptional adaptability and innovation.[3]

[3] TRADOC Pamphlet 525-7-8, Cyberspace Operations Concept Capability Plan 2016-2028, Appendix C

Cyber/Electromagnetic Contest: Always in Progress

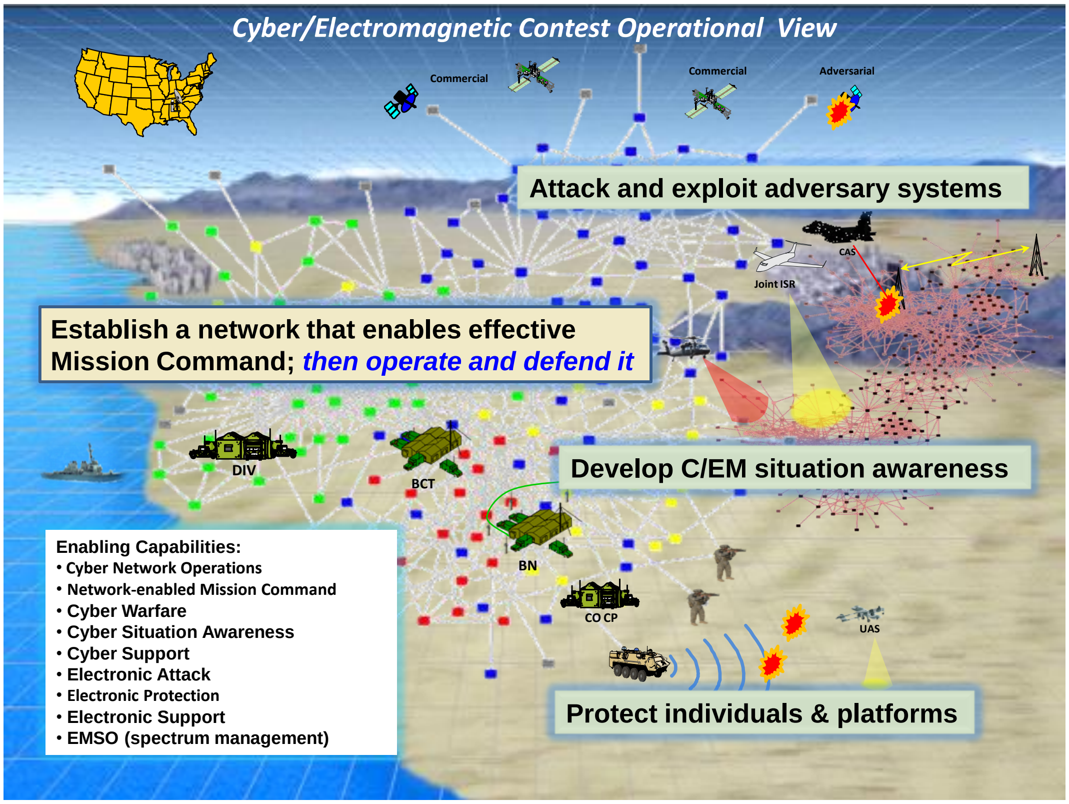

Bandwidth Management Issues
Public-Private partnerships to operate & defend critical infrastructure
Premium on current Cyber/EM situation awareness
Adaptive and innovative adversaries employing new technologies and techniques
Increasingly congested EMS commercial & military demands
Exceptional adaptability and innovation in acquisition & employment of capabilities
Networks at Risk 24/7
Although not part of a 'shooting war' in peacetime, we and our potential adversaries are continually setting the conditions for our future operations.

(U) Figure 7: A Constant Contest

(U//FOUO) As overt military operations begin, commanders establish objectives that they wish to achieve (e.g. air superiority, control of key terrain, access to sea lanes), including C/EM strategic, operational, and tactical objectives. Attaining success depends on developing the right mix of actions in time and space. C/EM activities integrate and synchronize use of all capabilities, as part of combined arms operations, across all domains.

(U//FOUO) The fundamental objective of the C/EM contest is to establish a network that enables effective Mission Command; then operate and defend it. In conjunction with this primary effort, commanders seek to develop C/EM situational awareness, which enables all aspects of the C/EM Contest. Operations are directed to attack and exploit adversary systems, and to protect friendly individuals and platforms. Support activities underpin these efforts to gain and maintain advantages.

(U//FOUO) Both cyber and the EMS are 'commons' – used by the general population as well as being echelon- and geography- independent. We are always competing to use the spectrum, if only because of the congestion caused by the many users. For that reason, C/EM activities reflect a unique mindset of key terrain: servers, addresses, websites, towers, satellites, spectrum wavelengths, etc. The terrain analogy has one caveat - in cyberspace 'new' key terrain can be created on short notice – which generates a very dynamic environment. Therefore, C/EM activities protect existing infrastructures, improve upon them, and engage in activities that degrade adversary use. The result is a framework where friendly forces are postured to succeed; adversaries are postured to fail.



Cyber/Electromagnetic Contest Operational View

Attack and exploit adversary systems

Establish a network that enables effective Mission Command; *then operate and defend it*

Develop C/EM situation awareness

Protect individuals & platforms

Enabling Capabilities:
- Cyber Network Operations
- Network-enabled Mission Command
- Cyber Warfare
- Cyber Situation Awareness
- Cyber Support
- Electronic Attack
- Electronic Protection
- Electronic Support
- EMSO (spectrum management)

(U) Figure 8: C/EM Contest Operational View

Means: Capabilities

(U//FOUO) Commanders will leverage all possible capabilities to gain and maintain desired advantages (i.e. meet the success criteria identified above). By defining desired conditions in cyberspace and the EMS, commanders and their staffs determine the right mix of cyber, electronic, and other capabilities to achieve advantage. For example, situational awareness is created by blending intelligence, network analysis, spectrum management, support activities, and physical actions (e.g. aerial and ground reconnaissance).

Implications

(U//FOUO) The notion of a C/EM Contest suggests development of a strategic vision that will make the Army successful as a fighting force in cyber and the EMS. We need to explore the inter-relationships and convergence to determine the right mix of capabilities. The Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM Contest CBA) is intended to explore this future to develop appropriate capabilities for commanders and soldiers. Some specific areas of investigation are:

- Our approach to operations conducted across largely commercial infrastructures must be defined.

- National policies must define the appropriate restrictions on the role of the military regarding C/EM activities. Legislation may be needed to ensure sufficient flexibility exists for C/EM activities.
- The C/EM Contest has implications for the assignment, education and training of operational and GENFOR personnel. Well integrated training paths are necessary.
- Commanders (and staffs) of all varieties must be developed who understand the challenge and opportunities of C/EM activities.
- Collective training must include C/EM activities.
- The C/EM Contest is a "Total Force" matter, fully involving the generating force, the operational force, active component, reserve component, and government civilian personnel.
- Materiel acquisition processes must be modified to gain agility.
- Capabilities, doctrine, facilities, and organizations are needed that provide the necessary wherewithal to commanders to pursue the C/EM contest. For example, headquarters must be structured for proper integration.

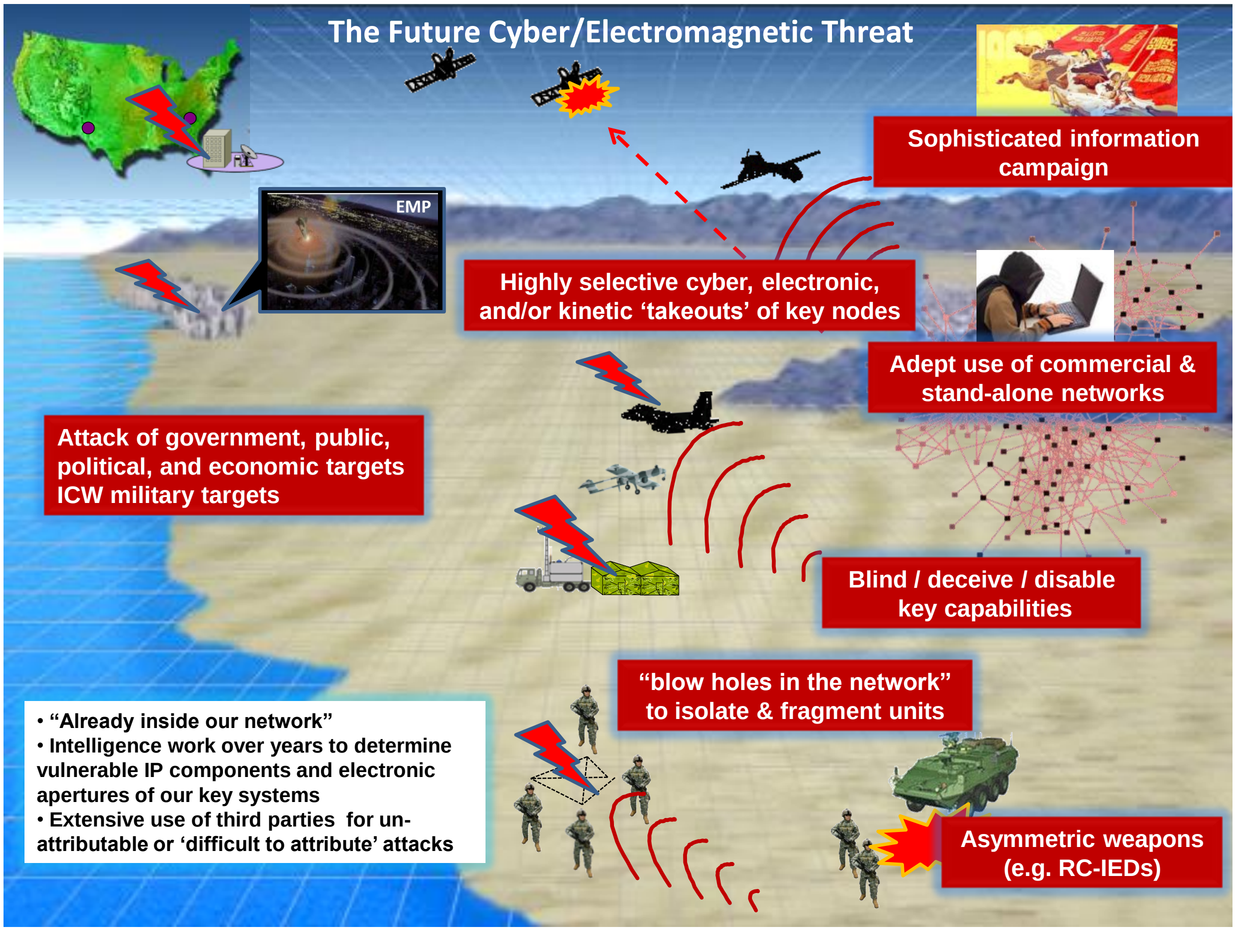
Summary

(U//FOUO) The "Cyber/Electromagnetic Contest" recognizes that combined arms operations now span cyberspace and the EMS; and that cyberspace and the EMS can be thought of as 'maneuver space'; i.e. areas where 'positional advantage' is possible. This perspective emphasizes the importance of warfighting across all domains using the full range of capabilities. Given the inter-relationships and convergence between cyberspace and the EMS wrought by technological advances, holistic consideration of C/EM activities is appropriate. Winning the C/EM Contest greatly facilitates our efforts; if not then our operations can be severely degraded. Commanders and their staffs must think broadly, in a combined arms perspective, and employ the full range of capabilities to 'win the contest'.

5-3 Defining the Threat

(U//FOUO) TRADOC's Operational Environment assessment recognizes rapid technological change. Consider the rapid progression of commercial cellular communications (with ever increasing data rates as 3G and 4G technologies are adapted). The rapid pace of commercial technology development means potential adversaries, terrorists and criminal organizations are using commercial off-the shelf (COTS) devices as soon as they become available. The Operational Environment assessment foresees:

(U//FOUO) *"The threat will be 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 – including the possibility of WMD/WME. They will operate conventionally and unconventionally employing adaptive and asymmetric combinations of traditional, irregular and criminal tactics using* *traditional military capabilities in old and new ways. Threats will challenge US access – directly and indirectly. They will attack US national and political will with very sophisticated information campaigns as well as seek to conduct physical attacks on the US homeland. Military operations will result in operations demanding long term commitments at extended distances and requiring a wide range of inter-agency and non-military tools to resolve. All of which will be carried out under the unblinking eye of an omni-present formal and informal media potentially giving local events global significance."* [4]


The Future Cyber/Electromagnetic Threat
EMP
Sophisticated information campaign
Highly selective cyber, electronic, and/or kinetic 'takeouts' of key nodes
Adept use of commercial & stand-alone networks
Attack of government, public, political, and economic targets ICW military targets
Blind / deceive / disable key capabilities
"blow holes in the network" to isolate & fragment units
Asymmetric weapons (e.g. RC-IEDs)

- "Already inside our network"
- Intelligence work over years to determine vulnerable IP components and electronic apertures of our key systems
- Extensive use of third parties for un-attributable or 'difficult to attribute' attacks

(U) Figure 9: Future C/EM Threat

(U//FOUO) These threats are prepared to maneuver against us in cyberspace and the EMS, in combination with both conventional and asymmetric means.

(U//FOUO) As noted in Figure 10, the C/EM contest is always underway and our adversaries continuously work to identify vulnerabilities and develop tools as weapons for use through cyberspace and/or the EMS. Our adversaries and enemies are able to

[4] 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 Environment 2009-2025, August 2009, pages 8-9.

infiltrate our networks and are already inside. They are adept at using commercial and stand alone networks and use those networks to attack government, public, political, and economic targets in conjunction with military targets. Adversaries have been collecting intelligence on the U.S. to determine vulnerable IP components and electronic apertures of our key systems and highly selective cyber, electronic, and/or kinetic takeouts of key nodes. They also make extensive use of third parties for un-attributable or 'difficult to attribute' attacks. The threat is not only a concern for the future but is immediate with use of asymmetric weapons such as RC-IEDs. Adversaries will continue to develop and refine their capabilities and the threat to U.S. forces will increase.

(U//FOUO) Human society is also making ever increasing use of cyber and the electromagnetic spectrum for communication and daily 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 is a powerful vehicle for Inform and Influence Activities to shape attitudes and perceptions, either for influence or deception. Clearly our current and potential adversaries are using cyber and the EMS for political and military advantage.

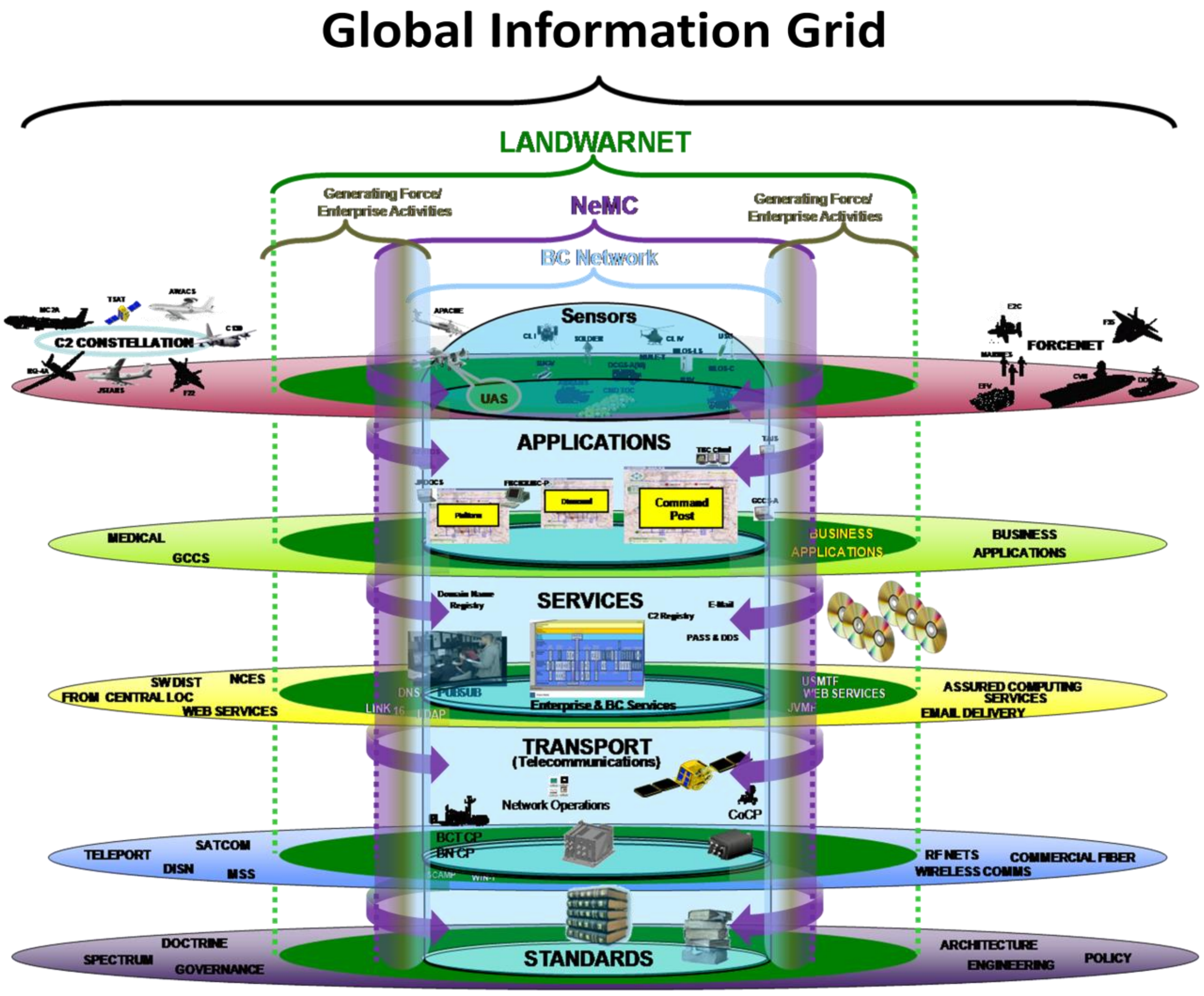
5-4 Understanding the "Network"

(U//FOUO) LandWarNet (LWN) is the Army's portion of the Global Information Grid, the Department of Defense construct for the total collection of protected and unprotected networks used by the Services and the headquarters. LWN constitutes all the Army owned or leased network infrastructure and consists of five layers: platforms and sensors, applications, services, transport infrastructure, and standards.

(U//FOUO) LWN is not a single network. Until recently, LWN consisted of separate, multiple, stove-piped systems and processes which prevented network-enabled, commander-centric operations (Network enabled Mission Command)[5]. As Army networking has grown over the years, units and functional staffs have built networks using a variety of commercial and military standards. The network consisted of the Army collection of networks supporting Army Title 10 and other assigned responsibilities, a theater network architecture for deployed Army units, and the planned Future Combat Systems (FCS) network. Today's network nests these requirements under a single concept called the Global Network Enterprise Construct (GNEC) as a strategy that will collapse these three network environments into a single network construct[6].

[5] TRADOC PAM 525-5-600, LandWarNet 2015 (11 February 2008) Pages 10.

[6] Army Network Modernization Strategy Framework DRAFT Version 1.0 XX June 2010.

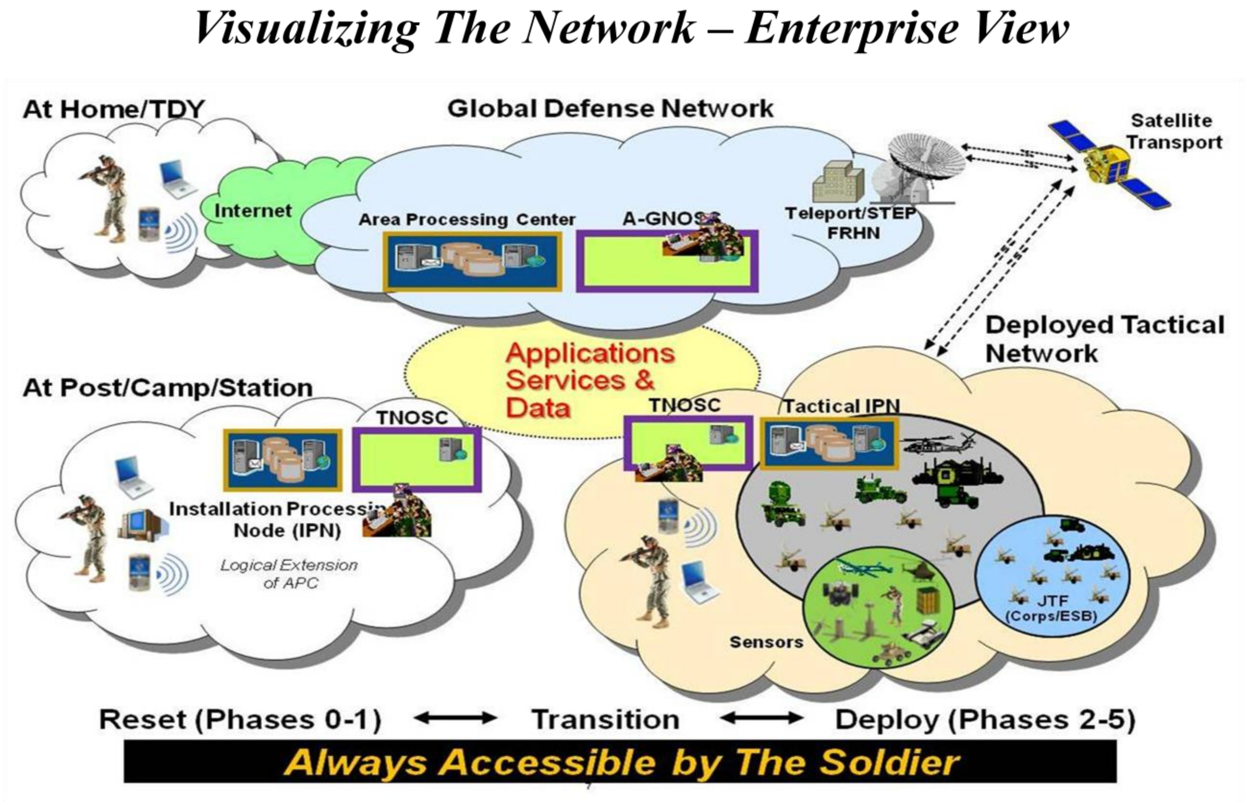


(U) Figure 10: Global Information Grid

(U//FOUO) GNEC is a part of the Army Network Modernization Strategy whose vision states: "*The Army enterprise network is a single, secure, standards-based, versatile infrastructure linked by networked, redundant transport systems, warfighting and business applications, and data to provide our Soldiers and Civilians the information they need, when they need it, no matter where they are, to enable full spectrum operations with our Joint, Coalition, and Interagency partners.*"[7] In the near future, the Army will operate a single global network that is present everywhere Soldiers serve (CONUS/OCONUS). It will be structured to support both Operating and Generating Force requirements and Soldiers in all roles and locations. The Army will provide an end-to-end network that brings all Soldiers appropriate network capability, having built out the required network infrastructure, providing Soldiers with deployment theater network environments through all of the Joint Operational Phases, and providing

[7] Army Network Modernization Strategy Framework DRAFT Version 1.0 XX June 2010.

incremental modernization to the Army as resources permit and in accordance with the over-arching Army Modernization Strategy and implementation Framework.



(U) Figure 11: Visualizing The Network – Enterprise View

(U//FOUO) The resultant LWN will be a secure, Soldier-driven network, supporting Soldiers in all their roles, in all their locations, all the time, on the move (OTM), while keeping up with technology through processes that identify and resource incremental modernization.

Section VI Functional Area Analysis Results

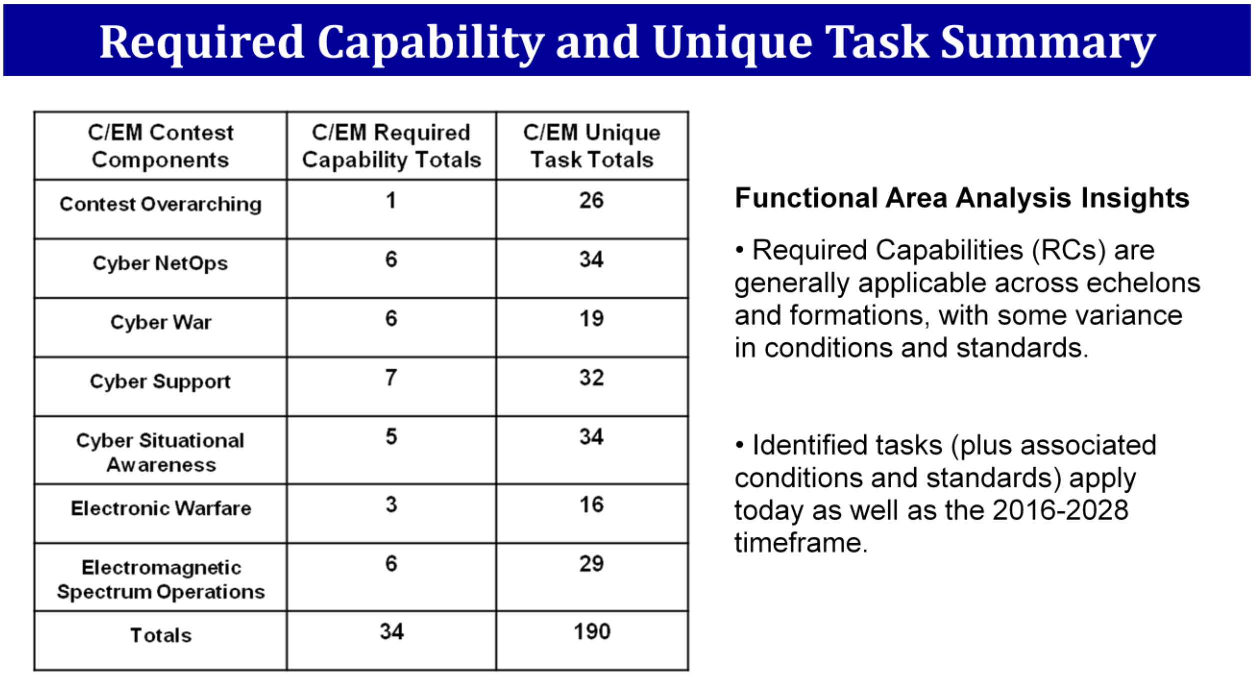
6-1 FAA Results

Associating Capabilities by Echelon

(U//FOUO) The end result of the FAA was the identification of Required Capabilities (RCs), tasks, conditions and standards. The C/EM CBA has identified specific required capabilities that must reside either organically or by having access to the capability.

Required Capabilities and Unique Tasks

(U//FOUO) (U//FOUO) Table 2 indicates the total C/EM Required Capabilities and unique tasks. The identified tasks, conditions and standards were compiled into an integrated list and identified by a standard Task Reference Number.



Required Capability and Unique Task Summary

C/EM Contest Components	C/EM Required Capability Totals	C/EM Unique Task Totals
Contest Overarching	1	26
Cyber NetOps	6	34
Cyber War	6	19
Cyber Support	7	32
Cyber Situational Awareness	5	34
Electronic Warfare	3	16
Electromagnetic Spectrum Operations	6	29
Totals	34	190

Functional Area Analysis Insights

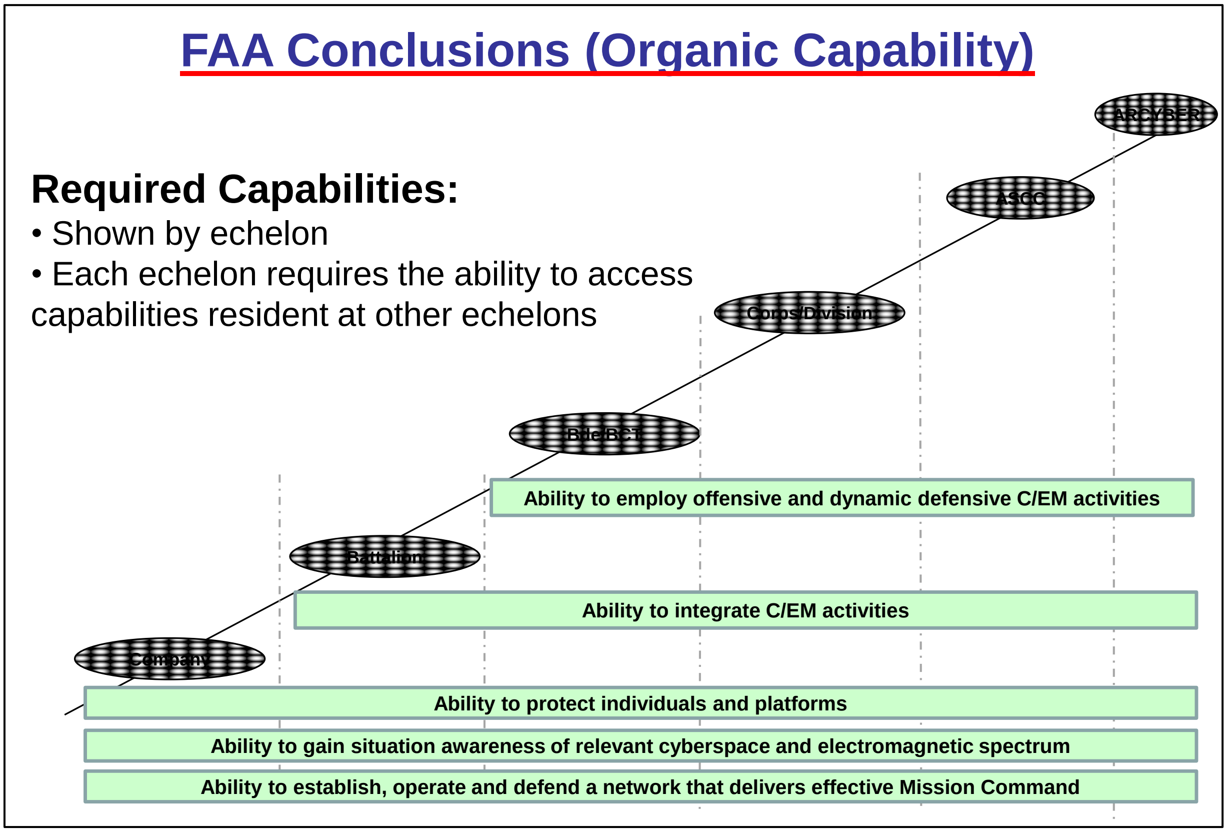
- Required Capabilities (RCs) are generally applicable across echelons and formations, with some variance in conditions and standards.
- Identified tasks (plus associated conditions and standards) apply today as well as the 2016-2028 timeframe.

(U//FOUO) Table 1: Functional Area Analysis RC / Task Summary

Organic Capabilities

(U//FOUO) While the FAA conducted thorough analysis across all Army formation and echelons, it focused on those units that most clearly needed C/EM performed as part of their mission set. In general terms, organic capability is needed when units require immediate and highly responsive and complex C/EM capabilities to perform their mission. Based on subject matter expert input, workshops, other studies’ conclusions, and the full range of scenarios and vignettes, capabilities were placed into two categories: “organic” versus “access to”. Organic capability is defined as that capability which must reside with an echelon, included on their associated table of organization and equipment. Access is defined by the ability of an echelon to request and employ additional support that is not resident in the organization on a permanent basis. Specific organic required capabilities include:

- (U//FOUO) All echelons require the ability to have C/EM situation awareness and to integrate C/EM activities as part of their overall mission.
- (U//FOUO) All echelons require the ability to leverage the overall network enterprise and require Mission Command essential capabilities.
- (U//FOUO) BCT/Brigade and above echelons require the ability to employ offensive C/EM capabilities and dynamic defense capabilities within their area of operations. This includes air and ground, organic and supporting capabilities.
- (U//FOUO) All echelons require capability to protect individuals and platforms.
- (U//FOUO) Select functional and multifunctional brigades require capabilities that provide access to adversaries' networks for exploitation and attack purposes. These brigades will support corps and divisions with this capability.
- (U//FOUO) BCT/Brigade requires capability to collect and exploit adversary capabilities and responsively support the operation.



FAA Conclusions (Organic Capability)

Required Capabilities:

- Shown by echelon
- Each echelon requires the ability to access capabilities resident at other echelons

Ability to employ offensive and dynamic defensive C/EM activities

Ability to integrate C/EM activities

Ability to protect individuals and platforms

Ability to gain situation awareness of relevant cyberspace and electromagnetic spectrum

Ability to establish, operate and defend a network that delivers effective Mission Command

(U//FOUO) Figure 12: FAA Conclusions

6-2 FAA Conclusions

(U//FOUO) The C/EM CBA study team and C/EM study community, after reviewing the resulting required capabilities and tasks, produced the following FAA conclusions:

- Required capabilities are generally applicable across echelons and formations, with some variance in conditions and standards.
- Identified tasks, conditions and standards apply today as well as for the 2016-2028 timeframe.
- Every echelon must engage in Cyber/Electromagnetic operations to some degree. In particular, C/EM integration, Cyber Network Operations, Cyber Situational awareness, Electronic Warfare, and Electromagnetic Spectrum Operations apply to all echelons.
- Both Cyberspace and the Electromagnetic Spectrum have ‘echelon-independent’ characteristics. Therefore, provision must be made for capabilities resident at one echelon to be available and responsive to needs at other echelons.
- Although enterprise approaches to cyberspace and electronic warfare are most efficient, sophisticated enemies will seek to fragment and isolate our formations and their supporting networks. Provisions must be made for units to be able to operate under degraded conditions, and in isolation.
- Many Electronic Warfare tasks are predominantly resident at the tactical and operational levels. Some Cyber tasks are predominantly resident at the strategic and operational levels.
- All echelons (units) require the ability to integrate C/EM capabilities within their planning and execution of combined arms operations.
- These tasks, in combination with each other, allow units to:
    - Have situational awareness of cyberspace and the electromagnetic spectrum while degrading adversary situational awareness
    - Operate and defend friendly networks while attacking and exploiting adversary networks.
    - Attack and exploit adversary individuals, facilities, platforms, and systems.
    - Protect friendly individuals, facilities, platforms, and systems.
- In many instances, the tasks for Cyber Network Operations and Network-enabled Mission Command are indistinguishable between each other.
- Electromagnetic Spectrum Operations are essential for successful Cyberspace Operations and Electronic Warfare.
- New and innovative acquisition processes are necessary. Current acquisition processes, and management of those processes, do not ensure a commander’s ability to win the C/EM contest.

Section VII Functional Needs Analysis Results

7-1 FNA Results

(U//FOUO) The FNA identified a total of 65 potential capability gaps for all echelons linked to tasks. Each gap was assigned an identification number for analytical and tracking purposes. As the study progressed and each potential gap was assessed against tasks, conditions, standards and current capabilities, the initial list of 65 gaps were combined and/or aggregated to a final total of 27 capability gaps for all echelons with their associated tasks. The gap number did not change during this analytical process and resulted in a list with the first gap number 02 and the last gap number 61. Table 3 shows the summary of the final 27 gaps by gap number and short title. Required Capability, Task, Programs of Record and Gap list is presented in Annex D.

Short Title	Number
C/EM Integrating Entity	02
Access	04
Legal Advisement for C/EM	06
Establish, Operate, Manage Enterprise Network/ Network enabled Mission Command	11
Transition Network C2	15
Single System and User ID	17
Integrate CyNetOps with Mission Partners	19
Network Defense in Depth	20
Access Critical Network Info, Services, & Applications	24
Cyber War Network Support	26
Dynamic Cyber Defense	28
Organic BDE Collect & Exploit Intelligence	29
Cyber Attack	32
Threat Hardware & Software Analysis	33
Cyber Vulnerability Assess & Operational Testing	36
EA Asset Deconfliction	37
Cyber Threat Investigation Sharing	38
C/EM Situational Awareness, COP	40
Conduct Electronic Attack	45
C/EM Modeling and Simulation	46
Detect Jamming	50
Dynamic Spectrum Management	51
Spectrum Impact Analysis	52
EMS Use Plan Export	53
Spectrum Use Prioritization	54
Defend/Protect Individuals and Platforms	57
Research, Development, Testing and Evaluation and Research, Development, and Acquisition	61

(U//FOUO) Table 2: Identified Gaps

7-2 FNA Conclusions

(U//FOUO) The C/EM study team referenced FM 5-19 Composite Risk Management to determine the impact of these gaps on the force. Gaps were prioritized by carefully selected C/EM subject matter experts, from across the Army. Gaps were assessed by probability and severity, in accordance with the methodology from FM 5-19. SME votes were based on individual expertise/perspective. SMEs were asked to vote separately on the probability and severity four times.

1. Overall impact of the gap on the total Army
2. Impact of the gap to the ASCC/ARCYBER
3. Impact of the gap to the Division/Corps
4. Impact of the gap to the BCT/BDE and below

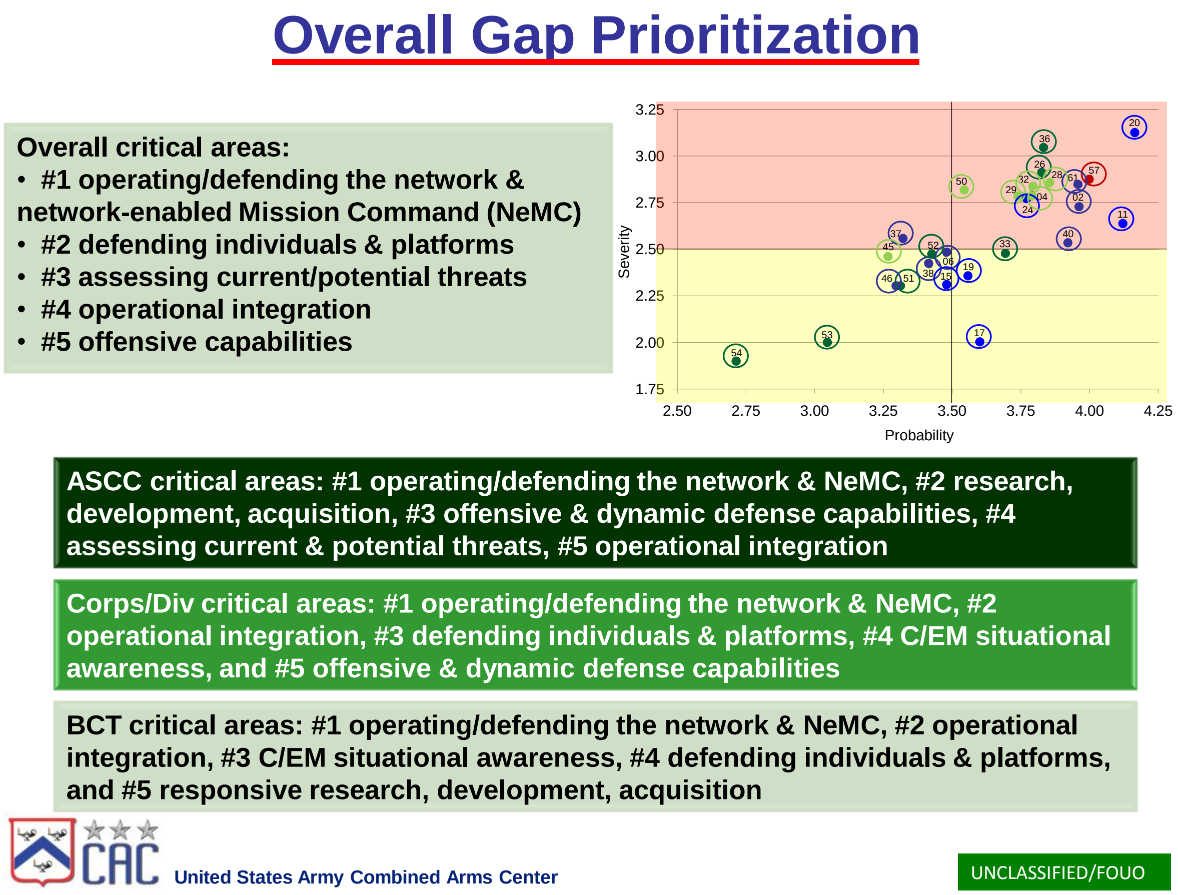
(U//FOUO) Overall and with each echelon, the top gap was “the ability to establish and integrate network work defense in depth”. Voters responded that all C/EM activities must start with a fully operational, responsive, sustained and defended network that supports and enables all aspects of C/EM activities and full spectrum operations.

(U//FOUO) For the ASCC, the importance of being able to build and sustain capability while conducting both offense and defensive C/EM activities was the next highest priority. The maintenance of a technical edge in cyberspace and the EMS is of critical importance at the ARCYBER and ASCC level in order to provide each theater the necessary framework for success. The ASCC is reliant on a responsive RDT&E and RDA capability in the GENFOR that can respond to requests for capabilities from the operational forces in order to build and sustain capabilities

(U//FOUO) Division/Corps voting reflected the importance of being able to conduct operations while defending individuals and platforms. In order to perform these missions, situational awareness is a must and will enable the commander to make decisions in an informed manner to not only defend our forces but to take the fight to the adversary.

(U//FOUO) At the BCT and below, the ability to establish, operate, defend, and provide tactical use of the network, along with the ability to integrate C/EM activities within full spectrum operations is critical. Situational awareness is also critical as it provides the commander the ability to employ all capabilities to include C/EM capabilities in their decision making process. The maintenance of a ‘technical edge’ is also critical at this echelon, in this case from a tactical perspective (primarily from a self protection and tactical network perspective). This echelon is particularly reliant on a responsive RDT&E and RDA capability in the GENFOR that can respond to requests for capability from the operational forces. This must entail a responsive acquisition process that supports rapid turn around and delivery of capability to the “tip of the spear”.

(U//FOUO) Figure 16 is a summary of the Gap Prioritization results.



Overall Gap Prioritization

Overall critical areas:
- **#1 operating/defending the network & network-enabled Mission Command (NeMC)**
- **#2 defending individuals & platforms**
- **#3 assessing current/potential threats**
- **#4 operational integration**
- **#5 offensive capabilities**

ASCC critical areas: #1 operating/defending the network & NeMC, #2 research, development, acquisition, #3 offensive & dynamic defense capabilities, #4 assessing current & potential threats, #5 operational integration

Corps/Div critical areas: #1 operating/defending the network & NeMC, #2 operational integration, #3 defending individuals & platforms, #4 C/EM situational awareness, and #5 offensive & dynamic defense capabilities

BCT critical areas: #1 operating/defending the network & NeMC, #2 operational integration, #3 C/EM situational awareness, #4 defending individuals & platforms, and #5 responsive research, development, acquisition

CAC United States Army Combined Arms Center

UNCLASSIFIED/FOUO

(U//FOUO) Figure 13: FNA Gap Prioritization

(U//FOUO) FNA gaps fall within five broad categories:

Network Defense in Depth, Establish, Operate & Maintain the Enterprise; Network-enabled Mission Command

- (U//FOUO) The Army does not have sufficient C/EM capabilities to defend in depth. This is inclusive of both networks and individuals/platforms. (Gap 20)
- (U//FOUO) The C/EM functional needs analysis fully encompasses the Network Enabled Mission Command ICD gaps, primarily in gaps 11, 19, 24, and 40. These are:
    - The Army has limited capability to combine local information/intelligence, position location information, processed sensor data and intelligence, and higher-level environmental information together to define contextual significance/implications and inform understanding, decisions, and action (Gap 40).

  - The Army requires the capability to access, select, filter, share, display and collaborate on fused operations and intelligence information, while operating away from their command post, in air or ground platforms, and while dismounted (Gap 40).
  - The Army has limited capability to access, select, integrate, display and share relevant information from multiple sources (Gap 40).
  - The Army has limited capability to digitally integrate Unified Action Partners during planning and execution (Gap 19).
  - The Army lacks the capability to dynamically adapt network infrastructure and resources to match network transport capabilities with the commander's priorities in support of FSO (Gap 11).

- (U//FOUO) The Army has limited capability to effectively and dynamically transition network command and control from garrison to deployed operations (Gap 15).
- (U//FOUO) The Army lacks a single system and user ID capability to allow Solders access to the network from home station, TDY or deployed at the time of their choosing (Gap 17).
- (U//FOUO) The Army does not have the ability to provide adequate access to critical information, services, and applications in the network (Gap 24).
- (U//FOUO) The Army does not have the ability to establish, operate, and manage a single integrated network that provides unity of effort, reduces complexity, and establishes single network architecture (Gap 11).
- (U//FOUO) The Army has limited ability to collect C/EM relevant information and intelligence, identify threat hardware and software that affects the network, and an ability to perform vulnerability assessments. Brigades do not have the organic capability to collect C/EM information, there are no tools at the operational and tactical level that automatically identify threats on the network, and there are no personnel with the knowledge to analyze C/EM threats and identify threat vulnerabilities (Gap 29, 33, 36).

Defend & Protect Individuals and Platforms

- (U//FOUO) The Army has a limited ability to defend and protect individuals and platforms at all levels (Gap 57).
- (U//FOUO) The Army has a limited ability to detect jamming. Units do not have an adequate capability to detect and locate low powered jamming effecting friendly equipment (ground and air) (Gap 50).

C/EM Interaction & Support

- (U//FOUO) The Army does not have the ability to develop and field materiel solutions to mitigate and defeat new and evolving capabilities because the Army's research, development, and acquisition processes are not responsive enough (Gap 61).

- (U//FOUO) The Army does not have an ability to dynamically manage and utilize the EMS to include joint partners because there is a lack of spectrum managers at battalion level and there is no automated system that performs this requirement (Gap 51, 52, 53, 54).
- (U//FOUO) The Army has limited ability to effective and dynamically deconflict EA assets in operational environments to minimize interference on friendly electronic attack systems (Gap 37).
- (U//FOUO) The Army has a limited ability to effectively integrate all aspects of C/EM modeling and simulation into training. There is a lack of M&S systems which accurately recreate the conditions of FSO (Gap 46).

C/EM Integration & Situational Awareness

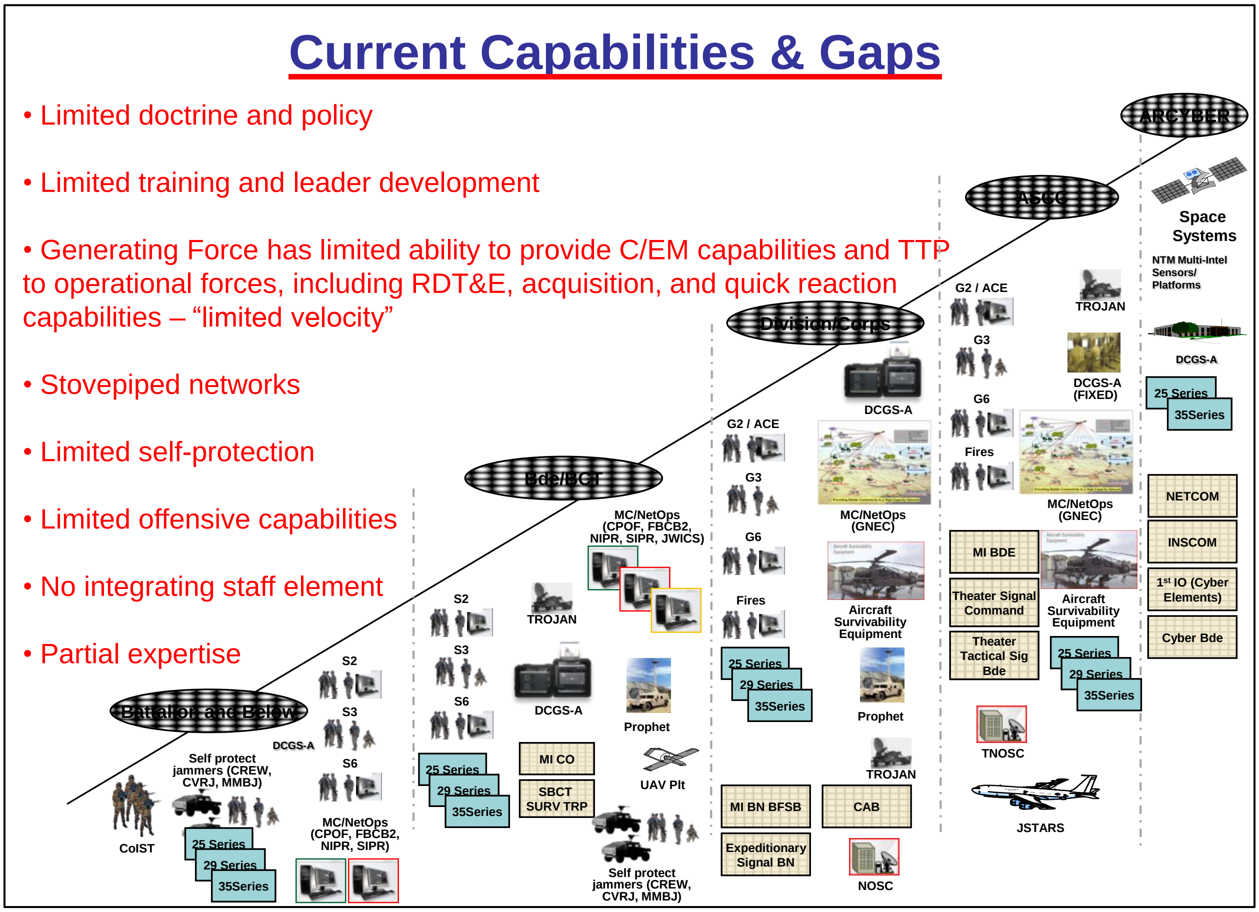
- (U//FOUO) The Army has limited capability to provide advisement of the legal implications of C/EM operations to commanders. Legal C/EM situational awareness is required to allow commanders to make effective decisions and limit negative 2nd and 3rd order effects (Gap 06).
- (U//FOUO) The Army has limited C/EM situational awareness at all echelons because the C/EM contest cannot be clearly described, depicted and displayed as a part of the Common Operating Picture (COP). This degrades the commander's overall SA, increases risk to mission and forces, and will substantially impact every phase of operations to include a robust Phase 0 supporting homeland defense type operations (Gap 40).
- (U//FOUO) The Army lacks C/EM practitioners to perform integrated C/EM because it is currently done in piecemeal fashion by the intelligence, signal, and EW communities. The stovepipe method of performing tasks prevents synergy of these closely aligned areas (Gap 02).
- (U//FOUO) The Army does not have the ability to integrate and employ the full range of C/EM capabilities at all echelons because there is no single integrating organization responsible for the planning, coordination, synchronization and execution of C/EM activities (Gap 02).(U//FOUO) The Army has limited ability to seamlessly pass information to cyber threat investigators after intrusions into to the network or misuse of the network is detected. The Army requires a means to share cyber crime information to the departments and agencies that are responsible for investigating cyber crime (Gap 38).

C/EM Offensive & Dynamic Defense actions

- (U//FOUO) The Army does not have adequate access to the adversaries' network (Gap 04, 26).
- (U//FOUO) The Army does not have offensive C/EM capabilities at the operational and tactical levels that can detect C/EM intrusions to the network and then react to the intrusions through a C/EM attack (Gap 32).
- (U//FOUO) The Army lacks an ability, within its formations, to ascertain what systems the adversary is using, then perform the necessary technical analysis to

determine how to attack/exploit these systems (thru Cyberspace or the EMS), and/or develop the best protective measures to adopt (thru Cyberspace or the EMS) (Gap 33).

- (U//FOUO) The Army does not have adequate capabilities to dynamically defend networks (Gap 28).
- (U//FOUO) The Army has limited ability to conduct effective and dynamic electronic attack (Gap 45).



Current Capabilities & Gaps

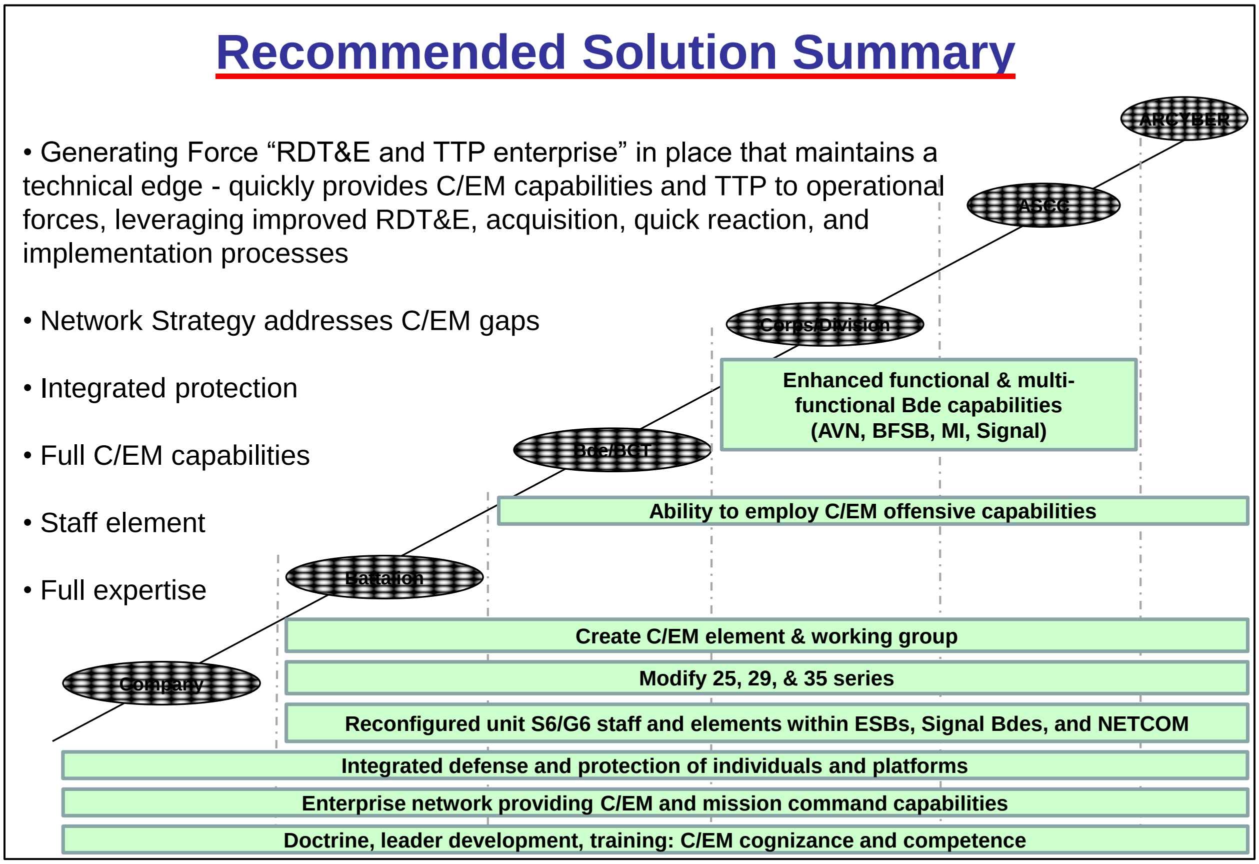
- Limited doctrine and policy
- Limited training and leader development
- Generating Force has limited ability to provide C/EM capabilities and TTP to operational forces, including RDT&E, acquisition, and quick reaction capabilities – “limited velocity”
- Stovepiped networks
- Limited self-protection
- Limited offensive capabilities
- No integrating staff element
- Partial expertise

(U//FOUO) Figure 14: FNA Conclusions

Section VIII Functional Solutions Analysis Results

8-1 FSA Results

(U//FOUO) The study team developed 39 different FSA solutions distributed throughout DOTMLPF and Policy listed below. The resulting solutions were prioritized using feasibility, affordability, impact on the Gap and DOTMLPF implications. The results were:



Recommended Solution Summary

- Generating Force “RDT&E and TTP enterprise” in place that maintains a technical edge - quickly provides C/EM capabilities and TTP to operational forces, leveraging improved RDT&E, acquisition, quick reaction, and implementation processes
- Network Strategy addresses C/EM gaps
- Integrated protection
- Full C/EM capabilities
- Staff element
- Full expertise

Enhanced functional & multi-functional Bde capabilities (AVN, BFSB, MI, Signal)

Ability to employ C/EM offensive capabilities

Create C/EM element & working group

Modify 25, 29, & 35 series

Reconfigured unit S6/G6 staff and elements within ESBs, Signal Bdes, and NETCOM

Integrated defense and protection of individuals and platforms

Enterprise network providing C/EM and mission command capabilities

Doctrine, leader development, training: C/EM cognizance and competence

(U//FOUO) Figure 15: Solution Summary

Solution Summary

Doctrine

D01 – Army Capstone Doctrine – Modify FM 3-0 Operations
D02 – Army War Fighting 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

Organization
O01 – Create the C/EM Staff Element and Working Group, Battalion through ASCC (No growth - Bundled solution with P01, P02, P03)
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)
O03 – Modify Expeditionary Signal Battalion (ESB) structure to provide network connectivity and defense capabilities
O04 – Designate a NETCOM element to coordinate network C2 transition
O05 – Reorganize Brigade/BCT S6 structure IAW the NetOps Construct
O06 – Franchise Theater Network Operations and Security Centers and Network Enterprise Centers
O07 – NetOps Positions in Cyber Brigades

Training
T01 – Incorporate basic C/EM Contest knowledge into individual training
T02 – Incorporate basic C/EM knowledge into home station training
T03 – Incorporate basic tasks that test C/EM knowledge into collective training and CTC events
T04 – Specialized Training and Certification
T05 – Propose a Joint Cyber Training Enterprise
T06 – Establish NetOps Training Program
T07 – Support IA Certification Requirements

Materiel
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
M04 – C/EM Modeling and Simulation
M05 – Defend and Protect Individuals and Platforms
M06 – C/EM Research, Development, Testing and Evaluation (RDT&E), Research, Development and Acquisition (RDA), and Tactics, Techniques, Procedures (TTP) Enterprise

Leadership
L01 – Incorporate basic C/EM knowledge into the Officer Education System, Warrant Officer Education System, Noncommissioned Officer Education System and Civilian Education System
L02 – Incorporate additional specialized C/EM training into 25, 29, and 35 series professional development (BNCOC, ANCOC, CCC, etc)
L03 – Incorporate the C/EM Contest into leader development & education opportunities during training exercises

Personnel

P01 – Create C/EM Integration Specialists for battalion through ASCC C/EM Elements (Bundled solution with O01, P02, and P03)
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)
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)
P04 – Institute special management procedures for specific ARCYBER experts
P05 – 25E Electromagnetic Spectrum Manager (Grade E6-E9)
P06 – Generating Force C/EM DA Civilians

Facility
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

Policy
Policy01 – Update Army Regulations, DA PAMS, DoD Instructions, CJCS Instructions, and US Codes
Policy02 – Update US Code Title 10
Policy03 – Create New Network Policies

Section IX Conclusions and Recommendations

9-1 Fundamental Principles and Common Ideas

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 defined nine fundamental principles 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.

Principle #2: Commanders must consider cyberspace and the EMS as part of their overall operation.

Principle #3: Units simultaneously occupy and act in five domains (air, cyber, land, sea, space) while leveraging the electromagnetic spectrum.

Units simultaneously act across the physical domains, cyberspace, and the electromagnetic spectrum

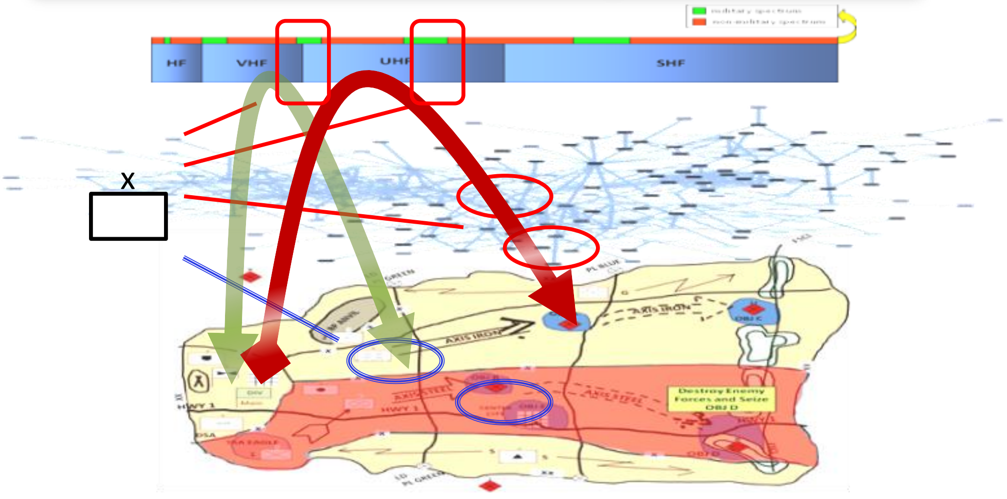


Figure 16: Unit Action Across Domains and Spectrum

It is important to discuss situational awareness in relation to the C/EM contest. C/EM situational awareness is defined as "The immediate knowledge of friendly, adversary and other relevant information regarding activities in and through cyberspace and the EMS. It is gained from a combination of intelligence and operational activity in cyberspace, the EMS, and in the other domains, both unilaterally and through collaboration with our unified action and public-private partners." C/EM situational awareness consists not only of the friendly (blue) situation and adversary (red) situation, but also of the neutral (green) and unknown (yellow) situations. In more practical terms, C/EM situational awareness includes who is on the network, who should be on the network, what is happening on the network, and how is the EMS being utilized by friendly, adversary, neutral and criminal actors. Given that cyberspace and the EMS transcend geographic considerations, units may require awareness of activities outside of their area of operations. In fact, current terms such as area of operations, area of influence, and area of interest may need to be modified.

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.

Principle #6: Cyberspace and the spectrum are 'commons' which defy geographic boundaries and echelon-driven restrictions.

Principle #7: C/EM activities as inherently joint.

Principle #8: 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.

Below are recommended modifications to traditional lexicon terms in order to include cyberspace and the EMS and develop the C/EM SA:

- **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."

9-2 Convergence and Its Implications

(U//FOUO) Joint doctrine recognizes the inter-relationship between cyberspace and the electromagnetic spectrum within its definition of cyberspace: "cyberspace is a global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Within cyberspace, electronics and the electromagnetic spectrum are used to store, modify, and exchange data via networked systems.[8]" This acknowledgement is due to the fact that cyberspace and the EMS are increasingly inter-related or 'meshed' with each other, with many parallels in the use of capabilities. Although certain aspects of cyberspace and the EMS are separate and distinct, understanding the interdependence and relationship is imperative; as cyberspace and the EMS should not be thought of separately, but as a combined, orchestrated part of the whole operation. This inter-relationship can be described in terms of interdependencies, technical convergence, and operational convergence.

Interdependence

(U//FOUO) Cyber is increasing reliant on the EMS, as networks and telecommunication infrastructures increasingly make use of wireless means. Our sensors (also part of the network) require the EMS in order to collect information and then to disseminate it. For this reason, cyber operations must include the employment of capabilities that manage and ensure our access to those portions of the EMS needed for the functioning of the network and related sensors. Conversely, integrated EW and Electromagnetic Spectrum Operations (EMSO) systems generate requirements for a viable network (therefore, a dependence on cyber). This is particularly important for collaborative EW systems, such as the proposed Integrated Electronic Warfare System (IEWS) – which requires a network to interact effectively.

[8] JP 1-02

Technological Convergence

(U//FOUO) Largely driven by advancements in commercial industry, technology is enabling widespread technological convergence between computers, communications, electronic devices, and sensors. This convergence is occurring at both the device level and the supporting infrastructure level. As stated before, smart devices are simultaneously computers, cell phones, cameras, and wireless devices. This trend is enabling a single device to function as sensor, a communication device, an electronic warfare device, and a weapon – often simultaneously. Technological convergence means that individual devices/platforms (and their supporting infrastructures) are both cyber and electronic in nature. And that individual systems and networks leverage both cyberspace and the EMS, and are vulnerable to attack and exploitation from both sources. Over time, the infrastructures used for cyberspace, EW, and EMSO may become indistinguishable – as technological convergence allows our network assets to become our EW assets (and vice versa).

Operational Convergence

(U//FOUO) These elements result in operational convergence: cyberspace effects can be generated in the EMS; EMS effects can be generated in cyberspace. Although aspects of cyberspace operations and electronic warfare are markedly different in implementation, they both focus on similar and often symbiotic effects. For example, a network can be disabled through either cyber warfare or electronic attack. And both can achieve 'kinetic' effects (e.g. cause a system to malfunction –perhaps catastrophically). Finally, both rely on assets such as signal intelligence and spectrum managers.

Leveraging Convergence

(U//FOUO) Properly leveraged, 'convergence' offers more opportunity than liability. In order to leverage these trends, operational, organizational, education and training, and force modernization adjustments are required.

(U//FOUO) From an operational perspective, it's clear that utilization of cyberspace and the EMS is so critical that cyber/electromagnetic activities must be a critical focus of operations, and tightly integrated within the overall operation. This means that C/EM activities must be closely tied to the operations process. Therefore, planners should be 'operators' (i.e. planners with operational experience) that take point in planning and executing Cyber/EM to maximize warfighting capability - desired objectives should drive the process. Cyber/EM must be a well-orchestrated part of the whole operation.

(U//FOUO) Organizationally, given that cyber and electronic capabilities are co-dependent capabilities (one does a lot to set conditions for the other), these capabilities should be highly integrated in combination to achieve desired conditions. Operations and planning staffs should be designed to inherently plan C/EM activities holistically.

(U//FOUO) Education and training should offer an appreciation for convergence and what it means for operations in terms of interdependence and integrated employment. commanders and their staffs must understand the co-dependent nature (convergence) between Cyberspace and the EMS. Although certain aspects of cyberspace and the EMS are separate and distinct, they must recognize that integrated employment is required.

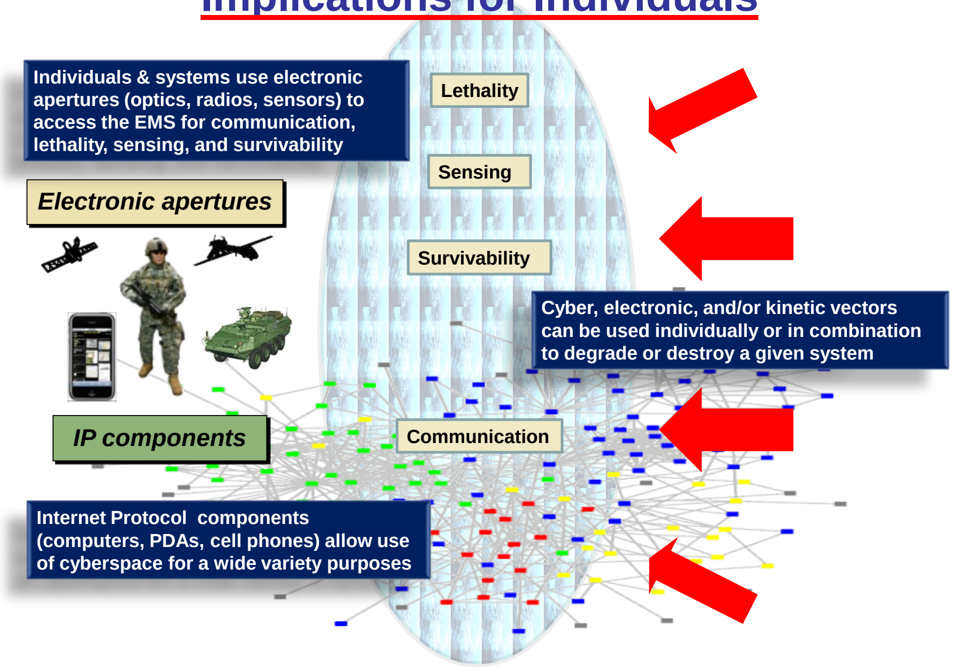
(U//FOUO) Finally, from a capability development perspective, it needs to be understood how technology is creating opportunities for single devices to perform multiple functions across cyberspace and the EMS. Possibilities exist now for single devices to combine communications, cyber attack, electronic attack, sensing and other functions to some degree. As we modernize, we may well decide to leverage these opportunities. In the future, convergence may eventually allow us to think of the network as the infrastructure for cyberspace operations and electronic warfare.

9-3 Implications for Individuals and the Network

Implications for Individuals

Soldiers already rely on both cyberspace and the EMS to accomplish missions while deployed and in garrison. Traditionally this has meant the use of radios, optics and sensors (electronic apertures) which access the EMS for lethality, sensing, survivability, and communications. As the Army becomes more modernized, Soldiers will see devices such as laptop computers, PDAs and smart phones, all IP components, on the battlefield. All of these devices represent the convergence between cyberspace and the EMS and allow Soldiers to access greater capabilities than they could without these devices. However, when adding capabilities such as these on the battlefield, it also adds vulnerabilities adversaries could attempt to exploit. Soldiers and adversaries can use cyber, electronic and/or kinetic vectors to achieve effects. For example, a cyber attack or jamming through the EMS can both have the same effect by preventing devices from working. Individual Soldiers must realize both the benefits and vulnerabilities inherent in the C/EM contest. The Army must plan for these when deciding what Soldiers will use in the field and provide the proper training and awareness.

Implications for Individuals


Individuals & systems use electronic apertures (optics, radios, sensors) to access the EMS for communication, lethality, sensing, and survivability
Lethality
Sensing
Electronic apertures
Survivability
Cyber, electronic, and/or kinetic vectors can be used individually or in combination to degrade or destroy a given system
IP components
Communication
Internet Protocol components (computers, PDAs, cell phones) allow use of cyberspace for a wide variety purposes

(U) Figure 17: Implications for Individuals

Implications for Networks

(U//FOUO) As discussed in paragraph 5-5, understanding the “network”, the study used the LandWarNet (LWN) definition of network, which consists of five layers: platforms and sensors, applications, services, transport infrastructure, and standards. The ‘five layer’ perspective helped illustrate the linkage between larger networks and individual systems within the overall C/EM contest. Future adversaries will be able to employ sophisticated C/EM techniques over time to gain the ability to disrupt or degrade key nodes/sensors and portions of our networks. Therefore, the Army’s network strategy needs to address specific design features that provide resiliency as well as enable mission command. These attributes include:

- (U//FOUO) C/EM infrastructure with the technological diversity and capacity to enable Army forces to respond to, bypass, and fight through network intrusions, and allow Army forces to continue to operate even when systems are degraded or disrupted.
- (U//FOUO) Redundant methods of transmitting, receiving, and storing information.
- (U//FOUO) Features that allow commanders to train and prepare to operate networks under suboptimal conditions.
- (U//FOUO) Create the necessary foundation for offensive and defensive C/EM capabilities by equipping selected systems to be C/EM platforms and delivery systems.

9-4 Maintaining Technical Advantage in the C/EM Contest

(U//FOUO) The operational environment (OE) has changed dramatically with the convergence of the cyberspace domain and the electromagnetic spectrum; astonishing rates of technologic advancements and global proliferation of information and communications technology. Adversaries that are innovative, networked, and technologically-savvy can rapidly capitalize on new emerging technologies to establish and maintain advantages, conduct command and control, recruit, coordinate logistics, raise funds, and propagandize their message. These changes and identified trends indicate that cyberspace and the electromagnetic spectrum (EMS) will remain important entities within the operational environment for the foreseeable future.

(U//FOUO) The 'technological convergence' of cyberspace and EMS capabilities has already occurred. It is the corresponding 'operational convergence', the holistic inclusion of cyber/electromagnetic capabilities into full spectrum operations, which must now be institutionalized across the force. For the Army to prevail in future conflicts, it must leverage both cyberspace and the EMS effectively at the time and place of our choosing, while simultaneously denying our adversaries the same capabilities. This point forms the foundation and is the essence of the Cyber/Electromagnetic Contest (C/EM) which recognizes that ultimate success in 21st century conflicts depends heavily on the ability to gain and maintain an advantage within these two separate but interrelated areas. TRADOC Pam 525-3-3 Mission Command Functional Concept describes the C/EM Contest as, "...that 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".

(U//FOUO) In order to gain and maintain an advantage in the C/EM Contest, the Army must pursue a framework of materiel (tools, weapons) and tactics, techniques, and procedures (TTPs) as in Figure 14. Commanders must be competent, enabled and have situational awareness of the C/EM contest and C/EM environment in order to extend operations in cyberspace and the EMS. Commanders and their units must continually ask four questions:

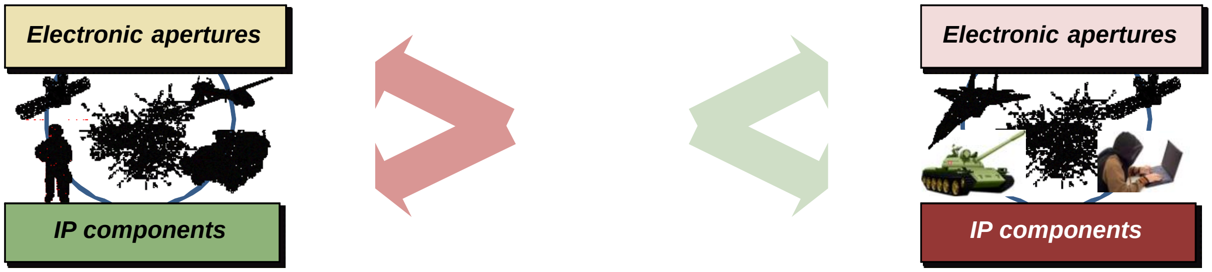
- How do we utilize cyberspace and the EMS?
- How do adversary systems utilize cyberspace and the EMS?
- How will our adversaries exploit and attack through cyberspace and the EMS?
- How can we exploit and attack through cyberspace and the EMS?
- How do we protect our use of and freedom of movement in cyberspace?

(U//FOUO) In an environment where nearly every piece of equipment utilizes both cyberspace and the EMS, these questions must be answered holistically and at "net speed". Due to the dynamic and rapidly changing nature of cyberspace and the EMS, commanders must be prepared to operate and respond at "net speed." Operations in cyberspace can occur nearly instantaneously. Army forces can attack or be attacked with a speed not achievable in the other domains. Success stems from rapid understanding of TTPs combined with rapid development of C/EM tools and weapons.

(U//FOUO) Networks and systems use cyberspace/EMS in an integrated way – the attendant tools, weapons and TTPs must also be integrated. Most devices today, down to the individual soldier level, possess "IP components" which leverage cyberspace, and "electronic apertures" which leverage the electromagnetic spectrum.

(U//FOUO) These components and apertures allow our devices/systems to function yet also represent vulnerabilities. In order to determine how to best exploit or attack a system, or a system of systems, identifying these components and apertures (and how they work in combination) allows determination of either how best to exploit and attack, or how best to operate, manage, and defend said devices.

'Maintaining the Edge'



How do our systems utilize cyberspace & EMS?

How will our adversaries exploit & attack?

How can we exploit & attack adversary systems?

How do adversary systems utilize cyberspace & EMS?

Operate, Manage, and Defend tools; TTPs

Offensive exploit tools; attack weapons; TTPs

- Maintaining a technical edge in the C/EM Contest requires dynamic discernment of both adversarial and friendly requirements, capabilities, and vulnerabilities, combined with innovative development of tools, weapons, and TTPs
- Networks and systems use cyberspace/EMS in an integrated way – the attendant tools, weapons and TTPs will also be integrated
- Dynamically adaptable weapon systems are required (platform, delivery system, payload)

(U) Figure 18: Maintaining the Edge

(U//FOUO) A focused dialogue between intelligence, operations, and materiel developers is required to develop the best possible combinations of tools, weapons, and TTP. Given the agile and innovative nature of our adversaries, this interaction must be very dynamic. The tools, weapons, and TTP are not limited to C/EM capabilities but are dictated by the capabilities available to the commander. Maintaining a technical edge in the C/EM Contest requires dynamic discernment of both adversarial and friendly requirements, capabilities, & vulnerabilities, combined with innovative development of tools, weapons, and TTPs. The Army must use the information about adversary capabilities to mitigate risks to Army/Joint networks. Such information can be used to engineer, install, operate and defend Army networks that are less vulnerable and susceptible to adversary attack and exploitation.

(U//FOUO) The most challenging aspects of maintaining advantage are continually establishing and operating capabilities in a secure fashion and ascertaining how the adversary plans to attack and exploit, while at the same time defining his vulnerabilities. Establishing and operating the network securely requires security to be considered and "built-in" during the network and system engineering processes. Understanding the adversary requires access (either direct or remote) to adversary devices, networks, and systems to generate this information. This is where the Army can leverage its abilities for gaining close access to the adversary's capabilities. Determining better methods to securely utilize the C/EM environment, careful attention to C/EM situational awareness, combined with operations such as site exploitation, distinctly facilitates material development and informs TTPs".

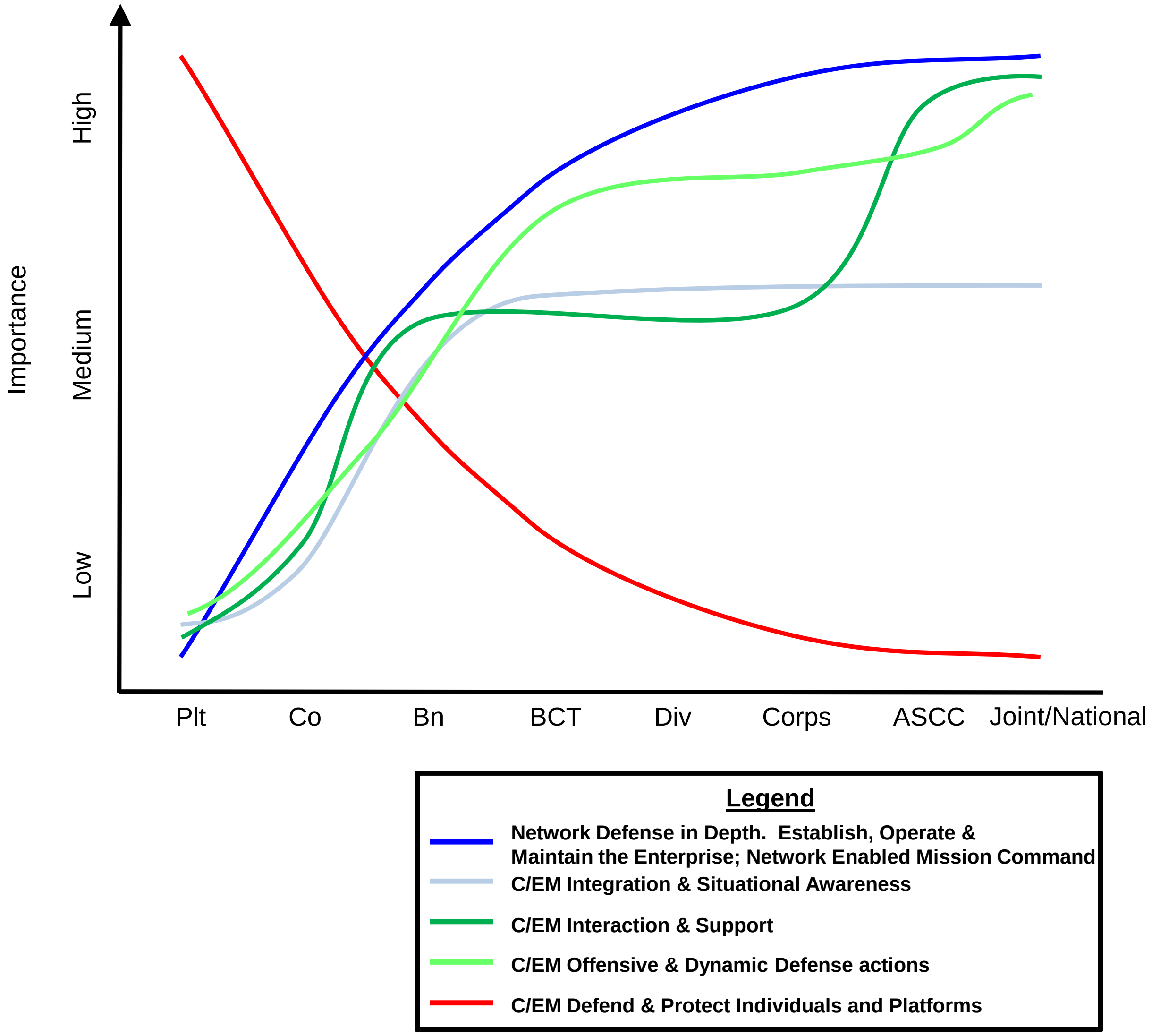
(U//FOUO) The C/EM contest will require dynamically adaptable tools and weapons, given the rapid pace of technological change and the innovative nature of our adversaries. To build a flexible infrastructure for these tools and weapons, it is helpful to think in terms of platforms, delivery systems, and payloads.

- Platforms are the devices or systems which 'launch' the C/EM tool or weapon
- Delivery systems are the devices or systems which access the designated IP components and/or electronic apertures.
- Payloads are the hardware and/or software which create the desired results

(U//FOUO) In order to have the best possible infrastructure for the C/EM contest, Army formations will need the best combination of platforms, delivery systems, and payloads. Materiel development must provide the best possible combination available, through a combination of programs of record and quick reaction capabilities.

9-5 Relative Importance of C/EM Capabilities by Echelon

(U//FOUO) As previously discussed, the C/EM contest is a "Total Force" matter, involving all units across all echelons on an ongoing basis which must be integrated into overall operations as an approach to combined arms. The C/EM contest must be recognized as a dimension of full spectrum operations in which an advantage can be gained or lost. As such, commanders at each echelon must be cognizant of the C/EM contest and understand how to properly leverage cyberspace and the EMS. Each echelon from the smallest tactical formation to the highest command has roles and responsibilities within the C/EM contest which differ depending on the echelon and its function. Figure 15 is a graphical representation showing the importance of key concepts of the C/EM contest by echelon. These key concepts will be further explored later in this document. Each area was evaluated by the study team subjectively in accordance with the findings of the study and determined which echelons each capability set they apply to and how important each is to that echelon. For example, at the platoon level “C/EM Defend & Protect Individuals and Platforms” is paramount, but is much less of a concern at the ASCC and Joint/National level. One of the ways this is evident is the use of CREW by Soldiers on the ground. This is a very important consideration for a platoon or company conducting operations, but less important for the ASCC or Joint/National level in CONUS. On the other hand, “Network Defense in Depth, Establish, Operation & Maintain the Enterprise; Network Enabled Mission Command” is of greater importance to the ASCC and Joint/National levels than to the platoon or company.



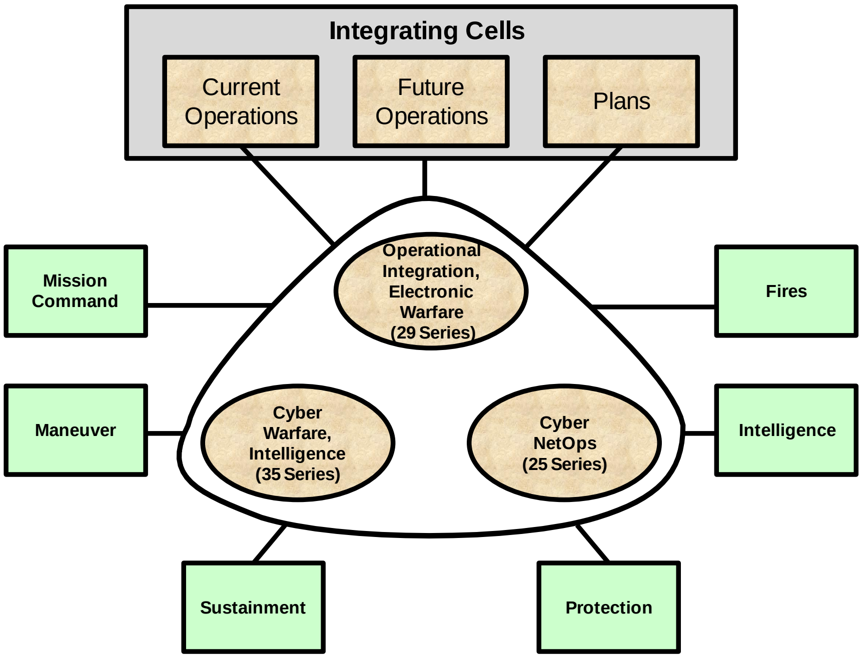
(U//FOUO) Figure 19: Relative Importance by Echelon

9-6 CBA Recommendations

(U//FOUO) Among all the solutions identified, several solutions demonstrate value across multiple gaps and provide the fundamental DOTMLPF construct which will enable the Army to fully engage in the C/EM contest. These solutions in priority order are:

- (U//FOUO) Modify Capstone and supporting doctrine to internalize the C/EM Contest from both an institutional and operational perspective. These changes are low cost, feasible, and will generate the necessary mindset within the force. Pursue policy changes to increase the Army's flexibility to pursue the C/EM contest.

- (U//FOUO) Create a C/EM Integration Staff Element, and a corresponding Cyber/Electromagnetic Working Group, Battalion through ASCC. Leverage the existing EW staff element and Working Group as the foundation for this element and Working Group.



(U//FOUO) Figure 20: C/EM Element and Working Group Integration

- (U//FOUO) Add additional C/EM-related personnel to the new C/EM Element for additional capacity and technical subject matter expertise.

- Add and adapt 25, 29, and 35 series career fields to the C/EM Element to provide necessary C/EM integration and technical expertise and additional capacity.

- (U//FOUO) Reconfigure elements within Expeditionary Signal Brigades, NETCOM, TNOSCs, NECs, and unit G6/S6 staff elements to better support Cyber NETOPS. These are no growth changes

- (U//FOUO) Incorporate C/EM challenges into Leader Development, Education and Training. Examples include individual training, collective training, and specialty training for C/EM professionals. These changes build on existing EW training initiatives.

- (U//FOUO) Modify and leverage the Army Network Modernization Strategy Framework by modifying the Network Enabled Mission Command (NeMC) ICD, Integrated Electronic Warfare System (IEWS) Initial Capability Documents (ICD) and LWN ICD in order to achieve the desired network enterprise, fully equip units for Network-enabled Mission Command, and provide the means for units to be effective across cyberspace and electromagnetic spectrum. Incrementally field capabilities using the LANDWARNET capability set framework.

- (U//FOUO) Modify the LWN ICD, NeMC ICD, IEWS ICD, and platform specific defensive suites to integrate defense and protection of individuals and platforms efforts. This will ensure the proper integration of individual and collective protective systems leveraging network, IEWS, and platform-specific countermeasure suites.

- (U//FOUO) Rely on Quick Reaction Capability programs to providing C/EM unique delivery systems and payloads in a timely manner and maintain currency of tools for threat hardware and software exploitation and vulnerability assessments.

- (U//FOUO) Modify the Army's Modeling and Simulation Strategy to provide C/EM modeling and simulation capabilities for analytic, experimentation, operational, and training purposes.

- (U//FOUO) Develop a C/EM RDT&E, RDA and TTP Enterprise to satisfy the Army's need for a responsive means to provide timely materiel solutions to the operational force.

- (U//FOUO) Ensure adequate facilities are available at the strategic, operational, and tactical levels in order to conduct C/EM activities.

APPENDIX A: References

Section I – Primary Required References

Capstone Concept for Joint Operations (CCJO), Version 3.0, 15 January 2009.

TRADOC Pamphlet 525-3-0, Army Capstone Concept (ACC)**,** *The Army in Joint Operations, The Army's Future Force Capstone Concept 2015-2024* TBP.

TRADOC Pam 525-7-8, *The United States Army's Cyberspace Operations Concept Capability Plan (CCP)*, 2016-2028, Director, ARCIC Approval DRAFT V0.9.

FM 3-0, *Operations*, February 2008

TRADOC Commander Memorandum to Vice Chief of Staff of the Army, *Posturing the Army for Cyber, EW, and IO as Dimensions of Full Spectrum Operations.* (16 Oct 09)

TRADOC Capabilities-Based Assessment (CBA) Guide Version 3.0 28 September 2009.

TRADOC Regulation 71-20, Concepts, Experimentation, & Requirements Determination, 06 Oct 09.

CJCSI 3170.01G, Joint Capabilities Integration and Development System (JCIDS), 1 March 2009.

TRADOC Pam 525-3-1, The U.S Army Operating Concept (AOC) Version 0.7, 18 December 2009

TRADOC Pam 525-7-6, The U.S Army Electronic Warfare Operations for the Future Modular Force 2015-2024 V1.0 16 August, 2007

TRADOC Pam 525-7-16, The U.S. Army Concept Capability Plan for Electromagnetic Spectrum Operations for the Future Modular Force 2015-2024, V1.0 28 December, 2007

TRADOC Pam 525-7-17, The U.S. Army Concept Capability Plan for Network Transport and Services for the Future Modular Force 2015-2024, V1.0, 12 August, 2008

DoDD 8570.01 Information Assurance Workforce Improvement Program, Incorporating Change 2, 20 April 2010

Section II – Required References

ARs, DA pamphlets, field manuals (FM), and DA forms are available at Army Publishing Directorate (APD) – Home Page.

TRADOC publications and forms are available at TRADOC Publications at http://www.tradoc.army.mil.

Field manual 2-01.3, Intelligence *Preparation of the Battlefield/Battlespace* (Oct 2009)

Field Manual 2-19.4, Brigade *Combat Team Intelligence Operations* (Nov 2008)

Field Manual 3-13, *Information Operations* (Nov 2003).

Field Manual 3-36, *Electronic Warfare Operations* (Feb 2009)

Field Manual 5-19, *Composite Risk Management* (Aug 2006)

Field Manual 6-02.70, *Electromagnetic Spectrum Operations* (Sep 2006)

Field Manual 6-02.71, Network *Operations* (Jul 2009).

Joint Operating Environment 2010.

TRADOC G-2 *Operational Environment* 2009-2025.

Department of the Army, Integrated Capabilities Development Team (ICDT) Charter, *Information and Cyberspace*, 31 March 2008.

Department of the Army, Memorandum for Vice Chief of Staff of the Army, *Posturing the Army for Cyber, EW, and IO as Dimensions of Full Spectrum Operations*, 16 October 2009.

Department of Defense, Memorandum For Secretaries of Military Departments, *The Definition of Cyberspace*, May 12, 2008.

Department of Defense, Memorandum For Deputy Secretary of Defense, *Definition of Cyberspace Operations*, 29 Sept 2008.

Department of Defense, Memorandum For Secretaries of the Military Departments, *Command and Control for Military Cyberspace Operations*, Nov 12, 2008.

Department of Defense, Memorandum For Secretaries of the Military Departments, *Command and Control for Military Cyberspace Operations*, Nov 12, 2008.

Department of Defense, Memorandum For Secretaries of the Military Departments, *Establishment of a Subordinate Unified U.S. Cyber Command Under USSTRATEGIC Command for Military Cyberspace Operations*, June 23, 2009.

Department of Defense, Memorandum for Chiefs of the Military Services, *Definition of Cyberspace Operations*, 18 Aug 2009.

Section III – Related References

A related publication is a source of additional information.

Army Posture Statement, 2007.

Army Strategic Planning Guidance, FY2006-2023.

Army Transformation Roadmap.

Battlespace Awareness Joint Functional Concept.

CJCSM 3500.04D *Universal Joint Task List* (UJTL).

Command and Control Joint Integrating Concept.

Senior Oversight Group Pre-Decisional DRAFT Version 0.7 TRADOC Pam 525-X.

FM 7-15 *The Army Universal Task List* (AUTL).

FM Interim 3-90.9 *Future Combat Systems Brigade Combat Team Operations*.

Homeland Defense and Civil Support JOC.

Joint Command and Control Functional Concept.

Joint Concept of Operations for Global Information Grid NetOps (GIG NetOps CONOPS).

Joint Publication 3-0 *Joint Operations*.

Joint Publication 3-13 *Information Operations*.

Major Combat Operations Joint Operating Concept.

Military Support to Stabilization, Security, Transition, and Reconstruction JOC.

National Defense Strategy of the United States.

National Counterintelligence Strategy of the United States.

National Intelligence Strategy of the United States.

National Military Strategy of the United States.

National Security Strategy of the United States.

Net-Centric Environment Joint Functional Concept.

Operational Environment 2009-2025,TRADOC, August 2009

Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction JIC.

Protection Joint Functional Concept.

Quadrennial Defense Review.

Strategy for Homeland Defense and Civil Support.

TRADOC Pamphlet 525-2-1, *The United States Army Functional Concept for See 2015-2024*.

TRADOC Pamphlet 525-3-2 *The United States Army Operating Concept for Tactical Maneuver 2015-2024.*

TRADOC Pamphlet 525-3-3, *The United States Army Functional Concept for Battle Command 2015-2024.*

TRADOC Pamphlet 525-3-4, *The United States Army Functional Concept for Strike 2015-2024.*

TRADOC Pamphlet 525-3-5, *The United States Army Functional Concept for Protect 2015-2024.*

TRADOC Pamphlet 525-3-6, *The United States Army Functional Concept for Move 2015-2024. Senior Oversight Group Pre-Decisional DRAFT Version 0.7 TRADOC Pam 525-X.*

TRADOC Pamphlet 525-3-90, *The United States Army Future Combat Force Operational and Organizational Plan for the Future Combat Systems Brigade Combat Team.*

TRADOC Pamphlet 525-4-1 The United States Army Functional Concept for Sustain 2015-2024.

TRADOC Pamphlet 525-7-1, *The United States Army concept Capability Plan for Unit Protection for the Future Modular Force 2012-2024.*

TRADOC Pamphlet 525-7-4, *The United States Army's Concept Capability Plan for Space Operations 2015-2024.*

TRADOC Pamphlet 525-66, *Military Operations Force Operating Capabilities*.

U.S. Strategic Command's (USSTRATCOM), *Operational Concept for Electronic Warfare (OCEW).*

U.S. Strategic Command's (USSTRATCOM), *Operational Concept for Cyberspace Operations (OCCO).*

Capabilities-Based Assessment (CBA) User's Guide Version 3 Force Structure, Resources, and Assessments Directorate (JCS J-8) March 2009.

TRADOC Regulation 71-20, Concepts, Experimentation, & Requirements Determination, 06 Oct 09.

CJCSI 3170.01G, Joint Capabilities Integration and Development System (JCIDS), 1 March 2009.

APPENDIX B: Glossary

Part I: Abbreviations and Acronyms

ACC	Army Capstone Concept
ACTF	Army Cyber Task Force
ADCON	Administrative Control
AEA	Airborne Electronic Attack
AFC	Army Functional Concept
AFCYBER	Air Force Cyber Command
AOI	Area Of Interest
AOWG	Action Officer Working Group
ARCIC	Army Capabilities Integration Center
ARCYBER	Army Forces Cyber Command
ARFOR	Army Forces
ARFORGEN	Army Force Generation
ASCC	Army Service Component Command
ASI	Additional Skill Identifier
AUTL	Army Universal Task List
BCT	Brigade Combat Team
BDE	Brigade
BOLC	Basic Officer Leaders Course
BN	Battalion
C2	Command and Control
C2W	Command and Control Warfare
CAAT	Combined Arms Assessment Team
CATS	Combined Arms Training Strategy
CAC	Combined Arms Center
CAC-CDID	Combined Arms Center- Capabilities, Development and Integration Directorate
CALL	Center for Army Lessons Learned
CBA	Capabilities Based Assessment
CCC	Captains Career Course
CCJO	Capstone Concept for Joint Operations
CCP	Concept Capability Plan
CDAD	Capabilities Development and Assessments Directorate
CDD	Capabilities Development Directorate/ Document
C/EM	Cyber / Electromagnetic
CERDEC	Communications-Electronics Research, Development, and Engineering Center
CI/KR	Critical Infrastructure / Key Resources
CIP	Critical Infrastructure Protection
CLA	Constraints, Limitations and Assumptions
COCOM	Combatant Commander

CONOPS	Concept Of Operations
CNA	Computer Network Attack
CND	Computer Network Defense
CND RA	Computer Network Defense Response Actions
CNE	Computer Network Exploitation
CNO	Computer Network Operation(s)
CoE	Center(s) of Excellence
CONOPS	Concept of Operations
COP	Common Operational Picture
COTS	Commercial Off The Shelf
CSMB	Capability Set Management Board
CTC	Combat Training Center
CyA	Cyber Attack
CyCM	Cyber Content Management
CyD	Cyber Defense
CyE	Cyber Exploitation
CyEM	Cyber Enterprise Management
CyNetOps	Cyber Network Operations
CyberOps	Cyberspace Operations
CyberSA	Cyber Situational Awareness
CyberSpt	Cyber Support
CyberWar	Cyber Warfare
DAC	Department of the Army Civilian
DCR	DOTMLPF Change Recommendation (Joint)
DCyD	Dynamic Cyber Defense
DHS	Department of Homeland Security
DICR	DOTMLPF (Army) Integrated Capabilities Recommendation (as they pertain to mostly non-material solutions in the Army)
DoD	Department of Defense
DOIM	Directorate Of Information Management
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities
DPS	Defense Planning Scenario
EA	Electronic Attack
EB	Executive Board(s)
EEA	Essential Elements of Analysis
EMS	Electromagnetic Spectrum
EME	Electromagnetic Environment
EMSO	Electromagnetic Spectrum Operations
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
FAA	Functional Area Analysis
FCB	Functional Capability Board
FDU	Force Design Update
FM	Field Manual

FNA	Functional Needs Analysis
FSA	Functional Solution Analysis
FSE	Full Spectrum Environment
FSO	Full Spectrum Operations
GCC	Ground Component Commander
GIG	Global Information Grid
GNEC	Global Network Enterprise Construct
GORB	General Officer Review Board
GOSC	General Officer(s) Steering Committee
GOTS	Government Off The Shelf
HHC	Headquarters and Headquarters Company
HLS	Homeland Security
HNC	Host Nation Coordination
HQDA	Headquarters, Department of the Army
i2WD	Intelligence and Information Warfare Directorate
ICD	Initial Capabilities Document
ICDT	Integrated Capabilities Development Team
ICT	Information and Communications Technology
IA	Information Assurance
IAW	In Accordance With
IE	Information Engagement
IEWS	Integrated Electronic Warfare System
ILE	Intermediate Level Education
INSCOM	Intelligence and Security Command
IO	Information Operations
IP	Information Protection
IPO	Information Proponent Office
IMC	Integrated Management Cell
IT	Information Technology
JCA	Joint Capabilities Areas
JCAC	Joint Cyber Analysis Course
JCD	Joint Capabilities Document
JCIDS	Joint Capabilities Integration and Development System
JFC	Joint Functional Concept
JFCOM	Joint Forces Command
JFLCC	Joint Forces Land Component Commander
JIC	Joint Integrating Concept
JIIM	Joint, Interagency, Intergovernmental, and Multinational
JNAC	Joint Network Analysis Course
JOA	Joint Operating Area
JOC	Joint Operating Concept
JOE	Joint Operational Environment
JP	Joint Publication
JPME	Joint Professional Military Education
JROC	Joint Requirements Oversight Council
JSAP	Joint Staff Action Plan

JTF	Joint Task Force
JUONS	Joint Urgent Operational Needs Statement
JWICS	Joint Worldwide Intelligence Communications System
LE	Law Enforcement
LWN	LandWarNet
MARCYBER	Marine Forces Cyber Command
MC	Mission Command
MCO	Major Combat Operations
METT-TC	Mission, Enemy, Terrain and Weather, Troops and Support Available, Time Available, Civil Considerations
MI	Military Intelligence
MILDEC	Military Deception
MLS	Multi-Level Scenario
MRE/MRX	Mission Readiness Exercise
M&S	Modeling and Simulation
MSFD	Multi Service Force Deployment
MOS	Military Occupational Specialty
NEC	Network Enterprise Center
NETCOM	United States Army Network Enterprise Technology Command
NIPS	Network Intrusion Prevention System
NetOps	Network Operations
NeMC	Network Enabled Mission Command
NG	National Guard
NGB	National Guard Bureau
NIPR	Non-classified Internet Protocol Router Network
NRF	National Response Framework
NSA	National Security Agency
NT	Network Transport
OE	Operational Environment
OIA&C	Office of Information Assurance and Compliance
ONS	Operational Needs Statement
OPCON	Operational Control
OSD	Office of the Secretary of Defense
PCC	Pre-Command Course
PEG	Program Evaluation Group
PEO	Program Executive Officer
PPBES	Planning, Programming, Budgeting and Execution System
PIA	Post Independent Analysis
PMJ	Professional Military Judgment
POR	Program Of Record
QA	Qualitative Analysis
QRC	Quick Reaction Capability
RC	Required Capabilities
RDA	Research, Development, and Acquisition
RDT&E	Research, Development, Test and Evaluation

REF	Rapid Equipping Force
ROE	Rules Of Engagement
SA	Situational Awareness
SAG	Senior Advisory Group
SE	Site Exploitation
SECDEF	Secretary of Defense
SES	Senior Executive Service
SI	Skill Identifier
SIGINT	Signals Intelligence
SIPR	Secret Internet Protocol Router Network
SM	Spectrum Management
SMDC	Space and Missile Defense Command
SME	Subject Matter Expert
SOG	Senior Oversight Group
SSC	Soldier Systems Center
SSE	Sensitive Site Exploitation
SSSP	Steady State Security Posture
SWAP	Size, Weight, and Power
TCM	TRADOC Capability Manager(s)
T/C/S	Tasks, Conditions and Standards
TE	Technical Exploitation
TRAC	U.S. Army Training and Doctrine Command Analysis Center
TRADOC	U.S. Army Training and Doctrine Command
TRISA	TRADOC Intelligence Support Activity
TSCP	Theater Security Cooperation Plan
TSE	Tactical Site Exploitation
UAV	Unmanned Aerial Vehicle
UCP	Unified Command Plan
UJTL	Universal Joint Task List
USCYBERCOM	U.S. Cyber Command
USNORTHCOM	U.S. Northern Command
USSOCOM	U.S. Special Operations Command
USSTRATCOM	U.S. Strategic Command
WfF	Warfighting Functions
WOAC	Warrant Officer Advanced Course
WOBC	Warrant Officer Basic Course
WOSSC	Warrant Officer Senior Staff Course

Part II: Terms and Definitions

Combined Arms (CA) – Combined arms is the synchronized and simultaneous application of the elements of combat power to achieve an effect greater than if each element of combat power was used separately or sequentially. (FM 3-0)

Computer Network Attack (CNA) – Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13, FM 3-0)

Computer Network Defense (CND) – Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. (JP 6-0/JP 1-02)

Computer Network Defense Response Actions (CND RA) – Deliberative, authorized defensive measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. Response actions extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks. (Assistant Secretary of Defense Memorandum, "Guidance for Computer Network Response Actions", dated 26 Feb 2010 2003)

Computer Network Exploitation (CNE) – Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 6-0/JP 1-02)

Computer Network Operations (CNO) – Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (JP 3-13, JP 1-02).

Counterintelligence – Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (JP 2-0).

Critical Infrastructure / Key Resources (CI/KR) – Critical Infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key Resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Critical infrastructure protection – Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, and others (JP 3-28).

Cyber Attack (CyA) – CyA actions combine CNA with other enabling capabilities (such as, EA, physical attack, and others) to deny or manipulate information and/or infrastructure (TRADOC Pam 525-7-8).

Cyber Content Management (CyCM) – CyCM is the technology, processes, and policy necessary to provide awareness of relevant, accurate information; automated access to newly discovered or recurring information; and timely, efficient, and assured delivery of information in a usable format (TRADOC Pam 525-7-8).

Cyber Counterintelligence – Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions (JP 2-01.2).

Cyber Defense (CyD) – CyD are actions that combine information assurance, computer network defense (to include response actions), and critical infrastructure protection with enabling capabilities (such as, EP, critical infrastructure support, and others) to prevent, detect, and ultimately respond to an adversaries ability to deny or manipulate information and/or infrastructure. CyD is integrated with the dynamic defensive aspects of CyberWar to provide defense in depth (TRADOC Pam 525-7-8).

Cyber/Electromagnetic Contest (C/EM) – A dimension of full spectrum operations which requires military forces to gain an advantage, protect that advantage and place adversaries at a disadvantage, across both cyberspace and the electromagnetic spectrum. This includes the ability to gain friendly information to ensure timely, accurate and relevant information. It involves information protection denying enemies, adversaries and others the opportunity to exploit friendly information for their own purposes. (TRADOC Pam 525-7-8)

Cyber Enterprise Management (CyEM) – CyEM is the technology, processes, and policy necessary to effectively operate computers and networks (TRADOC Pam 525-7-8).

Cyber Exploitation (CyE) – CyE is actions combining CNE with enabling capabilities (such as, ES, SIGINT, and others) for intelligence collection and other efforts (TRADOC Pam 525-7-8).

Cyber Network Operations (CyNetOps) – Is the component of CyberOps that establishes, operates, manages, protects, defends, commands, and controls the LandWarNet,[9] critical infrastructure/key resources (CIKR), and other relevant

[9] LandWarNet is the Army's contribution to the Global Information Grid that consists of all globally interconnected, end-to-end set of U.S. Army information capabilities, associated processes, and personnel for collecting,

cyberspace. NetOps consists of three core elements: enterprise management, content management, and network defense (includes computer network defense).

Cyber Situational Awareness (CyberSA) – Is the immediate knowledge of friendly, adversary and other relevant information regarding activities in and through cyberspace and the electromagnetic spectrum. CyberSA enables informed decision-making. It is gained from a combination of intelligence and operational activity in cyberspace, the electromagnetic spectrum (EMS), and in the other domains, both unilaterally and through collaboration with our unified action and public-private partners.

Cyberspace (Cyber) – A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-0 Change 2 dated 22 March 2010)

Cyberspace Operations (CyberOps) – Is the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in and through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (CJCS Memo dated 18 August, 2009).

Cyber Support (CyberSpt) – Are those supporting activities which are generated and employed to specifically enable CyNetOps and CyberWar. They include penetration testing, CyberOps red/blue/green teams, reverse engineering malware, site exploitation, incident handling, counter intelligence, law enforcement, forensics, RDT&E, combat development, and acquisition. These are low density/high demand capabilities that must be expanded to support emerging requirements. Collectively, they form an agile, responsive, and sustainable support enterprise for CyberOps.

Cyber Warfare (CyberWar). – Orients on adversaries to seize and maintain the initiative through the planning, coordinating, integrating and conducting cyber attack and cyber exploitation. The intelligence aspects of CyberWar complement and are integrated with the defensive aspects of CyNetOps providing defense in depth. CyberWar is the component of CyberOps that deters, denies, and defeats adversaries and consists of cyber attack and cyber exploitation combined with enabling capabilities. Cyber attack are actions that combine computer network attack (CNA) with other enabling capabilities (e.g., electronic attack (EA), physical attack, etc.) to deny or manipulate information and/or infrastructure in cyberspace. Cyber exploitation are actions that combine computer network exploitation (CNE) with the enabling capability of electronic warfare support (ES) for intelligence collection and other efforts in and

processing, storing, disseminating, and managing information on demand supporting warfighters, policy makers, and support personnel. It includes all U.S. Army (owned and leased) and leveraged DOD/joint communications and computing systems and services, software (including applications), data security services, and other associated services. LandWarNet exists to enable the war fight through Battle Command. (TRADOC Pamphlet 525-5-600) through cyberspace to gather data from adversary or other automated information systems and networks.

Defense Critical Electric Infrastructure – The term ‘defense critical electric infrastructure’ means any infrastructure located in the United States (including the territories) used for the generation, transmission, or distribution of electric energy that—

a. Is not part of the bulk-power system; and
b. Serves a facility designated by the President pursuant to subsection (d)(1), but is not owned or operated by the owner or operator of such facility. (111th US Congress – HR 4061, Grid Security Committee)

Defense Critical Electric Infrastructure Vunerability – The term ‘defense critical electric infrastructure vulnerability’ means a weakness in defense critical electric infrastructure that, in the event of a malicious act using electronic communication or an electromagnetic weapon, would pose a substantial risk of disruption of those programmable electronic devices and communications networks, including hardware, software, and data, that are essential to the reliability of defense critical electric infrastructure. (111th US Congress – HR 4061, Grid Security Committee)

Dynamic Cyber Defense (DCyD) – DCyD actions combine policy, intelligence, sensors, and highly automated processes to identify and analyze malicious activity, simultaneously tip and cue and execute preapproved response actions to defeat attacks before they can do harm. DCyD uses the Army defensive principles of security, defense in depth, and maximum use of offensive action to engage cyber threats. Actions include surveillance and reconnaissance to provide early warnings of pending enemy actions. DCyD is integrated with the defensive aspects of CyNetOps to provide defense in depth (TRADOC Pam 525-7-8).

Electromagnetic Environment (EME) – The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. It is the sum of electromagnetic interference; electromagnetic pulse; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static. This also may be referred to EME. (JP 3-13.1)

Electromagnetic Spectrum (EMS) – The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. See also **electronic warfare.** (JP 3-13.1)

Electromagnetic Weapon – The term ‘electromagnetic weapon’ means a weapon (other
than a nuclear device) capable of disabling, disrupting, or destroying electronic equipment by transmitting 1 or more pulses of electromagnetic energy, such as high-power radio frequency or microwave energy. (111th US Congress – HR 4061, Grid Security Committee)

Electronic Attack (EA) – Division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-13.1)

Electronic Protection (EP) – Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-13.1)

Electronic Warfare (EW) – Is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support (JP 3-13.1)

Electronic Warfare Support (ES) – Division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (JP 3-13.1, FM 3-0)

Frequency Deconfliction – A systematic management procedure to coordinate the use of the EMS for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management (JP 3-13.1).

Frequency Management – The requesting, recording, deconfliction of and issuance of authorization to use frequencies (operate electromagnetic spectrum dependent systems) coupled with monitoring and interference resolution processes (JP 6-0).

Full Spectrum Operations (FSO) – Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment. Mission command that conveys intent and an appreciation of all aspects of the situation guides the adaptive use of Army forces (FM 3-0).

Functional Area Analysis (FAA) – An FAA identifies the mission area or military problem to be assessed, the concepts to be examined, the timeframe in which the problem is being assessed, and the scope of the assessment. It also describes the relevant objectives and CONOPs or concepts, and lists the relevant effects to be generated. Since a capability is the ability to generate an effect, the FAA connects capabilities to the defense strategy via objectives, concepts, and CONOPs. Furthermore, the capabilities identified in the FAA also scope the assessment and identify which capabilities will be examined. The capabilities must be defined (with associated tasks, conditions, and standards) using the common lexicon for capabilities established in the Joint Capability Areas (JCAs).

Functional Needs Analysis (FNA) – The FNA assesses the capabilities of the current and programmed force to meet the relevant military objectives of the scenarios chosen in the FAA using doctrinal approaches. Using the standards and evaluation criteria described in the FAA, the FNA assesses whether or not an inability to achieve a desired effect (a capability gap) exists. The FNA also identifies any capability areas that may have overlaps or redundancies. These become opportunities to determine during the FSA whether there is unnecessary redundancy or overlap in solutions sets that can be streamlined to support developing solution sets for the validated gaps.

Functional Solutions Analysis (FSA) – The functional solutions analysis evaluates solutions from an operational perspective across the DOTMLPF domains. The FSA is a joint assessment of potential DOTMLPF and policy approaches to solving, or at least mitigating, one or more of the capability gaps identified in the FNA. The approaches identified should include the broadest possible range of joint possibilities for addressing the capability gaps. For each approach, the range of potential sustainment alternatives must be identified and evaluated as part of determining which approaches are viable. The results of the FSA will influence the future direction of integrated architectures and provide input to capability roadmaps.

Gap – A capability gap is a recognized inability of the force to accomplish any required task to standard given the conditions presented during the wargaming of a scenario. (TRADOC Capabilities-Based Assessment (CBA) Guide Version 3.0 28 Sept. 2009).

Global Information Grid (GIG) – The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 1-02).

Global Network Enterprise Construct (GNEC) – GNEC is an Army-wide strategy that will transform LandWarNet to an enterprise activity. The GNEC Vision is to "Operationalize LandWarNet; transforming to deliver a global, standardized, protected and economical network enterprise – effective, secure and well-managed. GNEC is the focused, timed-phased, prioritized, resource sensitive Army-wide strategy to transition LandWarNet from many loosely-affiliated independent networks into a truly global capability that is designed, deployed and managed as a single integrated enterprise." (Army CIO/G-6, 23 January 2009)

Grid Security Threat – The term 'grid security threat' means a substantial likelihood of:

a.(i) A malicious act using electronic communication or an electromagnetic weapon, or a geomagnetic storm event, that could disrupt the operation of those programmable electronic devices and communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system or of defense critical electric infrastructure; and
a (ii) Disruption of the operation of such devices and networks, with significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure, as a result of such act or event; or
b.(i) A direct physical attack on the bulk-power system or on defense critical electric infrastructure; and
b.(ii) Significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure as a result of such physical attack.
(111th US Congress – HR 4061, Grid Security Committee)

Grid Security Vulnerability – The term 'grid security vulnerability' means a weakness that, in the event of a malicious act using electronic communication or an electromagnetic weapon, would pose a substantial risk of disruption to the operation of those programmable electronic devices and communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system. (111th US Congress – HR 4061, Grid Security Committee)

Information - Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation.

Information Assurance (IA) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 3-13, FM 3-0)

Information Engagement (IE) –

- Definition 1 – The integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, Leader and Soldier engagement to support both efforts.
  (FM 3.0)
- Definition 2 – Actions aimed at informing and educating U.S., allied, and other relevant publics and actors in order to gain and maintain their trust, confidence, and support. Information Engagement is characterized by a comprehensive commitment to transparency, accountability, and credibility. (CG CAC White Paper)

Information Environment – The aggregate of individuals, organizations, and systems.

Information Operations (IO) – The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (JP 1-02)

Information Protection (IP) – Active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes. (FM 3-0)

Intelligence – The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity (JP 1-02).

Intelligence Preparation of the Battlespace (IPB) – An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process.

Intelligence, Surveillance, and Reconnaissance (ISR) – Activities that synchronize and integrate the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations (JP 2-01).

Internet – An electronic communications network that connects computer networks and organizational computer facilities around the world (Merriam Webster).

LandWarNet (LWN) – The Army's contribution to the Global Information Grid (GIG) that consists of all globally interconnected, end-to-end set of U.S. Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand supporting warfighters, policy makers, and support personnel. It includes all U.S. Army (owned and leased) and leveraged DOD/Joint communications and computing systems and services, software (including applications), data security services, and other associated services. LandWarNet exists to enable the war fight through Battle Command (TP 525-5-600, LandWarNet CONOPS).

Mission Command (MC) – Achieving the potential mission power of Army forces requires a balanced and comprehensive approach to developing capabilities that advance both the art and science of mission command and are integrated and synchronized from inception through employment. Mission command capabilities must enable leaders at all echelons to exercise the art and science of mission command to maximize the effectiveness of the force. (TRADOC 525-3-0, The Army Capstone Concept, 21 Dec 2009)

Networks – Are defined as interconnected, end-to-end sets of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information. Networks are considered to consist of five layers: platforms and sensors, applications, services, transport infrastructure, and standards. (LandWarNet CONOPS).

Network Enterprise Center – Provides local (post, camp, base) tenant units with access to the network, network services, communications, and information enterprise services.

Network Operations (NetOps) – Activities conducted to operate and defend the Global Information Grid. (JP 1-02)

Network Service Center – A global network operations and service desk functions, information services, and network connectivity through distributed TNOSCs, area processing centers, and regional hub nodes.

Operational Environment (OE) – Is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0).

Protected Information – The term 'protected information' means information, other than classified national security information, designated as protected information by the Commission under subsection (e)(2)

a. That was developed or submitted in connection with the implementation of this Section;
b. That specifically discusses grid security threats, grid security vulnerabilities, defense critical electric infrastructure vulnerabilities, or plans, procedures, or measures to address such threats or vulnerabilities; and
c. The unauthorized disclosure of which could be used in a malicious manner to impair the reliability of the bulk-power system or of defense critical electric infrastructure.
(111th US Congress – HR 4061, Grid Security Committee)

Relevant Cyberspace/EMS – Is defined as those portions of cyberspace and the EMS that the unit is using for operations (e.g. communications, sensing, attack, and defense). It also includes those portions of cyberspace/EMS that are potential avenues for adversarial operations. (Chief, Concepts Determination Division, CAC-CDID, COL Jeffrey Witsken).

Research, Development and Acquisition (RDA) – Total fielding of a system consisting of hardware, software, logistic support, manuals, organizations, doctrine, facilities, personnel, training and spares. (How the Army Runs)

Research, Development, Testing and Evaluation (RDT&E) – Research, development, test and evaluation efforts performed by contractors and government installations to develop equipment, material, or computer application software; its Development Test and Evaluation (DT&E); and its Initial Operational Test and Evaluation (IOT&E). (ACQuipedia Online Acquisition Encyclopedia: https://acc.dau.mil)

Sensitive Site Exploitation (SSE) – A related series of activities inside a captured sensitive site to exploit personnel documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents. (JP 3-31)

Site Exploitation (SE) – Related activities that gather and make use of the personnel, information and/or material found during the conduct of operations in order to support tactical, operational, and strategic objectives.

Specified Cyberspace/EMS – Is defined as portions of cyberspace/EMS assigned to a given unit for awareness/operational purposes that is beyond those portions normally of interest. (TRADOC Pam 525-7-8, Cyberspace Concept Capability Plan, 2016-2028)

Strategic Communication (SC) – Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. (JP 5-0)

Tactical Site Exploitation (TSE) – The actions taken to ensure those personnel, documents, electronic data, and other material at a site are identified, evaluated, collected, and protected IOT facilitate follow on actions.

Technical Exploitation (TE) – The application of specialized means to assess personnel, documents, electronic data, and other material IOT generate intelligence to support follow on actions.

APPENDIX C: Functional Area Analysis (FAA)

Appendix C FAA Complete Report

(U) Appendix C classified FAA supporting documentation is located on the C/EM CBA AKO-S Sharepoint site and on JWICS. In order to access the Cyber/EM CBA AKO-S site you will need to forward your AKO-S username to Mr. Malcolm Martin or Mr. Jim Richter at: malcolm.w.martin@conus.army.mil , james.richter@conus.army.mil or visit the AKO-S Sharepoint site at URL http://www.us.army.smil.mil/suite/page/18109 and request access. Your access will be granted within the next two business days during normal working hours.

(U) For access to the JWICS classified FAA supporting documentation, email the above POCs and request a copy of the file. This file contains in-depth T/C/S that support the study.

APPENDIX D: Functional Needs Analysis (FNA)

Appendix D FNA Complete Report

(U) Appendix D classified FNA supporting documentation is located on the C/EM CBA AKO-S Sharepoint site and on JWICS. In order to access the Cyber/EM CBA AKO-S site you will need to forward your AKO-S username to Mr. Malcolm Martin or Mr. Jim Richter at: malcolm.w.martin@conus.army.mil , james.richter@conus.army.mil or visit the AKO-S Sharepoint site at URL http://www.us.army.smil.mil/suite/page/18109 and request access. Your access will be granted within the next two business days during normal working hours.

(U) For access to the JWICS classified FNA supporting documentation, email the above POCs and request a copy of the file. This file contains more in-depth information on capabilities that support the study.

APPENDIX E: Functional Solutions Analysis (FSA)

Appendix E FSA Complete Report

(U) Appendix E unclassified FSA is located on both the NIPR and SIPR C/EM CBA AKO/AKO-S Sharepoint sites. In order to access the Cyber/EM CBA AKO/AKO-S site you will need to forward your AKO/AKO-S username to Mr. Malcolm Martin or Mr. Jim Richter at: malcolm.w.martin@conus.army.mil , james.richter@conus.army.mil or visit the AKO Sharepoint site at URL https://combinedarmscenter.army.mil/wgrp/cecba/default.aspx and the AKO-S Sharepoint site at URL http://www.us.army.smil.mil/suite/page/18109 and request access. Your access will be granted within the next two business days during normal working hours.