



**The United States Army
Concept Capability Plan for**

Unit Protection

**for the
Future Modular Force**

2012 - 2024

Version 1.0

28 February 2007



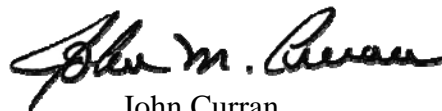
Foreword

*From the Director
U.S. Army Capabilities Integration Center*

The *United States Army Concept Capability Plan for Unit Protection for the Future Modular Force 2012-2024* will serve as the baseline document to integrate protection capabilities for the future Modular Force. The concept capability plan (CCP) focuses on the application of integrated protection capabilities from different proponents in the Army and introduces a goal to develop a 360° hemispherical protection capability across the force. The approval of this CCP will lead to a protection focused capabilities based assessment (CBA). This intensive study will identify protection solutions for the future Modular Force. While this CBA will focus on unit (group protection) operations, and the protection of that unit, the results will have far reaching impact on the protection of platforms and Soldiers. During its draft and staffing procedures the UP CCP has significantly influenced the development of other Army CCPs, specifically, Army Space and Army Combat Identification.

Within this document, the UP integrated capabilities development team has indicated specific functions the Army must successfully execute in order to protect operations from numerous threats. These functions limit enemy surprise and enable a commander to shape the battlefield for tactical advantage resulting in the ability to *see first, understand first, act first, reengage at will, and finish decisively*. The functions of *detect, assess, decide, act, and recover* will assist the integrated capabilities development team in developing integrated protection solutions during the 2012-2024 timeframe. As UP will support Army operations, it will further affect joint, interagency, and multi-national (JIM) operations, by providing an integrated protection sanctuary that enables freedom of movement and decisive operations. The protection improvements provided to Army operations may foster integrated solutions to the joint force.

As with all concepts, concept capability plans are in continuous evolution. This CCP will be refined and updated as new learning emerges from research, joint and Army wargaming, experimentation, and combat development. Many of the Unit Protection enabled capability requirements introduced in this CCP will be further developed in other proponent capability documents. As this CCP crosses so many joint and Army functional areas, I strongly encourage its use in our interaction with other proponents, Services, and joint organizations.



John Curran
Lieutenant General
Director, ARCIC

Executive Summary

Introduction

a. Unit protection (UP) is the integration of active and passive capabilities and processes, provided to operational and or tactical units, across the range of military operations (ROMO) to protect unit personnel, assets, and information against traditional, catastrophic, disruptive and irregular air, ground, chemical, biological, radiological, nuclear and high-yield explosives (CBRNE), electronic, information and intelligence threats, in order to conserve unit fighting potential so it may be applied by commanders at the decisive time and place.

b. Basis of UP. In support of unit protection operations, the Army must *detect, assess, decide, act, and recover* from varied types of threats by producing technical countermeasures and tactical procedures to reduce or eliminate the number and effectiveness of these attacks. These functions will assist a commander in shaping the battlefield for tactical advantage; enabling the ability to *see first, understand first, act first, reengage at will, and finish decisively*. UP will support Army, and consequently JIM operations, by providing an integrated protection sanctuary that enables freedom of movement and decisive operations. This capability will require the integration of UP functions and capabilities to see and understand the battlefield (the friendly and adversary environment); develop course of actions; act swiftly to provide friendly warning and nonlethal to increasingly lethal enemy warning, and proactive lethal and nonlethal protection; and recover UP systems and capabilities to enable the return of UP operations and provide sanctuary for relevant combat operations.

Operational Problem

a. The United States (U.S.) Army has numerous protection capabilities that are not integrated. Failure to integrate protection capabilities and provide adaptive solutions to protection will be detrimental to forces operating in the future operational environment. Protecting U.S. military forces has never been as complex a mission as it is in today's adversarial environment. Current and future adversaries will employ techniques such as rockets, artillery, and mortars, cruise and ballistic missiles, rotary and fixed wing aircraft, terrorist activity, weapons of mass destruction, insurgent activity, unmanned aircraft systems, electronic warfare, infrared electro-optical, radio frequency, directed energy weapons and improvised explosive devices. This environment will likely worsen, and adversaries will prove adaptive to our capabilities.

b. Protection capabilities must be integrated in order to provide 360° hemispherical unit protection; a modular, multi-layered, integrated, full dimensional protection family of systems (FoS) and or system of systems (SoS) capability against air, ground, CBRNE, electronic, information, and intelligence threats. These capabilities will aid friendly forces to counter the large range of hostile threats adversaries possess and are plausible to possess. The UP CCP serves to conceptualize the integration of capabilities in order to improve and reinforce a commander's ability to protect personnel, assets, and information on the battlefield that are critical to strategic, operational, and tactical level mission success.

Solution Synopsis

a. The integration of UP technologies and capabilities will provide critical 360° hemispherical protection during all phases of operations. The UP CCP conceptualizes the integration of protection capabilities from different proponents in the U.S. Army. These capabilities *may* be incorporated into Joint protection processes across the land, air, sea, space, and cyberspace domains. These capabilities provide the commander with an additive, modular, tailorable, integrated FoS/SoS protective suite that facilitate the ability to configure sensor and response systems to the environmental and threat target set.

b. These UP capabilities must integrate with Army battle command systems and joint command and control systems, global position systems and other force tracking systems to share information across the global information grid. The current listing of required capabilities should be interpreted as optimum capabilities during the 2012-2024 timeframe.

Key Ideas

The combination of UP capabilities, applied through Army echelons to the joint force offer a wealth of active resources against a thinking and adaptive force. UP will provide, through the integration of capabilities and doctrine, organizations, training, materiel, leadership and education, personnel, and facilities processes, a proactive and deadly protection force. The five functions: *detect*, *assess*, *decide*, *act* and *recover* are interconnected and compliment a full dimensional protection capability.

Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Monroe, Virginia 23651-1047

TRADOC Pamphlet 525-7-1

28 February 2007


Military Operations

THE UNITED STATES CONCEPT CAPABILITY PLAN FOR UNIT PROTECTION
FOR THE FUTURE MODULAR FORCE 2012-2024*

FOR THE COMMANDER:

OFFICIAL:

THOMAS F. METZ
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff



RANDALL L. MACKEY
Colonel, GS
Deputy Chief of Staff, G-6

History. This publication is a new United States Army Training and Doctrine Command (TRADOC) concept capability plan (CCP) developed as part of the Army Concept Strategy for the future Modular Force and as part of the capabilities based assessment (CBA) process.

Summary. TRADOC Pamphlet (Pam) 525-7-1, *The United States Army Concept Capability Plan for Unit Protection for the Future Modular Force 2012-2024* provides a capability plan for integrating Army unit protection requirements and capabilities and fuels the CBA. The UP CCP focuses on the strategic, operational and tactical application of integrated protection capabilities, both static and mobile, across the range of military operations. The ideas presented are fully integrated within the evolving context of the future operating environment, joint and Army strategic guidance, and the Army Concept Strategy, specifically *TRADOC Pam 525-3-5, The United States Army Functional Concept for Protect 2015-2024*.

Applicability. This pamphlet applies to all TRADOC, Department of the Army (DA) services, agencies, and activities. It functions as the basis for developing required solution sets related to the future Modular Force unit protection functions within the domains of doctrine, organizations, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) requirements.

Proponent and supplementation authority. The proponent of this pamphlet is the TRADOC Headquarters, Director, Army Capabilities Integration Center (ARCIC). The proponent has the

authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. Do not supplement this pamphlet without prior approval from Director, TRADOC ARCIC (ATFC-ED), 33 Ingalls Road, Fort Monroe, VA 23651-1061.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, TRADOC (ATFC-ED), Fort Monroe, VA 23651-1046. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program Proposal).

Distribution. This publication is only available on the TRADOC Homepage at <http://www.tradoc.army.mil/tpubs/pamndx.htm>.

Table of Contents

	Paragraph	Page
Foreword		i
Executive Summary		ii
Chapter 1		
Introduction		
Purpose	1-1	4
References	1-2	4
Explanation of abbreviations and terms	1-3	4
Functional Area	1-4	5
Scope	1-5	5
Relation to the Family of Joint and Army Concepts	1-6	5
Operational Outcome	1-7	10
Complementing the Joint Warfighting Force	1-8	10
Chapter 2		
Concept Capability Plan		
Basis of Unit Protection	2-1	10
The Problem	2-2	11
Joint Operating Environment	2-3	12
The Future Operating Environment	2-4	13
The Complex Protection requirement	2-5	13
The UP CCP	2-6	14
Unit Protection Functions	2-7	17
Unit Protection within the Joint Campaign Framework	2-8	19
Unit Protection and Military Operations (static & mobile)	2-9	21
Summary	2-10	29
Chapter 3		
Required Capabilities		
Unit Protection Operations	3-1	29

Contents (continued)

	Paragraph	Page
Chapter 4		
Migration Plan		
Assessment of Current Protection Capabilities Across the Detect, Assess, Decide, Act and Recover UP Range of Functions.	4-1	42
Spiraling Current Capabilities	4-2	55
Optimum Capabilities	4-3	71
Chapter 5		
Operational Architecture		
Army Unit Protection Operations Architecture Products	5-1	84
The Army Unit Protection OV-5Activity Model	5-2	85
Chapter 6		
DOTMLPF Implications and Questions Architecture		
Doctrine	6-1	88
Organizations	6-2	88
Training	6-3	89
Materials	6-4	90
Leadership and Education	6-5	91
Personnel	6-6	93
Facilities	6-7	93
Chapter 7		
Wargaming and Experimentation Study Questions		
Introduction	7-1	94
Past and Future Experimentation	7-2	95
Study Questions	7-3	96
Chapter 8		
Alternative CCP		97
Appendices		
A. References		99
Glossary		102

Chapter 1 Introduction

1-1. Purpose

a. This pamphlet provides a plan for integrating protection capabilities and upon approval may result in a protection focused capabilities based assessment (CBA). The unit protection (UP) CBA may identify tasks, capabilities needed and gaps to provide integrated UP. The UP CBA may recommend doctrine, organizations, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) solutions and solution sets for UP capability gaps during the 2012-2024 timeframe.

b. UP is the integration of active and passive capabilities and processes, provided to operational and or tactical units, across the range of military operations (ROMO) to protect unit personnel, assets, and information against traditional, catastrophic, disruptive and irregular air, ground, chemical, biological, radiological, nuclear and high-yield explosives (CBRNE), electronic, information and intelligence threats, in order to conserve unit fighting potential so it may be applied by commanders at the decisive time and place.

c. As the Department of Defense (DOD) transforms to a modular, scalable, and tailorable force supporting full spectrum dominance, Army proponent and joint service protection capabilities must be integrated and capitalized upon to provide UP across the ROMO. Current and future adversaries will continue to employ techniques such as rockets, artillery, and mortars (RAM), cruise and ballistic missiles, rotary and fixed wing aircraft, terrorist activity, weapons of mass destruction (WMD), insurgent activity, and improvised explosive devices (IEDs). In support of UP operations, the Army must *detect, assess, decide, act, and recover* from these varied types of threats by producing technical countermeasures and tactical procedures to reduce or eliminate the number and effectiveness of these attacks. These functions will assist a commander in shaping the battlefield for tactical advantage, enabling the ability to *see first, understand first, act first, reengage at will, and finish decisively*.

d. The UP concept capability plan (CCP) is nested within approved joint transformation documents the DOD *Capstone Concept for Joint Operations*, and the DOD joint operating, functional, and integrating concepts. In addition, this plan supports Army concepts *the Army in Joint Operations, Operational and Tactical Maneuver*, and the Army functional concepts of *Command, See, Move, Strike, Protect, and Sustain*.

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of Abbreviations and Terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Functional Area

a. The UP CCP identifies capabilities required to execute protection in support of the force protection joint functional area during the 2012-2024 timeframe. Subsequently, this plan also reaches across the battlespace awareness, command and control (C2), force application, and net-centric operations joint functional areas. In addition, this plan is fully nested with the Army concept strategy documents, from the *Army in Joint Operations* through the six Army functional concepts.

b. ROMO. The ROMO addressed includes stability operations (SO) through major combat operations (MCOs) at the strategic, operational, and tactical levels of war, during concurrent and overlapping operations, in both static and mobile environments. The timeframe under consideration ranges from 2012-2024.

1-5. Scope

a. This CCP focuses on protection functions and the integration of desired capabilities to preserve the operational and tactical freedom of movement. Currently these functions and capabilities are not inherent in all units. The application of the indicated protection capabilities inherently have impressive and far reaching affects on strategic operations. The UP CCP supports the attainment of joint dominance across the full spectrum operations, and considers current, projected, and desired Army protection capabilities in support of joint, interagency, and multi-national (JIM) operations.

b. This CCP may support analysis, which should produce recommendations to change specific requirements to improve protection with organic and non-organic Army unit capabilities. Unit as defined in this plan is not size or function specific; rather, unit indicates a military group organized for offensive, defensive, or stability operations. This CCP does not examine UP capabilities in support of Civil Support operations.

1-6. Relation to the Family of Joint and Army Concepts

a. The Capstone Concept for Joint Operations (CCJO). The CCJO addresses three fundamental actions for employment by the joint force (JF) in any campaign, acquire knowledge, extend reach, and create effects. The UP CCP supports the acquire knowledge action by providing a protection detect, assess, and decide capability spanning the various threat domains of air, ground, CBRNE, information, electronic, and intelligence. The UP plan will provide a protection sanctuary for forces extending the reach of the JF. Finally, the application of an integrated protection capability will create numerous beneficial friendly effects on the battlefield. The UP CCP supports the CCJO key characteristics of *being knowledge empowered, networked, interoperable, expeditionary, adaptable, tailorable, enduring, precise, fast, resilient, agile, and lethal*. The CCJO address the future threat environment and focuses on solutions for adversary adaptive abilities, and the mature and emerging challenges of catastrophic, irregular, disruptive, and traditional threats. The UP CCP seeks to resolve protection gaps to provide a 360° hemispherical protection capability against these varied threats.

b. Joint Operating Concepts (JOC)

(1) *Homeland Security JOC*. The UP CCP addresses the ROMO and the different levels of war. UP may be applied to homeland security construct of detect, deter, prevent, and defeat attacks against the homeland. UP may be provided to forces in support of homeland defense operations, as this plan addresses offensive and defensive protection operations, applicable to forces in the forward, approaches, and homeland regions. UP will support the homeland defense operational domains of air and space, land, and cyber defense. Maturation of this CCP within a joint context may also prove effective in the maritime domain.

(2) *MCOs JOC*. The central theme of the MCO JOC is to achieve decisive conclusions to combat and set the conditions for decisive conclusion of the confrontation. The UP CCP will assist the force in achieving this goal through the provision of integrated protection capabilities and functions. These capabilities conserve unit fighting potential, so it may be applied by commanders at the decisive time and place. Lastly, UP will support the MCO foundation of using a coherent joint force that decides and acts based upon pervasive knowledge, and the execution principles of achieve decisive outcomes and conclusions, employ a knowledge-enhanced effects-based approach, gain and maintain operational access, engage the adversary comprehensively, generate relentless pressure by deciding and acting distributively, achieve coherency of action, and protect people, facilities and equipment throughout the operational environment.

(3) *Stability Operations JOC*. The SO JOC states the JF must be prepared to conduct counterinsurgency operations, unconventional warfare, and counterterrorist activities, as well as limited conventional operations in order to impose a level of security that can eventually be enforced by civilian police forces. The UP functions aid the commander by increasing security and decreasing recovery time and actions, which will in turn facilitate improved freedom of maneuver. Further explanation of UP in support of SO may be referenced in chapter 2.

c. Joint Functional Concepts

(1) *Battlespace Awareness*.¹ The UP CCP addresses five critical functions in support of protection operations. Three of the five (detect, assess, and decide) support the attainment of battlespace awareness during the full spectrum of operations. The UP CCP incorporates the aspects of battlespace awareness, particularly the need for persistent and pervasive sensing, persistent surveillance, actionable intelligence, aided target recognition (ATR), interrogation, precise identification, and faster, better decisionmaking. Battlespace awareness in 2015 provides *actionable intelligence* to commanders and warfighters and provides commanders and force elements with the ability to make better decisions faster by enabling a more thorough understanding of the environment in which they operate.

(2) *Command and Control*. The UP CCP recognizes the importance of command and control in a combat environment for the conduct of Army operations in support of joint operations. Command and control is the ability to recognize what needs to be done in a situation

¹ Except in this paragraph and when referring to the actual joint functional concept, "battlespace" has been replaced with "operational environment."

and to ensure that effective actions are taken. In 2015, U.S. commanders will habitually be operating in a joint and multilateral environment as part of joint and/or combined operations. The ability for all these players to collaborate with one another will be instrumental in the success or failure of these operations. A main focus of the UP CCP is to enable integrated/interoperable protection capabilities, which share common C2 in support of UP functions.

(3) *Force Application.* In its simplest form, force application can be described as the maneuver and engagement of combat forces to generate the effects desired on the enemy. The UP CCP supports the force application joint functional concept through the application of detect, assess, decide, act, and recover UP functions, which conserve unit fighting potential so it may be applied by commanders at the decisive time and place. Forces must possess combinations of stealth, speed, information superiority, connectivity, protection, and lethality to enable maneuver. The UP act function will include lethal and nonlethal and kinetic and non-kinetic actions, in support of proactive, defensive, and warning (enemy/friendly) protection operations.

(4) *Net-Centric Environment.* The UP CCP incorporates net-centricity as an underlying, fundamental aspect of future UP operations. The networking of all joint force elements creates capabilities for unparalleled information sharing and collaboration [and] a greater unity of effort via synchronization and integration of force elements at the lowest levels. Net-centricity provides the capability to exploit all human and technical elements of the JF and its mission partners by fully integrating collected information, awareness, knowledge, experience, and decisionmaking, enabled by secure access and distribution, to achieve a high level of agility and effectiveness in a dispersed, decentralized, dynamic, and possibly uncertain operational environment. It also provides a foundation across the full spectrum of joint operations for providing the ability to electronically share sensor data among multiple sensors in order to increase capability over that provided by any single sensor. UP will harness net-centricity via integrated detection and assessment capabilities against various threat domains.

(5) *Protection.* The focus of the UP CCP includes those activities necessary to provide successful protection as identified in the *protection* joint functional concept. The UP CCP supports the concept that protection is composed of a variety of active and passive measures (for example, weapons, pre-emption, and warning) in the air, land, sea, and space domains. Protection must be proactive, focused, and conducted by integrating military and cross government capabilities against our adversaries. The JF will achieve this through the scaled and tailored selection and application of multi-layered, active and passive, lethal and nonlethal measures, within the air, land, sea, and space, across the ROMO, based on assessment of an acceptable level of risk. The goal is to prevent adversaries from employing capabilities that would restrict or prevent the JF from conducting decisive actions at a time and place of our choosing. The Army UP functions of *detect*, *assess*, *decide*, *act*, and *recover* support the ideas applied in protection.

d. Joint Integrating Concepts (JIC)

(1) *Global Strike JIC.* Global strike is defined as responsive joint operations that strike enemy high-payoff targets as an integral part of joint force operations conducted to gain and maintain operational environment access, achieve other desired effects, and set conditions for

follow-on decisive operations to achieve strategic and operational objectives. UP will support global strike operations by providing 360° hemispherical protection to forces executing global strike operations, and will be effective from fort to port to forward staging areas. In addition, the UP *act* capability will caveat global strike operations via the application of proactive (*act*) protection capabilities.

(2) *Integrated Air and Missile Defense (AMD) JIC*. The UP CCP supports the integrated AMD JIC's position for the integration of joint AMD capabilities. Integrated Army and joint AMD capabilities are required for providing 360° hemispherical protection capabilities. These AMD capabilities must not only be integrated, but in order to obtain a 360° hemispherical protection capability, these capabilities will require integration with ground, CBRNE, electronic, information and intelligence protection capabilities.

(3) *Seabasing JIC*. The UP CCP is tied to the *Seabasing JIC* by supporting, supplementing, or replacing integrated sea-base force protection capabilities and systems. UP capabilities may be utilized during the different phases of seabasing operations, enroute to a seabase, on the seabase, and offshore return to the seabase. In addition, UP capabilities may support seabase logistic operations from seaborne staging to re-supply objective and return. Maturation of this plan may include the integration of Army UP and joint seabasing force protection capabilities.

(4) *Command and Control JIC*. The UP CCP supports the C2 JIC through the application of detect, assess, and decide functions and will provide UP capabilities in support of a commander's unity of command and effort. In addition, this plan supports the C2 JIC *principle of the offensive*; the purpose of an offensive action is to seize, retain, and exploit the initiative. This plan describe 360° hemispherical protection operations and required capabilities that will transition protection operations from mere defensive operations and provide a venue to execute specific protection capabilities in a offensive mission set.

e. The Army Family of future Modular Force Concepts

(1) *The Army in Joint Operations, The Army's Future Force Capstone Concept 2015-2024*. The UP CCP supports the seven key operational ideas presented in TRADOC Pam 525-3-0. These are *shaping and entry operations, operational maneuver from strategic distances, intratheater operational maneuver, decisive maneuver, concurrent and subsequent SO, distributed support and sustainment, and networked-enabled battle command*. In addition, this CCP supports the current and emerging threat challenges of traditional, irregular, catastrophic, and irregular threats posed to the Army in support of joint operations. As this concept supports the joint concept family, it subsequently supports the Army in joint operations; the application of the UP functions will be viable to the Army in such operations and maturation of this plan may compel a necessary adaptation of 360° hemispherical protection capabilities compatible within a JIM framework.

(2) *The U.S. Army Operating Concept for Operational Maneuver*. The UP CCP supports the *Operational Maneuver* concept by protecting large landpower forces tailored and employed, for major combat and other operations during the 2015-2024 timeframe. Integrated UP

capabilities will support the commander in achieving the defeat mechanisms indicated in the concept for operational maneuver; destruction, dislocation, and disintegration, and the seven key operational ideas. The protection of forces throughout the execution of these mechanisms is vital to decisive operations.

(3) *The U.S. Army Operating Concept for Tactical Maneuver*. The UP CCP will support a commander's ability to execute precision maneuver, the dynamic combination of movement, effects, and information. The UP functions provide a commander an enhanced ability to *see first, understand first, act first, reengage at will, and finish decisively*. The combination of the UP functions will provide a proactive protection capability. This capability will enable a commander in the *commitment of fighting forces* to time critical tactical operations while they are provided battlefield freedom of movement, via a 360° hemispherical protection capability.

(4) *U.S. Army Functional Concept for Battle Command 2015-2024*. The UP CCP is tied to the *Battle Command* concept via the *detect, assess, and decide* functions of UP. These functions provide commanders situational awareness (SA) and situational understanding (SU); *decision superiority*, and aid knowledge of self, environment, and the enemy. The integrated abilities to detect, assess, and decide in support of protection from air, ground, CBRNE, information, electronic, and intelligence threats increase a commander's probability to develop an effective course of action (COA) and finish decisively.

(5) *U.S. Army Functional Concept for See 2015-2024*. Naturally, the ability to finish decisively requires knowledge superiority. The UP CCP proposes an integration of knowledge capabilities via sensors which provide a unit a comprehensive verbal, visual, and aural exchange of battlefield information regarding friendly and adversary air, ground, CBRNE, information, electronic, and intelligence threats, capabilities, and positions. UP knowledge data must enable real or near real-time, compartmentalized delivery and the transfer of relevant operational environment data between echelons to support COA development against threat activities. This data will enable predictive analysis and knowledge discrimination and must not overwhelm the user.

(6) *U.S. Army Functional Concept for Move 2015-2024*. The UP CCP will enable the *Move* concept effects by aiding the provisions of increased capability to achieve assured access (via the protection of critical assets), reduced vulnerability to enemy counters (via a 360° hemispherical protection capability), higher levels of active and passive force protection (via the UP act function), rapid seizure of the initiative and increased capability to conduct and sustain simultaneous operations distributed within a non-linear operational environment (via a 360° hemispherical protection capability), present a multidimensional threat to the enemy (via nonlethal to increasingly lethal enemy warning and proactive lethal and nonlethal protection), rapid transition to decisive operations and maintain tempo (via a 360° hemispherical protection capability), and rapid decision in tactical actions and engagements (via UP detect, assess, and decide).

(7) *U.S. Army Functional Concept for Strike 2015-2024*. The UP CCP supports the *Strike* concept via the function of *act*. The UP act function will provide nonlethal to increasingly lethal enemy warning and proactive lethal and nonlethal protection which may include specific

strike capabilities and actions. In addition, UP act will support strike key ideas of execute seamless deployment of lethal and nonlethal effects and synchronize and exploit joint interdependencies.

(8) *U.S. Army Functional Concept for Protect 2015-2024*. The capabilities required for the execution of UP will enable the execution of desired affects as indicated in the *Protect* concept and specifically expands upon the ideas of unit protection presented in this concept.

(9) *U.S. Army Functional Concept for Sustain 2015-2024*. This plan for protection will provide the necessary sanctuary for sustainment operations and may serve as a baseline for improved base, critical asset, and convoy protection, and other reconstitution operations which will require both static and mobile protection capabilities.

1-7. Operational Outcome

a. In accordance with the National Military Strategy, the national military objectives are to protect the U.S., prevent conflict and surprise attack, and prevail against adversaries. The operational outcome of UP is full spectrum dominance. The functions of UP will provide the Army and hence, the joint warfighter with the capabilities needed to provide 360° hemispherical protection against air, ground, CBRNE, information, electronic, and intelligence threats.

b. The UP functions applied to Army and JIM forces will exercise proactive protection capabilities, and enable the freedom of time critical movement throughout the battlefield and ROMO.

1-8. Complementing the Joint Warfighting Force

a. This CCP complements Army and the JF by providing freedom of maneuver through the execution of detect, assess, decide, act, and recover. Protection extends from the homeland as the base for force projection operations, through friendly nations and coalition partners in a region (during forcible entry or sea base operations), and within the area of operations (AO). It is established in the initial stages of deterrence and continues through the achievement of full spectrum dominance to completion of redeployment.

b. UP spans the spectrum of military operations from SO and smaller scale contingencies to MCOs.

Chapter 2 Unit Protection Plan

2-1. Basis of Unit Protection

a. In support of UP operations, the Army must *detect, assess, decide, act, and recover* from varied types of threats by producing technical countermeasures and tactical procedures to reduce

or eliminate the number and effectiveness of these attacks. These functions will assist a commander in shaping the battlefield for tactical advantage, enabling the ability to *see first, understand first, act first, reengage at will, and finish decisively*. UP will support Army, and consequently JIM operations, by providing an integrated protection sanctuary that will enable freedom of movement and decisive operations.

b. UP objectives may be accomplished via the spiraling of advanced integrated protection solutions to the force in order to create an objective, mobile, 360° hemispherical protection capability. This capability will require the integration of UP functions and capabilities to see and understand the battlefield (friendly forces, the adversary, and the environment), to develop COAs to act swiftly, (friendly warning and nonlethal to increasingly lethal enemy warning, and proactive lethal and nonlethal protection), to recover UP systems and capabilities, enabling the return to UP operations and to provide sanctuary for other relevant combat recover operations.

2-2. The Problem

a. Protecting U.S. military forces has never been as complex a mission as it is in today's adversarial environment. This environment will likely worsen and adversaries will remain adaptive. The U.S. Army has numerous protection capabilities that are not integrated. The exposure of the widely distributed facilities of the joint support structure to attack by unconventional forces, long-range fires, aviation, and the remnants of enemy forces will present additional opportunities for ground defense. Corps, division, and brigade combat teams (BCT) will be required to dedicate subordinate forces to defend critical support facilities and vital support operations, such as sustainment convoys. This security requirement will demand new solutions that integrate air, electronic, and ground defenses of both stationary and moving infrastructure within the operational environment. Failure to integrate protection capabilities and provide modular and adaptive solutions to protection will be detrimental to forces operating in a JIM environment. Protection capabilities must be integrated in order to provide 360° hemispherical UP; a modular, multi-layered, integrated, full dimensional protection Family of Systems (FoS) and System of Systems (SoS) capability against air, ground, CBRNE, information, electronic, and intelligence threats. These capabilities allow friendly forces to counter the full range of hostile threats our adversaries possess and are plausible to possess.

b. Events leading to and culminating from the 9/11 attack on the U.S. homeland increased the government's awareness of enemy capabilities, and also educated adversaries of neglected areas within our military and government structures, providing seams to exploit for their operational and strategic advantage. The future Army in joint operations must possess UP capabilities to protect personnel, assets, and information critical to strategic, operational, and tactical level mission success. UP capabilities must be additive, modular, and tailorable, adopting FoS and SoS approaches while possessing integrated architectures. UP capabilities must be effective in both static and mobile environments, and provide the ability to protect the force during maneuver operations.

2-3. Joint Operational Environment

a. Protection is a process, set of activities, or utilization of capabilities by which the JF protects personnel (combatant/noncombatant), physical assets, and information of the U.S., allies, and friends, required to ensure fighting potential can be applied at the decisive time and place against the full spectrum of threats. The JF will achieve this through the tailored selection and application of multi-layered, active and passive, lethal and nonlethal, offensive and defensive measures, within air, land, sea, space, and cyberspace domains, across the ROMO, based on assessment of an acceptable level of risk. Evolving threats will take on new, more challenging characteristics in the 21st century. Adversaries will closely observe emerging U.S. capabilities in an effort to identify and exploit weaknesses using asymmetric approaches. An asymmetric approach uses simple counters to negate U.S. capabilities and avoids a direct match with U.S. strengths.

b. Fundamental capabilities that 21st century adversaries may pursue to counter U.S. strengths include WMD delivered by tactical ballistic missiles; reconnaissance, surveillance, and target acquisition via unmanned aircraft systems (UAS); precision strike technology; large caliber rockets; cruise missiles; and electronic and information warfare. The adversary may also use asymmetrical means such as electromagnetic pulse (EMP), particle beam weapons, high power microwave and laser directed energy weapons to disrupt, deny, or destroy mission critical electronic based assets. Advances to adversary technology may increase use of infrared, electro-optical, and radio frequency guided missiles.

c. Some countries or non-state entities will rely on asymmetric capabilities as a substitute for, or complement to, large conventional forces. The use of RAM to attack bases and IEDs to disrupt lines of communication (LOCs) illustrate this fact. Regional competition will reinforce the perceived need to acquire unmanned systems that provide high operational effectiveness at a nominal cost, as a substitute for manned vehicles, air, or ground. The following types of threats should be expected in any future conflict-

- Air assault and attack helicopters will target logistics LOCs.
- Precision munitions will strike friendly critical assets.
- Medium-range ballistic and cruise missiles will strike staging areas and critical choke points.
- Special forces, terrorist, and paramilitary attacks will create tangible damage through the use of mines, IEDs, and RAM while diverting disproportionate numbers of U.S. forces to protect facilities, personnel, and coalition partners.

d. In addition, adversaries will attempt to deny the inherent protective characteristics of “sanctuary” areas to U.S. forces by employing low- and high-tech means. Enemies will conduct a wide variety of tactical actions to confuse and defeat U.S. forces while avoiding decisive overmatch in a symmetrical, conventional fight. The enemy will-

- Seek to increase uncertainty and expand opportunity for surprise.
- Use continuous, non-decisive engagements that will reduce exposure and complicate U.S. targeting; loss of contact with the adversary will have greater consequences than in more

open surroundings against more predictable echeloned enemy forces.

- Threaten and interdict lines of operations and communications on a continuous basis.
- Take maximum advantage of available state-of-the-art technology weapons, for example, beyond line-of-sight (BLOS).
- Reduce engagement ranges of weapon and acquisition systems, degrading U.S. advantages in standoff engagement, through techniques such as camouflage and deception, “hugging” U.S. forces and civilian populations, and technical countermeasures.

2-4. The Future Operational Environment

a. Analysis of current and future operations suggest that adverse terrain and weather, coupled with adaptive enemies, (representing social, physical, and economic failed states, fractured societies with rampant crime and international linkages, and religious and ethnic tensions), will likely characterize future operating conditions and opponents. Future opponents will understand and leverage our existing infrastructure to their advantage and target fixed facilities and areas where we are likely to operate.

b. The emergence of unconventional and asymmetric threats, radical extremist and terrorist efforts aimed at the U.S. and other developed members of the global economy, and the burdens of post conflict operations increase the mission requirements of the U.S. military. There are now a nexus of dangerous new actors, methods, and capabilities that imperil the U.S., its interests and alliances in strategically significant ways.

2-5. The Complex Protection Requirement

a. The protection requirement throughout the ROMO is increasingly complex. The U.S. military operational environment has evolved to an all encompassing arena and includes advanced and rapidly adjustable adversary capabilities. These adversary capabilities require U.S. Army and JFs to examine unconventional and revolutionary ways to tackle an adaptive force through the integration and capitalization of current and future capabilities. U.S. forces must meet the adversary head on, by enacting solutions to developing threats. The battlefield is not just the close fight between large and small hostile forces. It is comprehensive, involving all phases of operations, using all elements of national power, from the onset of deployment notification, through ceasefire, and the rebuilding of nation states.

b. The military force operational environment is extremely fluid. Military forces must be able to rapidly and seamlessly transition between missions, and conduct different missions simultaneously with an appropriate mix of forces in depth. Army and JFs, without peer in high intensity warfare, must be able to operate across the spectrum of conflict. UP capabilities will include the ability to protect forces so that they may operate decisively despite overlapping operations driven by expanding mission requirements, from MCOs to SO, all while supporting the global war on terrorism. The changed operational environment, the future environment, and adversary capabilities are depicted in figure 2-1.

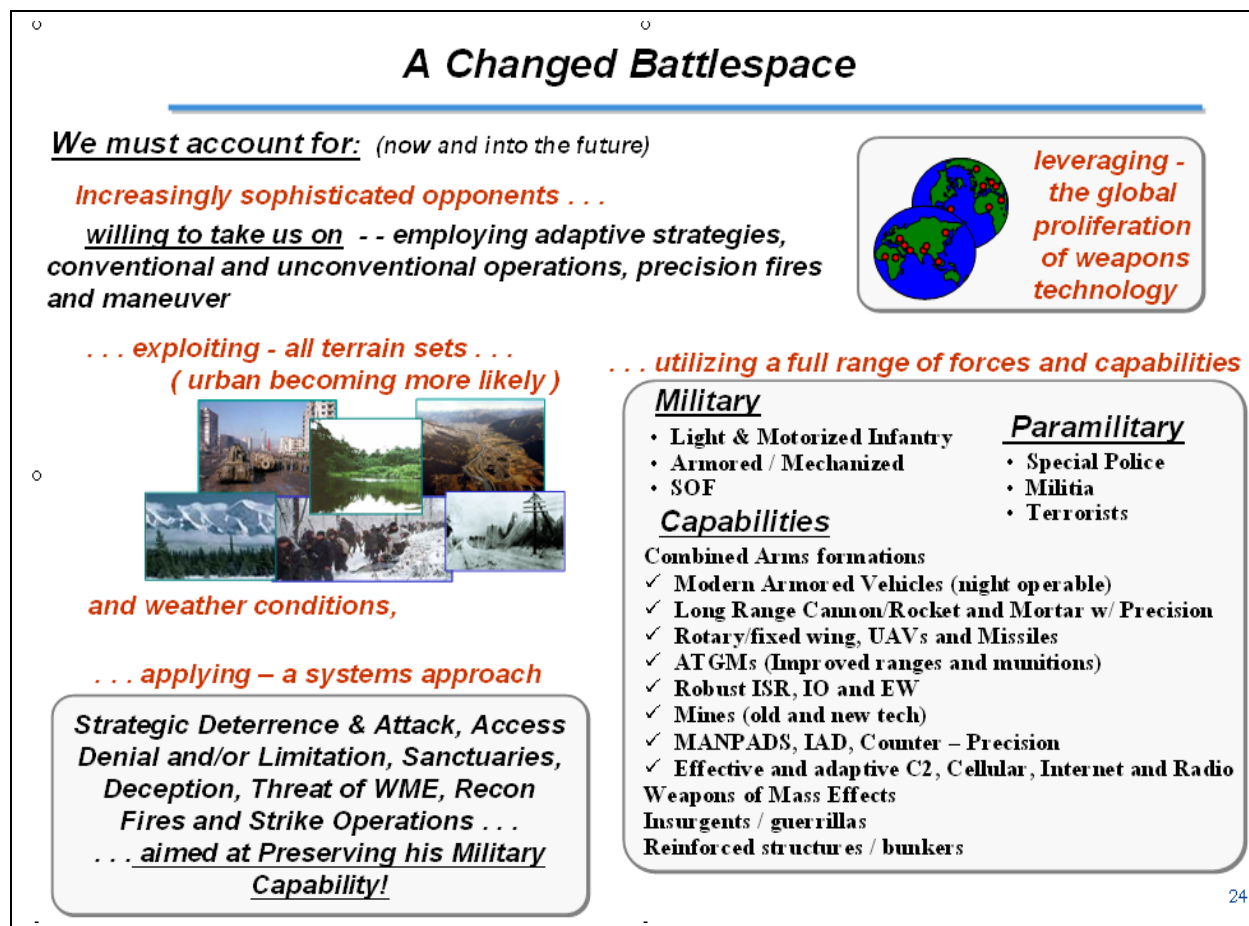


Figure 2-1. A Changed Battlespace

2-6. The UP CCP

a. Lessons learned in recent combat operations, plus DOD and Army transformation supporting the global war on terrorism demand integrated capabilities. The UP CCP is an example of these efforts. Integrating UP capabilities will eliminate duplicative technology developments, improve efficiency and military operational effectiveness, force interoperability of protection systems while lessening protection demands on Soldiers, commanders, and their staffs. This integration of UP technologies and capabilities will provide critical 360° hemispherical protection during all phases of operations. The UP CCP conceptualizes various protection capabilities (available and desired) and suggests an optimum required capability, a comprehensive UP suite of capabilities. The UP CCP conceptualizes the integration of protection capabilities from different Army corps. In summary, these corps provide the following capabilities-

(1) Air Defense Artillery Corp provides protection to the force from air and missile threat; they will see first, warn, intercept, and then when able provide the necessary positional information for friendly forces to execute attack operations.

(2) Military Police (MP) Corp provides security to our forces, either mobile or static.

(3) Chemical Corp provides capabilities of detect, protect, and recover from enemy chemical, biological, radiological, nuclear (CBRN) attacks.

(4) Engineer Corp provides the capabilities of survivability, mobility, and countermobility to the force.

(5) Military intelligence (MI) Corp provides the expertise in intelligence, surveillance, and reconnaissance (ISR) and counterintelligence requirements and capabilities.

(6) Signal Corp provides the ability to distribute and protect vital information to the force, increasing SA and SU and improving battle management, C2 communications, computers, and intelligence operations.

(7) Aviation Corp provides ISR and security which helps protect the force against surprise attack and observation by hostile air and ground forces. Aviation capabilities aid freedom of maneuver for the command by providing reaction time and maneuver space.

(8) Field Artillery Corp provides the capability to execute detection, impact point prediction, fires and counterfires to the force.

(9) Ordnance Corp provides the capability to recover from high yield explosives through emergency ordnance disposal units.

b. An objective UP capability applied through Army echelons to the JF is depicted in figure 2-2. These capabilities offer a wealth of active resources against a thinking and adaptive force. The improved protection sanctuary gained via the integration of capabilities and DOTMLPF processes provides a proactive, and when necessary, lethal UP capability.

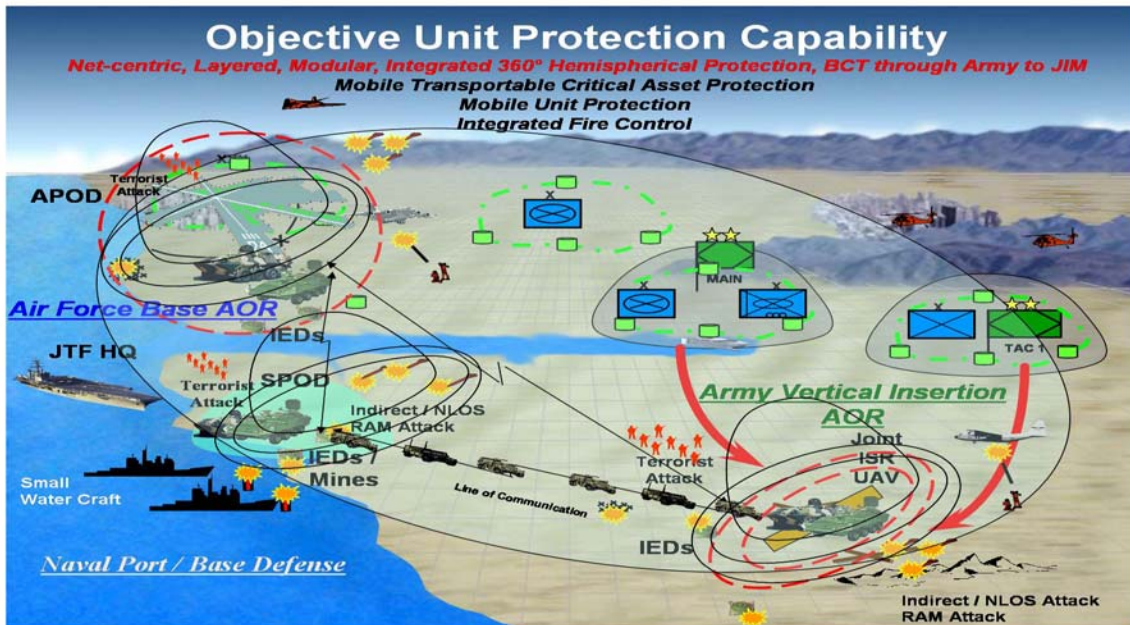


Figure 2-2. The Unit Protection Capability

c. The evolution of the UP CCP and portrays the independent protection capabilities of integrated AMD, early warning, mobility, fires, mobile strike, persistent ISR, counterintelligence, civil affairs, JC2, Army battle command system (ABCS), IED defeat, counter RAM, security, detainment, impact point prediction, SA, SU, and CBRNE protection combined in an integrated UP capability to provide 360° degree hemispherical protection and then, an objective, joint integrated UP capability is depicted in figure 2-3. This list of capabilities is not all inclusive, but is used to illustrate the numerous protection related capabilities available, some of which may be integrated via conclusive analysis to provide an improved protection capability during the 2012-2024 timeframe.

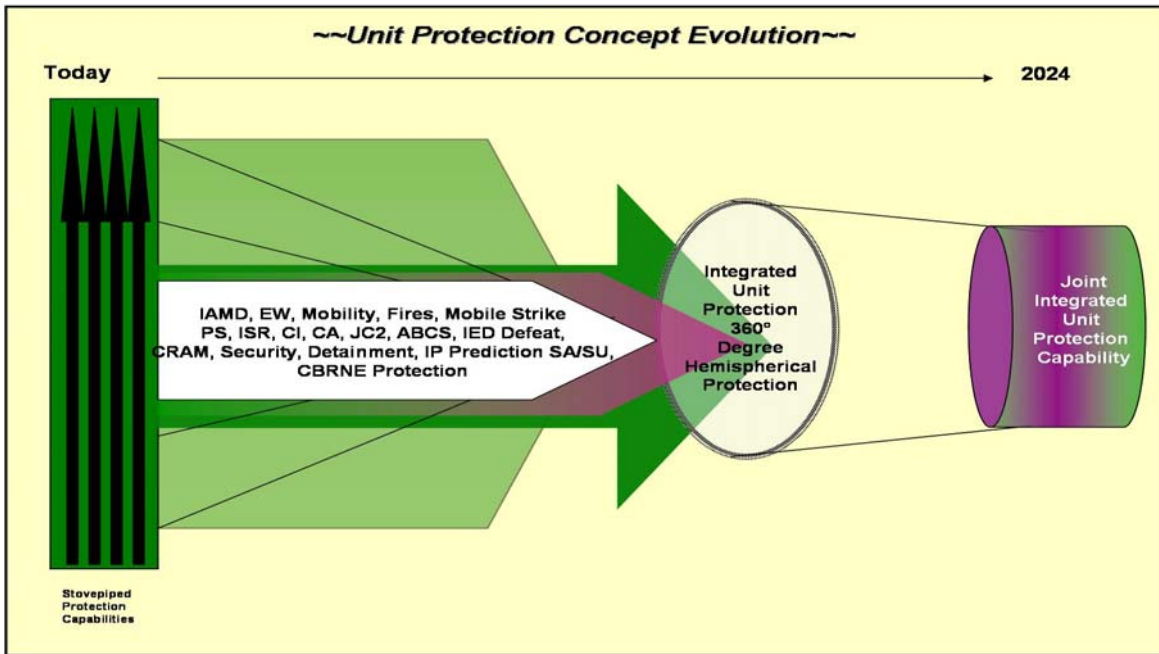


Figure 2-3. Objective Joint Unit Protection Capability

2-7. Unit Protection Functions

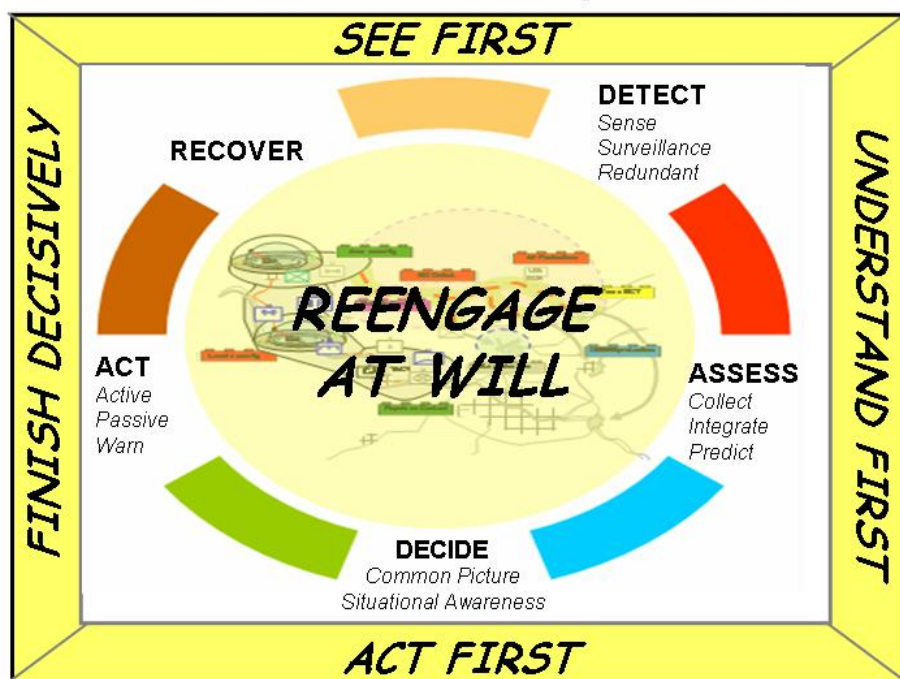
a. Successful UP across the ROMO relies upon the ability to execute functions to *detect*, *assess*, *decide*, *act*, and *recover* from various types of threats (see fig 2-4).

(1) *Detect*. Detect includes a unit's ability to sense the full range of friendly and hostile air, ground, CBRNE, electronic, and intelligence activities to provide real-time SA enabling 360° hemispherical UP. Integrating sensors and sensor technology, databases, intelligence collection, physical security and communications systems is essential to accurate and timely threat detection. In order to detect, military forces must collect timely, unambiguous, and accurate data on adversary capabilities and actions planned or employed against friendly personnel, assets, or information.

(2) *Assess*. Assess includes the ability to recognize, classify, and identify data and information upon detection to correctly formulate procedures and drive COA, enabling the ability to decide. UP assess will include the ability to share friendly and adversary information relevant to the protection environment in order to facilitate SU. SU is achieved when a decisionmaker or other human-in-the-loop analyzes the SA and is able to use that information to appreciate and comprehend the state of the battlefield and future adversarial COA, branches, and sequels. It is the product of applying analysis and judgment to the common operational picture (COP) to determine the relationships among the factors of mission, enemy, terrain, troops, time, and civil considerations. The objective is to enter an opponent's decision cycle, decipher their

plans, warn friendly units, and develop friendly COAs enabling friendly forces to deny adversary plans.

360° Hemispherical Unit Protection Functions and the Quality of Firsts



Protect personnel, assets, and information across the ROMO

Figure 2-4. UP Functions, a Holistic Framework

(3) *Decide*. Decide is the ability to reach an appropriate judgment after planning and analyzing the COA. The decide function also includes the ability to task, monitor, and change an action after a decision has been made. These capabilities are enabled by an integrated C2 capability as part of the ABCS.

(4) *Act*. Act includes the capability to execute the sub-functions of active and passive measures to protect the force. These actions can be proactive or reactive, and include the ability to execute warning.

(a) *Warning*. Warning includes the reaction to actionable intelligence by disseminating warnings or predictions in a timely, accurate, and unambiguous manner. Specifically, warn includes the acknowledgement and communication of hazards implicit in a wide spectrum of hostile and friendly activities. The UP warn capability includes the ability to execute friendly warn and enemy warn operations.

- Friendly warn. Friendly warn operations include digital and aural (system and verbal) warning to enable the affected body and location to take protective measures prior to the impact of a specific adversary action.
- Enemy warn. Enemy warning may be executed through specific nonlethal capabilities that interrogate, challenge, and warn an enemy that further action (hostile or presumed hostile) will result in increasingly lethal U.S. counteraction.
 - o These enemy warnings will be effective against air, ground, CBRNE, electronic, and intelligence threat capabilities.
 - o Enemy warning includes the capability to deter, interrupt and cease enemy action.

(b) Active and Passive protection Measures. The application of active and passive measures resists adversary plans and actions directed against friendly personnel, assets, and information. The utilization of the act function and its related protection capabilities enable a commander to preserve operational capabilities via the improved protection of personnel, assets, and information.

- Active Measures. Active measures include the ability to deter, prevent, and deny adversary plans and actions, to include offensive actions.
- These offensive actions may take the form of preemptive and direct attack against enemy C2 nodes, assembly areas, weapon caches, AMD, and computer network attack (CNA).
- Passive measures. Passive measures and reactive protection include the ability to deter, prevent, and deny adversary plans and actions from using a capability the enemy would otherwise employ against the JF.
- These measures provide the capability to defend against adversary actions once those actions are executed or when friendly forces are confident the adversary will imminently use adverse actions.
- These measures may include specific types of camouflage; cover for supplies and personnel during a NBC attack or the utilization of bunkers during RAM attack.

(5) *Recover*. The UP function of recover includes actions taken during or after an event to restore in a minimum amount of time all UP capabilities that protect personnel, assets, and information. The recover function is specific to UP capabilities and includes, but is not limited to the execution of battle damage assessment, battle damage repair and reconstitution operations vital to restore UP functions and capabilities. The successful execution of the recover function is vital to a commander's operation; the application of UP recover facilitates the supported unit's ability to continue offense, defensive, and SO and execute internal recovery operations.

2-8. Unit Protection within the Joint Campaign Framework

a. The JF will conduct a phased campaign to achieve assigned objectives. UP will provide a 360° hemispherical protection capability to people, assets, and information; providing a multi-layered and overlapping sanctuary, adequately protecting in conventional, irregular, catastrophic, and disruptive threat environments. Protection will take place on land, in the air, on the seas, in space, and the electronic and virtual domains, and is applicable globally and across the ROMO.

Protect operations will have specific implications for planning and executing activities within the joint campaign.

b. UP functions span the breadth of all Army key operational ideas for joint operations as described in the Army capstone concept. They include operational maneuver from strategic distances, shaping and entry operations, intratheater operational maneuver, decisive maneuver, subsequent and concurrent SO, distributed support and sustainment, and networked-enabled battle command. The UP level of effort, within a joint campaign, may vary depending on type of operation being conducted or the occurrence of actual events.

(1) *Operational Maneuver from Strategic Distances.* Future Modular Force commanders and their staffs will begin planning for protection operations within the overall concept of operations. Protection includes the capability to provide a level of deterrence and prevent hostile acts against the U.S. and its allies.

(2) *Shaping and Entry Operations.* The future Modular Force will conduct entry and shaping operations, to impede achievement of initial enemy objectives; a proactive means of unit protection. In entry operations the inclusion of modular protect capabilities will enhance survivability by reinforcing organic capabilities, especially where friendly host nation's assets are not available or when the entry point is under an adversary's control.

(3) *Intratheater Operational Maneuver.* Movement by ground, sea, and air will extend the reach of the joint force commander (JFC), expand capabilities to exploit opportunities, and generate dislocating and disintegrating effects. This will require joint interdependent protect capabilities in the domains of ground, sea, and air. Movement is also supported by strike capabilities and joint fires as proactive protection means.

(4) *Decisive Maneuver.* Decisive maneuver requires simultaneous and distributed operations with continuous action, and a controlled operational tempo leading to direct attack of key enemy capabilities and centers of gravity. These actions serve to achieving the initiative. The future Modular Force will require mobile protection systems capabilities operational on a continuous basis, in all environments allowing for freedom of movement.

(5) *Subsequent and Concurrent Stability Operations.* Lessons learned support that MCO often lead to SO. Operational UP will be required to ensure the success of SO via the provisions of protect capabilities for the future Modular Force, civil populations and assets, and applicable host nation and allied military forces.

(6) *Distributed Support and Sustainment.* This will maintain freedom of action and provide continuous sustainment of committed forces in all phases of operations, throughout the operational environment, and with the smallest feasible deployed logistical footprint. UP will provide the necessary sanctuary for logistics operations and may serve as a baseline for improved base and critical asset and convoy protection, and other reconstitution operations which will require both static and mobile protection capabilities.

(7) *Network-Enabled Battle Command.* Network-enabled battle command will facilitate required SU, self-synchronization, and effective application of joint and Army protect

capabilities during operations. Net-centricity provides the capability to exploit all human and technical elements of the JF and its mission partners by fully integrating collected information, awareness, knowledge, experience, and decisionmaking, enabled by secure access and distribution, to achieve a high level of agility and effectiveness in a dispersed, decentralized, dynamic, and uncertain operational environment. UP will harness net-centricity via integrated detection and assessment capabilities against various threat challenges.

2-9. Unit Protection and Military Operations

a. UP will be applied across the battlefield and throughout the ROMO; from offensive to defensive and during SO, in both static and mobile environments.

b. UP applied in a static environment. Locations that require protection may remain static. Static environments include temporary and permanent areas occupied by forces for the purpose of conducting offensive, defensive, and SO. These areas include, but are not limited to, domestic and foreign U.S. military bases, sea ports of debarkation/embarkation, aerial ports of debarkation/embarkation, mission staging areas, tactical assembly areas, forward operating bases, forward area refueling points, distribution nodes, specific host nation infrastructure locales and geo-political assets. The protection of these static environments requires the integrated ability to detect against air, ground, CBRNE, information, electronic, and intelligence threats. This detection will require the stand-off distance ability to rapidly assess threats and adequately warn personnel.

c. Furthermore, UP applied in a static environment will require the integrated ability to act through the employment of active, passive, lethal, nonlethal, directed energy and kinetic energy measures, thereby defeating adversary actions directed at friendly forces. The combined functions of UP will provide a commander the ability to execute an integrated suite of protection options which they can tailor and operationally maximize, resulting in the conservation of their unit fighting potential for its application at the decisive time and place (see fig 2-5).

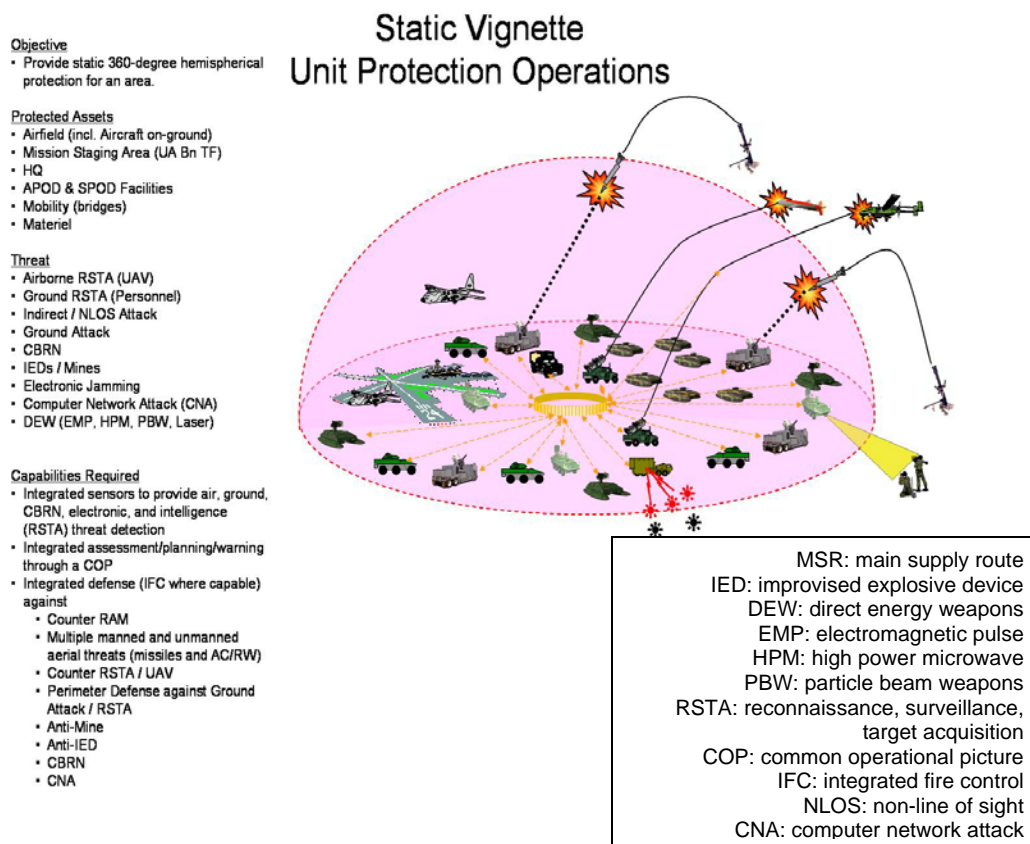


Figure 2-5. UP Operations in a Static Environment

d. Static Vignette

(1) The division conducts early entry operation into a permissive lodgment to facilitate future cross boundary combat operations. The division commander assigned the combat support brigade (CSB) the mission to protect the lodgment insuring critical personnel, assets, and information are available to support to the division commander’s shaping operations and future BCT operations. The CSB commander is also tasked to provide protection capabilities to the BCTs to support their movements into their AO (see fig 2-6).

(2) The CSB commander’s ability to perform the mission with assigned units is severely constrained during the early flow into the theater. The commander will support the BCT with the majority of available tactical units. The ground defensive, security, and other protection missions will be performed with tailored protection capabilities using light weight, modular, and integrated protective systems. This system of protection systems is composed of various protection materials, intelligent munitions, smart sensors, and communication devices that can implement obstacle intent or attack enemy threats autonomously, initiate combat reports, respond to remote commands, and mitigate the effects of enemy actions.

(3) Using allocated space and airborne reconnaissance assets in conjunction with UP capabilities the CSB BCT enhances early entry force protection and survivability. The tailored protection capabilities enable organic and attached forces to perform protection missions at division designated facilities by building zones, or rings, in depth of systems of protection systems linked and integrated into intelligent protection packages.

(4) Some capabilities are utilized along the lodgment boundary, via the emplacement of long-range sensor and assess systems supported by UAS. On designated routes into the lodgment, robotic access control point equipped with detect and assess capabilities are established at stand-off distance, focusing on friendly and hostile air, ground, CBRNE, information, electronic, and intelligence activities. All protection capabilities are integrated into ABCS, providing the CSB and supported units the ability in real-time to act in the lodgment with remote controlled intelligent effects systems, such as ISR robotic capabilities and real-time video display and integrated shooter system in support of protection operations. Joint command and control (JC2) provides the linkages between sensor systems and response systems to insure a rapid response during all phases of the entry operation.

(5) The CSB Staff also coordinates unit air protection requirements with Army and joint fires, intelligence, and air protection with the appropriate division staff points of contact.

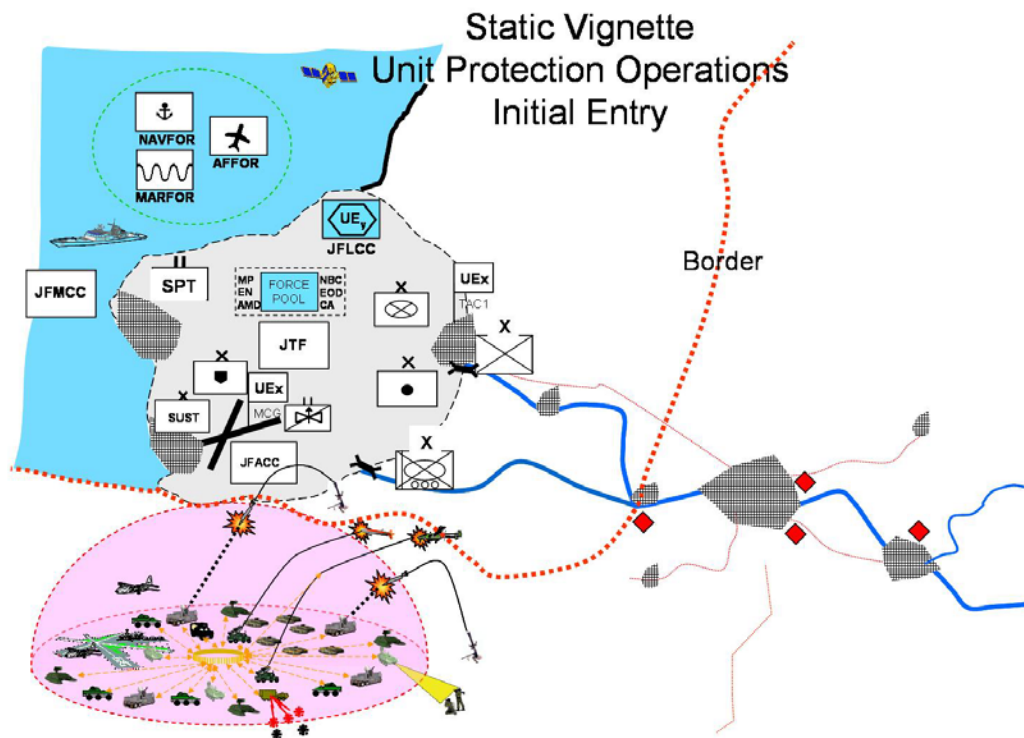


Figure 2-6. UP Operations in a Static Environment

e. UP Applied in a Mobile Environment

(1) Integrated protection will apply to forces executing operations that involve mobility, whether from strategic distance, during entry operations, intratheater, or decisive maneuver. This integrated capability includes the protection of movement(s) from home station to a departure airfield or port to en-route movement through to the arrival into the Joint operational area. Mobile UP will take place in both domestic and foreign locales and require coordination and cooperation with civil authorities and the execution of joint interdependencies.

(2) Once operations commence; offense, defense, or SO, mobility will inherently enhance UP through the application of movement and uncertainty of location. The protection of mobile formations and forces will require the same application of integrated static UP capabilities, and will protect the commander's freedom of maneuver and combat power, ensuring the full application of effects at the decisive time and place (see fig 2-7).

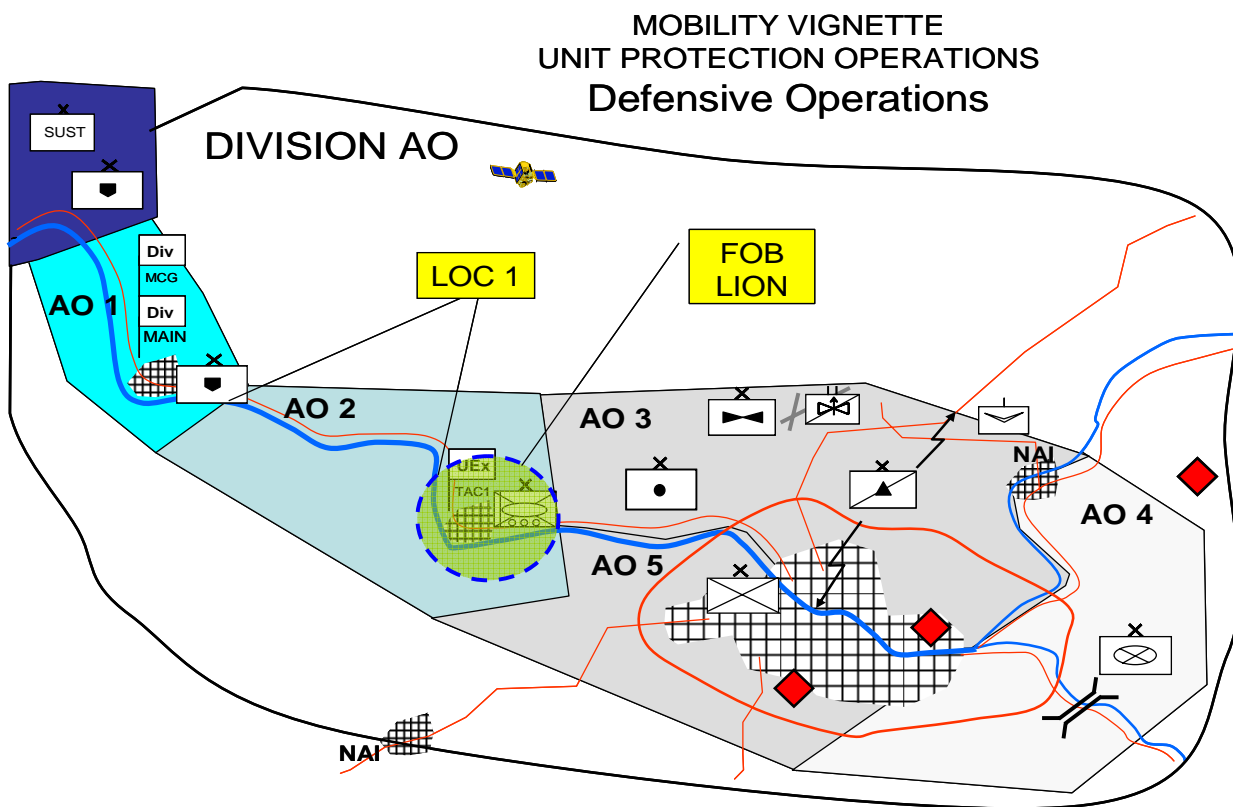


Figure 2-7. UP Operations in a Mobile Environment

f. Mobile Vignette

(1) Division has directed the establishment of a forward operating base to facilitate future combat operations. The CSB is assigned the mission to protect LOC 1 and forward operating base Lion for the next 72 hours (see fig 2-8). The CSB commander assigns the LOC protection mission to an assigned combat support MP battalion (BN) with tailored protection

capabilities in direct support. The combat support MP BN establishes a mobility corridor to support protection of convoys along the designated LOC. The CSB staff also coordinates unit air protection requirements with Army and joint fires, intelligence, and air protection with the fires brigade (BDE), battlefield surveillance BDE, aviation BDE, and appropriate division staff points of contact.

(2) Specialized ground protection equipment including sensor and shooter systems integrated into a system of protection system is positioned at key points in the mobility corridor to monitor the environment, sensing and reporting hazards to the commander's C2 nodes. The integrated reporting feature not only insures that all who transit the corridor have the most up-to-date information on hazards in the corridor, but informs the larger COP. MPs are continuously patrolling the LOC to assess the condition of the main supply routes and are interfacing with the local communities in an effort to gather intelligence that will improve SU of the environment. Engineer units are positioned in the corridor at key points to maintain the MSRs with specialized lightweight rapid repair capabilities.

(3) During convoy operations, unmanned vehicles (air and ground), working together autonomously, move ahead of the convoys to detect, assess, warn, and respond to hazards identified in the corridor. UAS sweep the entire corridor from 500 meters either side of the LOC, detecting activities, behaviors, and objects that are processed through the protection units databases to automatically aid hazards identification to include the enemy, IED, mines, ambush sites, etc. Remote controlled intelligent effects systems, such as light and heavily armed robotics, respond to targets combat identified by the sensor systems, providing lethal and nonlethal effects when prompted. Unmanned ground vehicles, with mission tailored packages, respond to identified hazards in an effort to destroy or neutralize the hazard at stand-off distance. Minimally manned autonomous, robot enabled intelligent control points are established along the route to deter vehicle borne improvised explosive devices, and remove civilians from the main supply routes.

(4) The convoy commander is provided a ground protection direct fire protective system which is positioned throughout the convoy to protect personnel and assets. The convoy commander and all convoy elements are able to maintain a protection SA and SU of the corridor through LandWarNet and JC2.

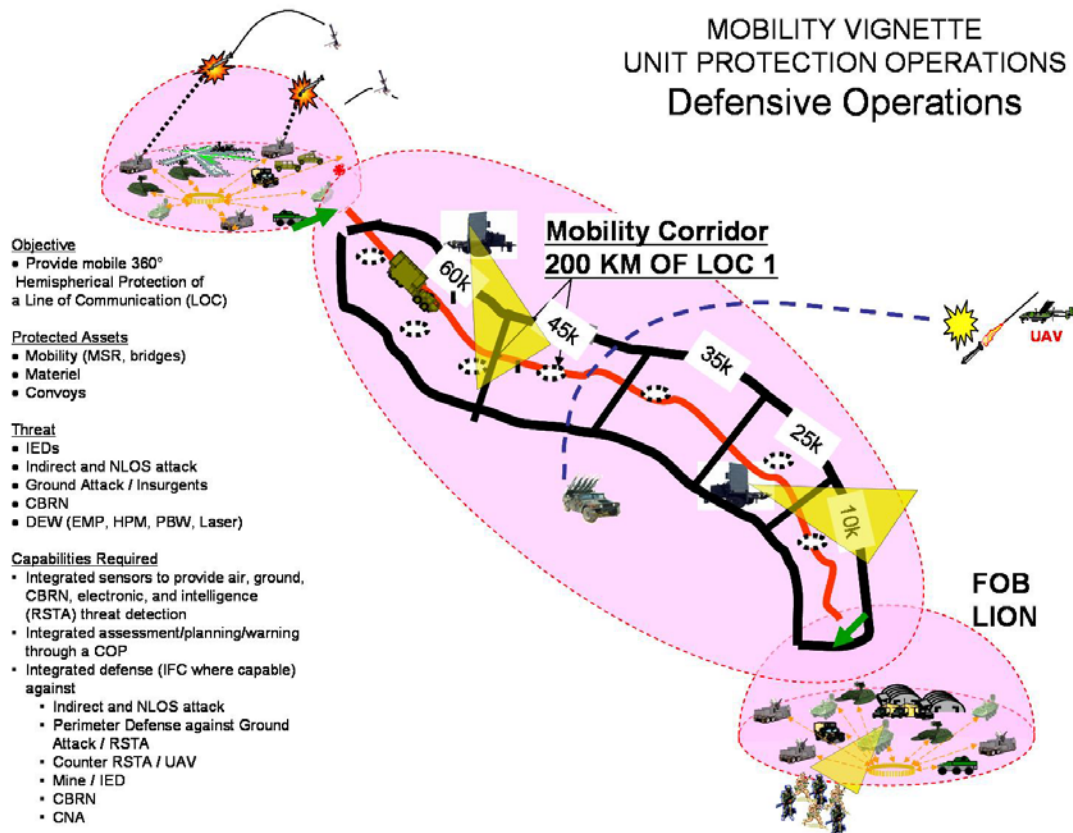


Figure 2-8. UP Operations in a Mobile Environment

g. Offensive Operation

(1) Offensive operations carry the fight to the enemy by closing with and destroying enemy forces, seizing territory and vital resources, and imposing the commanders will on the enemy. The offense focuses on seizing, retaining, and exploiting the initiative. This active imposition of land power makes the offense the decisive type of military operations, whether undertaken against irregular forces or the armed forces of a nation state.

(2) UP facilitates the offense by providing freedom of maneuver for attacking forces. A commander can utilize UP detect capabilities to increase SA and SU through the integrated sensing of air, ground, CBRNE, electronic, and intelligence threats achieved through a FoS/SoS UP detect capability. This detection function provides the commander relevant information to formulate courses of action against adversary forces. UP detect and assess functions facilitate an improved, unambiguous early warning capability distributable through JC2 to the protected force. Through the application of active and passive measures a commander can protect the force against active air, ground, CBRNE, electronic, and intelligence threats.

(3) Offense operations are enhanced through an integrated, network of sensors and shooters protection system that will provide integrated fire control for deterring multiple threats to units. The integrated fire control capability includes the ability for a system to detect and assess all threats throughout the ROMO, and automatically select and execute the optimum deterrent capability, lethal or nonlethal. The integrated fire control capability requires the integration of sensor and shooter systems and processes. This integrated and networked protection capability will protect the massing of offensive forces and add depth to offensive formations. These capabilities in turn deny freedom of maneuver to enemy forces. Integrated UP capabilities inherently increase the security of strategic, operational and tactical areas of operations by providing point and wide area integrated protection in noncontiguous, non-linear offensive operations.

f. Defensive Operations

(1) Defensive operations counter enemy offensive operations. They defeat attacks, destroying as many attackers as necessary. Defensive operations preserve control over land, resources, and population. Successful defensive operations retain terrain, protect populations, and protect key resources.

(2) UP will support and provide a commander enhanced defensive capabilities through the integration of UP functions. The unit commander will require the fused detection of threats and an integrated ability to discern the type and level of threat elements in the AO and interest. Improved SA and SU will provide the commander an enhanced ability to discern and predict enemy courses of action, and provide actionable warning to protected personnel, assets, and information.

(3) Proper assessment of friendly assets and adversary capabilities assist in the distribution of timely and unambiguous warning and the development of necessary passive and active measures, actions, and postures. The commander will be aided with scalable, tailorable, modular, and integrated passive and active measures to deter and defend against air, ground, CBRNE, electronic, and intelligence threats. These active and passive defensive capabilities will deliver a full suite of protection capabilities. The application of the UP act sub-functions, will serve to deter and prevent adversary offensive capabilities. Passive act capabilities can serve to dissuade an adversary's action, through the existence of a credible threat of unacceptable counteraction. Ultimately, the application of passive UP act capabilities will preclude and preempt hostile actions.

(4) The UP capabilities protect the massing of defensive forces, add or deny depth to the defensive positions, and assist in denying the freedom of maneuver to attacking enemy forces. These capabilities in turn provide freedom of maneuver for defending forces, and facilitate a rapid return to offensive operations.

g. Stability Operations

(1) Stability operations sustain and exploit security and control over areas, populations, and resources. These operations involve employing military and cooperative agency capabilities

and can involve both coercive and cooperative actions. They may occur before, during, and after offensive and defensive operations, however, they also occur separately, usually at the lower end of the ROMO. Stability operations lead to an environment in which the other instruments of national power can predominate (in cooperation with a legitimate government).

(2) The main objectives of SO are restoring or establishing order, providing humanitarian assistance, establishing new governance, restoring essential services, and assisting in economic reconstruction. Security and support requirements from protection of vital facilities to the maintenance of civil order and humanitarian services may arise with little warning and at widely separated locations throughout the theater. The faster and more effectively forces respond to these challenges, the less effort will be required to cope with them, and the less likely it is they will escalate to an intensity threatening the political and military integrity of overall theater operations.

(3) Recent SO indicate a JFC must understand there are always opponents, internal and external, opposed to foreign military presence. The JFC will encounter numerous armed groups ranging from residual military forces, opposing paramilitary groups, insurgent forces, organized criminal gangs, to terrorist cells. Resistance strategies often include violence against civilians and attacks on the military and civilian members of the coalition. Resistance to security, transition, and reconstruction operations may be passive or active. Passive measures may include demonstrations, strikes, or boycotts. Active measures could range from blocking delivery of humanitarian aid to terrorist activities, such as assassinations, causing electromagnetic interference for critical transmitters, bombings, suicide attacks, or military operations, such as raids and ambushes.

(4) UP capabilities will support a commander during SO through the combined capabilities provided during offensive and defensive operations. Though SO are neither implicitly offensive nor defensive in nature these operations may at times require *specific* offensive or defensive capabilities. Stability operations will additionally have their own UP functional mission requirements. All commanders involved in SO will benefit from the increased SA and SU that the functions of UP detect and assess provide. These capabilities will enhance a commander's visualization of the battlefield and the overall awareness of the AO and area of interest. The UP detect and assess functions, aided with a robust counterintelligence (CI) and civil affairs plan will assist the commander in predicting and determining patterned civil/adversary plans and motives. The integrated UP warn sub-function will facilitate the commander by providing unambiguous and relevant information to the protected force, the JIM community, and host nation friendly government and non-government agencies. When necessary, the commander will be armed with numerous active, passive, lethal, nonlethal, directed energy and kinetic energy measures to deploy against an adversary.

(5) The UP act function provides the commander specific capabilities that are especially beneficial during SO, (such as, nonlethal and passive defense measures). These options will be crucial, especially during politically and militarily sensitivity SO. The UP functions will further aid the commander by increasing security and decreasing recovery time and actions, which will in turn facilitate improved freedom of maneuver. The integrated UP functions will free

resources and personal to commit to other mission essential missions not related to the overall protection of the operational area.

2-10. Summary

a. The functions of UP are interrelated and supportive of a commander's ability to understand, plan, and dedicate specific capabilities to the protection of the force (see fig 2-4).

b. The application of an integrated and modular 360° hemispherical protection capability via the UP *detect, assess, decide, act* and *recover* functional construct will improve a commander's ability to protect personnel, assets, and information of the future battlefield.

Chapter 3 Required Capabilities

a. The functional capabilities required by an Army or JFC to execute a 360° hemispherical UP mission are outlined below. These capabilities provide the commander with an additive, modular, tailorable, integrated FoS/SoS protective suite that facilitate the ability to configure sensor and response systems to the environmental and threat target set. These UP capabilities will integrate with JC2, sharing information across the global information grid (GIG), integrating into the global position systems and other force tracking systems.

b. This current listing of required capabilities should be interpreted as optimum capabilities during the 2012-2024 timeframe. The UP required capabilities listing is not all inclusive and will be further refined and developed as the UP CCP matures, and as joint capabilities integration and development system analysis is executed. Technological and threat advances may also drive changes to the listed capability requirements.

c. The UP functions and their related capabilities collectively contribute to the commander's ability to *see first, understand first, act first, reengage at will, and finish decisively*.

3-1. Unit Protection Operations

a. Detect. UP detect capabilities will enable the commander to sense the full range of friendly and hostile air, ground, CBRNE, and electronic activities to provide real-time SA enabling 360° hemispherical UP. Accurate and timely detection of threats and hazards require the effective integration of sensors, databases, surveillance, and communications systems in order to collect timely, unambiguous, and accurate data on adversary capabilities and actions planned or employed against friendly resources (personnel, physical assets, or information).

(1) As a minimum, UP detect FoS/SoS capabilities will-

- Integrate with JC2, and the GIG to provide seamless information systems ISR interoperability with the protected force.
- Operate in real-time.

- Detect threats directly (first hand) or virtually through the UP FoS/SoS and external information operations intelligence networks.
- Detect at stand-off distances (such as distances beyond an adversaries engagement envelope).
- Provide persistent surveillance.
- Provide pervasive surveillance (provide for area and point detection, to include dead spaces).
- Provide overlapping sensor detection capability.
- Support all weather, climate, and terrain operations, from open desert, to dense vegetation, mountainous, and urban locales.
- Support operations in EMP and CBRN environments.
- Be undetectable or unrecognizable by adversary systems and capabilities.

(2) The UP FoS/SoS *detect* capabilities will provide additional unique capabilities.

(a) Support the four Army AMD mission sets: provide air and missile defense, contribute to third dimensional SA and SU, contribute to airspace management, and contribute to operational force protection.

(b) Integrate sensors with a suite of UP FoS/SoS sensor capabilities. Provide stand-off detection of friendly and hostile aerial platforms via ground and elevated sensors.

(c) Detect or receive, through secure data feeds, such things as-

- Tactical ballistic missiles (TBMs).
- Short-range ballistic missiles (SRBMs).
- Medium-range ballistic missiles (MRBMs).
- Intermediate-range ballistic missiles (IRBMs).
- Intercontinental ballistic missiles (ICBMs).
- Sea-launched ballistic missiles (SLBM).
- Cruise missiles (CMs).
- RAMs.
- Large-caliber rockets (LCRs).
- Air-to-surface missiles (ASMs), to include anti-radiation missiles (ARMs), both manned and UAS delivered.
- UAS.
- Manned platforms, fixed-wing (FW) and rotary-wing (RW) aircraft.

(d) Detect air platforms and objects of all sizes and radar cross section (RCS) and launch point designations. Execute continuous tracking through all phases of flight. Support integrated fire control, allowing the detection to trigger timely engagement with applicable weapon systems at non-line-of-sight (NLOS)/BLOS distances.

(e) Detect and counter electromagnetic radiation spectrum or other forms of electronic jamming in all adversary environments. Detect the full range of enemy, friendly, and

environmental, to include populations activities that may threaten UP and or impede operations. These capabilities will include the ability to-

- Locate and track friendly and hostile individuals, vehicles, objects, chemicals (including explosives), and activities in all environments.
- Incorporate “smart” technologies that can be remotely operated, serviced (on-board diagnostics and repair capability), tuned (redirected to other targets), and reprogrammed remotely (electronically reconfigured and optimized for other targets).

(f) Sense, detect and discern CBRNE threats. This capability will include the ability to-

- Detect the presence of IED fillers.
- Detect traditional and non-traditional CBRN agent contamination.
- Detect CBRNE hazards prior to and after event.
- Identify and assess agents (CBRN or toxic industrial material (TIM)).
- Project downwind hazards and distances.
- Provide real-time meteorological/other data.
- Provide battlefield ordnance awareness.
- Integrate appropriate disparate (non-CBRNE specific) sensor data.
- Stand-off traditional and non-traditional agent detection.
- Provide 360° battlefield views (stand-off sensors coupled to real-time networked displays and change detection/other software).
- Provide remote CBRNE tactical support planning and decisionmaking tools.

(g) Sense and monitor electromagnetic interference. This capability will include the ability to-

- Sense and monitor electromagnetic interference caused by friendly military, local government or non-government agencies; intentional or unintentional.
- Detect hostile network intrusion activity, electronic warfare (EW), jamming, and CNA.
- Detect interruptions in JC2, GIG, and other information systems ISR systems or networks, and other networks.
- Self-diagnose (assess detect sensor(s) operational status).

(h) Provide human and technical detection of the threat and or other impediment information and activities.

(2) These required UP detect capabilities provide the ability for a commander to *see first*, through a 360° hemispherical COP.

b. Assess

(1) UP *assess* capabilities will as at minimum collect, integrate, and display tactically relevant and relational threat information from local protection systems and joint GIG information and intelligence in order to recognize, classify, and identify detected elements, report on their activities and determine threat intent with sufficient fidelity to facilitate planning/implementation of countermeasures.

(2) As a minimum, all UP assess capabilities will-

- Integrate with JC2 systems, and the GIG to provide seamless information systems ISR interoperability with the protected force.
- Operate in real-time.
- Provide complementary assessment capabilities.
- Disseminate (physically or virtually) assessment status to all echelons, formations, and the individual Soldier when applicable.
- Support all weather, climate, and terrain operations, from open desert, to dense vegetation, mountainous, and urban locales.
- Support operations in EMP and CBRN environments.

(3) The UP FoS/SoS *assess* capabilities will provide additional unique capabilities. They are discussed below.

(a) Facilitate the AMD mission to contribute to third dimensional SA and SU and will include actions and capabilities that provide visualization and understanding of aerial activities or events occurring in the third dimension operational environment.

(b) Facilitate the AMD mission to contribute to airspace management and includes actions and capabilities that enable fires and manned/unmanned airspace users in a JIM environment while-

- Protecting friendly forces.
- Ensuring the synchronized use of airspace.
- Enhancing the battle command of forces using that airspace.

(c) Determine munitions delivery method.

(d) Assess threat jamming existence and capability.

(e) Provide impact point prediction (time and location) for both incoming and outgoing air threats and friendly air (missile, RAM) activities.

(f) Determine adversary air threat launch locations, to include missiles and manned and unmanned air craft.

(g) Determine enemy and friendly air object or platform identification through positive and procedural means that account for friendly identification, friend or foe inoperability.

(h) Provide ATR for ground threats via the use of an operationally relevant database (achieved by fusing of real-time local and imported situational and intelligence data, provided by sensor systems) and algorithms to evaluate all types of collected sensor data against database models for behaviors, man-made changes to the environment, and hazards based on molecular characteristics to identify the target/hazard.

(i) Provide precision identification using passive (biometric sensors, voice pattern, and stress anxiety analysis, and systems to determine the contents of containers or vehicles) and active (scalable effects systems (lethal and nonlethal), used to produce action or reaction to specific events).

(j) Determine air, ground, CBRNE, electronic information and intelligence threat intent.

(k) Assess network availability and operational status.

(l) Assess adversary network capability and status.

(m) Determine the physical and virtual (spectrum) locations of adversary communications assets and real-time operational status.

(n) Assess adversary electronic attack (EA) and CNA capability.

(o) Quickly and accurately determine the characteristics of an EA and CNA to include-

- Criticality and vulnerability of the systems under attack.
- Source of the attack.
- Purpose of the attack.

(p) Assessment of threat capabilities, operations and, current and expected threat actions across ROMO to provide the commander with an assessment for the development and execution of countermeasures.

(q) Intent of threat elements.

(r) Associations of threat elements.

(s) Location of potential threat attack and defense operations.

(t) Recommend the preferred friendly C2 for an enemy attack.

(u) Potential attack and defense means.

(v) Anticipated times for attack.

(w) Likely locations of threat listening post/observation post.

- (x) Probable post attack/defense escape routes.
 - (y) Likely threat IED techniques.
 - (z) Predicted IED detonation means.
 - (aa) Predicted IED timing (day versus night, day of week).
 - (ab) Predicted IED infiltration routes, emplacement.
 - (ac) IED ex-filtration route for insurgents.
 - (ad) Munitions storage (areas or locations).
 - (ae) IED and other munitions production facilities.
 - (af) Preferred supplementary or complementary operations (small arms to kill, small arms fire to capture, secondary).
 - (ag) Recommend the preferred friendly counter ISR and EW technologies.
 - (ah) Key threat indirect fire attack features.
- (3) These required UP assess capabilities provide the ability for a commander to *understand first*, through a 360° hemispherical COP.

c. Decide

(1) UP *decide* capabilities will provide a commander battle command C2 capabilities that will have seamless information systems ISR interoperability with the force it supports. As a minimum, UP decide FoS/SoS capabilities will-

- (a) Provide real-time SA allowing commanders, staff, and Soldiers to visualize the battlefield three dimensionally.
- (b) Provide a shared common picture of the operational environment.
- (c) Provide graphical displays, with friendly and enemy proposed and current unit locations.
- (d) Provide target/hazard identification and tracking.
- (e) Provide the ability to task and synchronize the UP FoS and SoS sensors, act measures, and units to include available networked fires.

(f) Support, as required, autonomous effective and fast sensor-to-shooter systems of precision-guided and intelligent munitions that can quickly render targets and hazards harmless.

(2) The UP FoS and SoS *decide* capabilities will provide additional unique capabilities, such as-

(a) Interactive, flexible, and adaptable processes that provide an easy to use and understand interface capability; allowing for the decisionmaker's own insights.

(b) Fuse large amounts of data into information that can be quickly acted upon and will support decision support system.

(c) Effective in near simultaneous protection measures analysis required in UP operations.

(d) Automated tools.

(e) Mission planning and rehearsal, and joint mapping tool kit will support rapid COA analysis.

(f) Provide predictions about factors governed by the laws of physics.

(g) Capable to execute analysis information which will present and organize information to support a decision.

(h) Trigger timely full range (to include BLOS and NLOS response to the detected threat via integration with UP assess, decide, and act capabilities (including automatic engagement and integrated fire control/direction).

(3) The UP decides BCSs will provide the commander the capability to decide, task, and monitor at the tempo and fidelity to ensure unit success, and will aid in the *ability to understand* and *act first*.

d. Act

(1) Act includes the capability to execute active and passive measures, and warning to protect personnel, assets, and information from adversary plans and actions. Warning includes the reaction to actionable intelligence by disseminating warnings or predictions in a timely, accurate, and unambiguous manner. Specifically, warning includes the acknowledgement and communication of hazards implicit in a wide spectrum of hostile and friendly activities. Warning additionally includes the ability to execute both friendly and enemy warning. Warning the adversary will serve as a means to deter threat activity, and will be executed at strategic, operational and tactical levels.

(2) Active measures will require scalable lethal and nonlethal, kinetic and non-kinetic effects and weapons, and directed energy to neutralize threat attack, and will be proactive or reactive. Passive measure will require the same capabilities, but will not be lethal in nature. Passive measures will generally be those actions the unit takes to provide protection from impending attacks, such as bunkers, and donning mission oriented protective posture equipment. The utilization of the *act* function and its related capabilities enable a commander to preserve operational capabilities for decisive operations. As a minimum, UP *act* FoS and SoS capabilities will-

(a) Integrate with JC2, and the GIG to provide seamless information systems ISR interoperability with the protected force.

(b) Operate in real-time.

(c) Support all weather, climate, and terrain operations, from open desert, to dense vegetation, mountainous, and urban locales.

(d) Support operations in EMP and CBRN environments.

(e) Disseminate warning (physically, audibly, virtually, and visually) to all echelons, formations, and the individual Soldier.

(f) Provide unambiguous and actionable warning to friendly forces.

(g) Provide redundancies in act capability applications.

(h) Include proactive passive options (for example, the means to reduce the vulnerability of friendly forces, command centers, and other critical assets, to the effects of threat systems).

(i) Provide active options, such as the means to deter, neutralize, and destroy on-going hostile attacks.

(j) Provide attack options, such as the means to integrate fires to deter and destroy threats and preclude attacks on friendly forces, command centers, and other critical assets.

(k) Provide the capability to execute nonlethal, graduated warning to the adversary which will deter, interrupt, or cease intended or further hostile action.

(3) The UP FoS and SoS *act* capabilities will possess additional unique capabilities, such as-

(a) Provide warnings to friendly forces of impending air threat type and impact point and time.

(b) Provide warnings to friendly forces of impending friendly air operations.

- (c) Provide warnings of friendly and adversary ground activities.
- (d) Provide virtual and visual marking of obstacles, hazards, and IEDs.
- (e) Incorporate a wide array of warn technologies including-
 - Audible systems.
 - Visual systems.
 - Soldier-manual alert.
 - Canine assistance as a necessary capability.
 - Robotic systems.
 - Autonomous systems.
- (f) Provide warning of CBRNE events or attacks.
- (g) Provide CBRNE warning at the tactical level to include wind patterns, speeds, and other CBRNE effects.
- (h) Provide warning of specific agent type.
- (i) Provide warning of anticipated time of contamination arrival.
- (j) Provide warning of possible CBRNE threats.
- (k) Provide warning of multi-level CBRNE hazard confirmation.
- (l) Populate the COP at the operational and tactical levels part of the standard NBC warning and reporting system.
- (m) Provide warning to prepare for residual enemy CBRNE weapon elimination.
- (n) Warn the commander of potential or actual degradation to the information systems ISR network resulting from threat activity or equipment failure.
- (o) Warn of network connectivity loss and interference to affected network managers and users.
- (p) Provide warnings of failed sensor(s) connectivity.
- (q) Disseminate precise warnings and actions taken to isolate, repel or mitigate the effects of-
 - Network attack.
 - Unauthorized access to sensor information.

(r) Intelligence warning capabilities which provide alert to all echelons and will include the ability to disseminate warnings via normal communication channels, as well as some intelligence specific means.

- (s) Provide intelligence warning of probable associations of threat elements.
- (t) Provide warning of the locations for predicted threat attack and defense operations.
- (u) Provide warning for the preferred C2 of attack.
- (v) Provide warning for the predicted attack and defense means.
- (w) Provide warning for the anticipated times for attack.
- (x) Provide warning for the likely locations of threat listening post/observation post.
- (y) Provide warning for the probable post attack/defense escape routes.
- (z) Provide warning for the likely threat IED techniques.
- (aa) Provide warning for the predicted IED detonation means.
- (ab) Provide warning for the predicted IED timing (day versus night, day of week).
- (ac) Provide warning for the predicted IED infiltration routes, emplacement.
- (ad) Provide warning for the IED exfiltration route.
- (ae) Provide warning for the predicted munitions storage (areas or locations).
- (af) Provide warning for the predicted IED and other munitions production facilities.
- (ag) Provide warning for the preferred counter ISR and EW technologies.
- (ah) Provide warning for the key threat indirect fire attack features.
- (ai) Provide protection and fires against the following air-threats:
 - TBM.
 - SRBM.
 - MRBM.
 - IRBM.
 - ICBM.
 - SLBM.
 - CM.
 - RAM.

- LCR.
- ASMs, to include ARMs.
- UAS.
- Manned platforms, FW and RW aircraft.

(aj) Engage air platforms and objects of all sizes and radar cross section. (RCS).

(ak) Nullify data saturation opportunities for enemy forces executing missile and aircraft attack.

(al) Execute active fires against enemy launch point designations, air defense sites, missile, and aircraft.

(am) Engage air threats during all phases of adversary capability flight.

(an) Protect friendly aircraft against adversary air defense activities.

(ao) Support integrated fire control, allowing the detection of an air or ground threat to trigger timely and automatic engagement, when required, of threat systems and or weapons with applicable friendly air and ground weapon systems at NLOS/BLOS distances.

(ap) Embedded automated ability for the protected force to repel network attacks.

(aq) Transparently and automatically reroute priority network information around degraded/compromised network through terrestrial, airborne, and space communications assets.

(ar) Ability to locate, identify, and destroy (physically and electronically) adversary network attack/intrusion capability.

(as) Integrate physical protective, procedural, and antiterrorism security measures.

(at) Neutralize the full spectrum of hazards along a route and prevent re-seeding of hazards with or without the aid of precision detection.

(au) Provide graduated response (attack) to include remote controlled intelligent lethal and nonlethal munitions systems.

(av) Combine preventive prophylaxis to counter CBRNE attack.

(aw) Defeat CBRNE hazards prior to their use.

(ax) Effective decontamination of materials.

(ay) Effective deployment/employment of friendly CBRN units and equipment:

- Individual protection equipment (IEP) and collective protection equipment (CPE).

- Breathing capability on strategic delivery platforms.
- Breathable filters.
- Ingress and egress between CPE systems.
- Vaccines against biological agents (natural, industrial, or militarized).

(az) Provide reliable, near continuous access to enterprise information and service both on the move and at the halt.

(ba) Provide network redundancy and self-protection.

(bb) Defeat adversary ISR capabilities with active and passive measures.

(bc) Execute sensor reporting and analysis that predicts the most likely threat actions and assesses threat capabilities.

(bd) Multi-discipline counterintelligence to assess threat intelligence collection capabilities.

(4) The UP *act* capability will provide the commander the ability to execute enemy and friendly warning, and active and passive protection measures to ensure unit success. These combined capabilities will aid in the ability to *act first, reengage at will, and finish decisively*.

e. Recover

(1) UP *recover* capabilities provide tools that enable the rapid restoration of operational readiness for all affected *detect, assess, decide, and act* UP systems and processes, to include UP FoS, SoS and logistics capabilities, during and following attacks. As a minimum, UP *recover* capabilities will-

(a) Enable the battle damage assessment and battle damage repair process.

(b) Utilize embedded systems and technologies that enable self-recover processes and capabilities.

(c) Utilize self-healing technologies and components in the design of future systems.

(d) Utilize unmanned systems to enable UP recover capability restoration.

(e) Leverage existing and require additional improvements in sustainment functions.

(2) The UP FoS and SoS recover capabilities will provide additional unique capabilities, such as-

(a) Decontamination materials and processes that do not degrade sensitive equipment and systems capability, such as aircraft and electronics.

(b) Improved decontamination materials and procedures, such as distribution of CBRN decontamination unit capabilities to non-CBRN units.

(c) Treatment or medicine to return the injured to pre-contaminated health.

(d) International standards and protocols for marking contaminated areas.

(e) Unmanned decontamination platforms and systems.

(f) Precision roll-on/roll-off decontamination means.

(g) Improved contaminated area marking systems.

(h) Assess and repair information infrastructure at strategic, operational, and tactical levels.

(i) Detect and recover lost or corrupted information.

(j) Assess the impact of lost or corrupted information at strategic, operational, and tactical levels.

(3) The UP *recover* function will provide the commander the ability to restore the UP capabilities of *detect*, *assess*, *decide*, and *act*, and will return 360° hemispherical protection to the AO. These actions will not only provide protection, but additionally facilitate internal recovery operations ensuring unit success. This capability will aid in the ability to *finish decisively*.

Chapter 4

Migration Plan

a. This chapter serves to detail current capabilities and address development of current capabilities to optimum future desired capabilities. Bridging the gap between current and future capabilities is a complex task to accomplish, but nevertheless attainable.

b. The future capabilities described in this chapter are crafted in a best case scenario. They are the optimum UP capability for the timeframe, threat, and ROMO that our forces will encounter. The incremental goal of bridging the gap from current to future capabilities is depicted in figure 4-1.

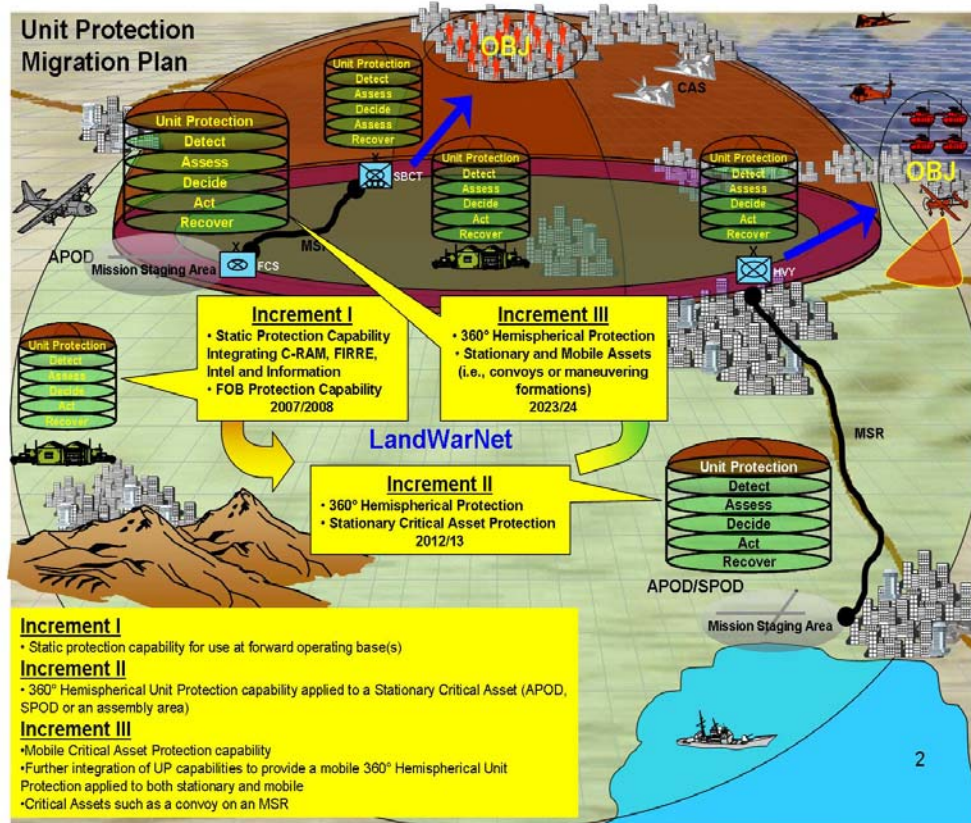


Figure 4-1. Bridging the Gap from current to Future Capabilities

4-1. Assessment of Current Protection Capabilities Across the Detect, Assess, Decide, Act and Recover UP Range of Functions

a. There is no doubt that the U.S. military is the world’s leader in innovation and technology. There is a wealth of protection related capabilities, equipment, technologies, and procedures available to our forces and allies. These technologies, though equally effective in defending against numerous adversary capabilities, lack a common capability underpinning the theme of DOD transformation, the ability to integrate and interoperate. Current protection capabilities are stove piped and ill-equipped to provide the rapid, comprehensive, and integrated capabilities required for the future force.

b. Detect. The following section describes current detect capabilities against adversary air, ground, CBRNE, information, electronic and intelligence threats.

(1) *Air*

(a) Current AMD systems use deployed space, air, and ground based sensors to detect the launch of ballistic missile from threat regions, CMs, UAS, ASMs, RAM, as well, have residual capability to detect FW and RW aircraft. The detection of FW and RW is important due to the focus on “friendly protection.” These sensors use radar and infrared techniques to track the aforementioned adversary’s air platforms and warn the defended assets of the attack, as well as determine if the platforms should be engaged by AMD interceptors.

(b) There are numerous limitations with the current capability to detect air threats. These limitations include: the ability to detect short-range, medium-range, intermediate-range, submarine-launched, and intercontinental ballistic missiles from space-based sensors beyond the ascent/boost phase of the ballistic missile’s flight; the ability to detect short-range, medium-range, intermediate-range, and submarine-launched ballistic missiles from a threat of 360° due to the sensors primarily being sectorized; the ability to detect CMs, UAS, ASMs, FW, and RW at extended ranges necessary to keep threat platforms outside the protected area’s “keep out” ranges necessary for negating the effects of air delivered WMD; the ability to detect CMs, UAS, ASMs, FW, and RW beyond line of sight limitations of ground based sensors; the ability to detect low radar cross section ballistic and non-ballistic threats at significant ranges; the ability to detect significant numbers of RAM launched at static and mobile protected assets.

(2) *Ground*

(a) Current ground detection systems have not been designed or built to function as FoS and SoS. This fact has resulted in the limitations within the current system. They do not share their information or data within their own nets or with other theater information systems ISR. This has resulted in the inability to provide the commander an integrated seamless system of protection systems. Current detection systems require extensive improvements to reduce false and nuisance alarm rates, distinguish friend from enemy, and defeat highly deceptive enemy forces. They provide limited wide area, long-range detection and surveillance (fixed and mobile), access control, intruder tracking and classification, remote/stand-off detection of explosive and delay/denial threat devices or integrated SA.

(b) Today’s units detect explosive hazards utilizing contingency components, which use an array of different detecting capabilities. These include detection by metallic sensors, explosive sensing, radar, and infrared. These systems are mounted on vehicle platforms that are manually and remotely operated, and mounted on hand-held devices. Other sensors also include visual sensors and the use of “mine dog” detachments. These components are contingency tools not readily available to all units, and are provided to units as mission dictates and in theater.

(3) *CBRNE*

(a) Current technology uses intelligence and ground based systems, to detect CBRNE in land, water, and air, focused on point/stand-off and early warning applications. Gathering intelligence not only allows prediction of an attack, but detection before an attack. Ground based systems use current detectors that detect the vapor of most chemical warfare agents and few

toxic industrial chemical (TIC). Detection is very rapid for chemical agents, but requires more time to identify a biological agent and is presumptory information without laboratory confirmation which can take hours to days. Though most detectors do not quantify the agent concentration, some provide relative hazard indications, and more sensitive detectors provide absolute quantification capabilities. Most of the sensitive detectors are commercial off the shelf technology and available only to specialized units.

(b) The majority of the Army's current detectors are point detectors. The Army has developed limited chemical and biological stand-off detection capability and currently only stationary chemical stand-off detection is fielded. Point detectors provide a detect-to-treat capability where a detect-to-warn capability is preferred. Currently fielded radiological detectors detect most radiation, but primarily at the military significant hazard level. Those detectors that detect alpha radiation and other low level sources are low density pieces of equipment or commercial off the shelf and not available to all units. Radiological detection deficiencies include the lack of radioisotope identification and detectors that take samples for future analysis. There is a complete lack of radiological standoff detection capabilities.

(4) *Information*

(a) Current information detect capabilities, which use active measures to protect LandWarNet components, are the ability to detect intrusion, jamming, and other electronic countermeasures, and CNA. Hardware and software solutions include commercial firewalls, anti-virus programs, and intrusion detection analysis tools for network related protection. The limiting factor is that no single solution exists to offset stove piped networks across the Army.

(b) Currently, the variety of unique and proprietary network configurations hinders the ability to share electronic protection resources across the battlefield, creating a substantial risk to deployed forces and unnecessary duplication of effort and cost. Additionally, current capabilities do not detect intrusion activity in real-time for unregistered (not previously detected) anomalies, and are not integrated down to platform level.

(5) *Electronic Protection*

(a) Electronic protect capabilities, which use active and passive means to protect personnel, facilities, and equipment are the ability to protect, detect, warn, and react to electromagnetic spectrum EA weapons. Current and future electromagnetic spectrum threats include the use of directed energy weapons, IEDs, infrared, radio frequency, electro-optical, and thermal and emissions guided munitions.

(b) Current electronic protection ground capabilities do not detect laser, particle beam weapons, radio frequency, radar, infrared, or electro-optical, and hardening assets against the effects of EMP and high power microwave are minimal and not sufficient.

(6) *Intelligence*

(a) Current intelligence detect capabilities are comprised of human intelligence (HUMINT) to include counter intelligence and HUMINT collectors assigned to the BCT MI company, Stryker BCT, surveillance troop and division MI BN, and the theater and military intelligence brigades. Current force structure identifies five military intelligence brigades and theater intelligence groups. Each consists of a headquarters (HQ) and HQ company, a forward collection communication and electronics BN, and a U.S. Army Reserve theater support brigade. The military intelligence brigades include the theater intelligence group structure, an operation BN, and an aerial exploitation/reconnaissance BN. This concept transitions the groups to brigades and will be referred to as such in subsequent paragraphs.

(b) Each organization will have four to five subordinate BNs. Assigned are: an operations BN, a forward collection BN (CI/HUMINT), a forward collection BN (signal intelligence (SIGINT)), a theater support battalion and a strategic SIGINT BN. Military intelligence brigades coordinate, manage, and direct intelligence and surveillance; they conduct collection management, all-source intelligence analysis, production; and they disseminate information in support of national, joint, interagency, multi-national, regional combatant command, and Army service component requirements. The following are current capabilities to assist in detect-

- Biometric automated technologies/counter human deception detection (CHDD). Advances in technology, especially in biometrics (physiological, neurological, thermal analysis) will enable future CI agents and HUMINT collectors to more accurately identify not only personnel for identification purposes, but will provide various types of signatures regarding indicators of deception
- Related technological advances in information systems will provide future CI and HUMINT with automated analysis and data sharing in order to assist in identifying deception in subjects scrutinized for intelligence purposes (such as screening, investigations, source vetting, collection, etc.).
- CHDD will surpass current polygraph techniques for measuring physiological signatures/indicators and the associated subjective analysis and evaluation.
- Additionally, these same technologies will develop physiological signatures which can be entered and tracked through biometric devices and databasing. This will aid in identification, tracking, and stand-off detection of persons of interest whose profiles exist.
 - SIGINT: Guardrail common sensor (airborne collection).
 - Prophet: BCT MI company, Stryker BCT (SBCT), surveillance troop division MI BN and corps (ground collection).
 - Imagery Intelligence (IMINT): Shadow tactical unmanned aerial vehicle (SBCT surveillance troop). Hunter (UAS), Raven (UAS) companies and BNs. Tactical/distributed exploitation system.
 - Measurements and Signatures Intelligence (MASINT).
 - PPS-5D (or ground surveillance radar) (SBCT surveillance troop) being phased out. Remotely monitored battlefield sensor system (BCT MI company, SBCT surveillance troop) being phased out.

c. Assess. The following section describes current assess capabilities against adversary air, ground, CBRNE, information, electronic, and intelligence threats.

(1) *Air*

(a) Current AMD systems use data obtained from ground and space-based sensors to determine if a ballistic or non-ballistic air platform poses a threat to assets that are protected by AMD forces. The assessment of these threat platforms relies on accurate and timely data from the sensors, as well as software algorithms developed for the AMD systems that determine the classification of the platform (ballistic, non-ballistic, manned, and unmanned), identification of the platform (friend, hostile), and probable intent of platform. The assessment process includes the determination of what areas will be affected by the air threat platform(s) and the follow-on actions of warning those affected areas and determining if the engagement process should begin against the threat platform(s).

(b) Current limitations of assessment include the positive classification and identification of the platform. Current technologies do not provide a reliable method to identify friendly and hostile platforms throughout their flight. A ground based sensor's line-of-sight limitation can also play a significant role in assessing the air threat. The threat's intent is also difficult to determine based on today's technologies and the ability to arm a ballistic or non-ballistic platform with a weapon of mass destruction, which adds significant ambiguity to the threat's intent. The inability to share data obtained from joint and allied sensors to develop an unambiguous air picture/COP also hinders the current assessment process.

(2) *Ground*

(a) Ground assessment systems are stand-alone and do not provide a seamless system of protection systems. Unless an assessment can be made at the point of sensing, such as CBRNE detection, assessment systems rely extensively on a human in the loop to distinguish friend from enemy and defeat highly deceptive enemy forces. The operator is forced to process an input from the moment detection is made to the point of a decision. Today, imagers are the operator's primary tool for making an assessment.

(b) Current imager limitations do not readily enable the operator to make a combat identification to determine intent for all alerts at stand-off ranges. There are few automated aides or a range of interrogators to help him make a combat identification. As a result, the commander must require Soldiers to move close enough to the hazard to observe and determine intent, placing them in harms way. Even if automated assessment tools did exist today, commanders have no capability to fuse all the available intelligence into a relevant local database that would enable these automated assessment tools.

(3) *CBRNE*

(a) *Assess* provides forces with the capability to collect, analyze, identify, locate, report, and disseminate CBRNE/TIM hazard information to affected and non-affected personnel. Sufficient timely and accurate information to commanders at all levels through early and direct

warning capability is crucial so they can assume appropriate protective postures and develop options to continue operations. CBRN information systems enable the Soldier to perform hazard analyses, operational effects analyses, and warning reports.

(b) Current warning and reporting capabilities are not networked-enabled with ABCS. Limitations with current databases will not allow interfacing with the geographical information system (GIS) to provide input to the COP to give a clear and accurate picture of all CBRNE events/attacks/hazards in real-time. Limitations also exist in global systems communicating with each other through cooperative linkages. Since no linkages currently exist between various detection technologies (such as, biological integrated detection system, phased array radars, stand-off motion detectors, passive monitors, vehicular embedded detectors with global positioning system linkages and automatic position reporting, individual detectors networked to centralized data servers, etc.), no cooperative CBRNE/TIM detection policies are required and the limitation still exists.

(4) *Information*

(a) Current information *assess* capabilities include the ability to assess network availability and operational status, and the ability to assess availability of the electromagnetic spectrum. Limits of these capabilities are the same as those discussed in *detect*.

(b) In addition, these capabilities require time consuming human intervention and analysis which causes delay in alerting users to potential threats to the network.

(5) *Electronic*. There are no current systems or capabilities that *assess* electronic targeting of ground units or platforms.

(6) *Intelligence*

(a) Intelligence capabilities provide the unit commander the assessment of threat capabilities and operations across ROMO. These capabilities include the ability to recognize, classify, and identify detected elements and report on their activities. Others require that analysts receiving the sensor data or report to determine the identity and activity of the detected element. Analysts will fuse incoming sensor data and reports to create a picture of the threat activity in the protected unit's area of interest or AO.

(b) A current problem in Operation Iraqi Freedom/Operation Enduring Freedom is the sharing of information and communicating SA to the right echelon when needed. Problems consist of separate analytical centers and collectors not linked and not able to collaborate adequately. There is a need to evolve into a collaborating environment and to link collectors and sensors to analytic centers. Joint intelligence operations capability-Iraq (JIOC-I) was developed to meet these multi-national force Iraq requirements. The JIOC-I concept is described in figure 4-2.

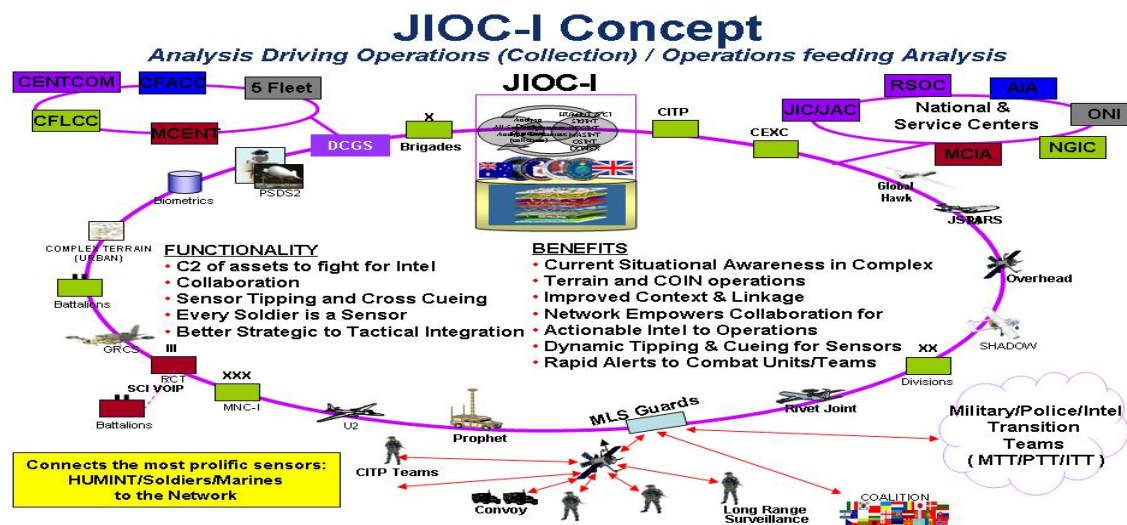


Figure 4-2. JIOC-I Concept

(c) Analytical Tools

(1) The JIOC-I system was developed to simultaneously share intelligence across all echelons, down to dismounted Soldiers on patrol. JIOC-I provides advanced applications and a fused data repository to enable dynamic knowledge production and dissemination, and thus better use of existing information. This shared intelligence system consist of state-of-the-art data ingestion and network-centric services to handle high data volumes and refresh rates for a coherent ISR picture.

(2) JIOC-I functionality and systems/processes this concept enables are-

- **Functionality:**
C2 of assets to fight for Intelligence.
Collaboration.
Sensor tipping and cross cueing.
Every Soldier is a sensor.
Better strategic to tactical integration.

- **Enables:**
Current SA in complex terrain and counterinsurgency operations.
Improved context and linkage.
Collaboration for actionable intelligence to operations.
Dynamic tipping and cueing for sensors.
Rapid alerts to combat units/teams.

(3) MASINT: Uses of state-of-the-art technology processing to detect, identify, and assess enemy capabilities and intentions. PPS-5D (ground surveillance radar) (SBCT

surveillance troop), remotely monitored battlefield sensor system (BCT MI company, SBCT surveillance troop).

(4) Counterintelligence and Human Intelligence. Counterintelligence and Human Intelligence Automated Tool Set (CHATS) (AN/PYQ-3 (V)). The CHATS is the mobile CI/HUMINT and document exploitation team leader's automation device. It consists of commercial off the shelf and government furnished equipment enclosed in cases that conform to most airline checked baggage standards. The system is composed of a laptop computer with internal power management capability, printer, scanner head, digital camera, precision lightweight global positioning system receiver, cables, and adapters to ensure ease of use in different environments.

(5) The counterintelligence and human intelligence automated management system (CHAMS) software provides users with the capability to collect, manage, receive, store, and export text, electronic data and digital imagery information, as well as to prepare, process and disseminate standard messages. It will transmit messages and data to the all source analysis system (ASAS) light, counterintelligence/interrogator operations workstation (CI/I Ops WS), individual tactical reporting tool (ITRT), and appropriate MP units. It is capable of communicating through the Army common user system (ACUS), intelligence electronic warfare (IEW) special purpose communications, and combat network radio (CNR) systems. The CHATS is accredited to operate at the secret level. The only shortfall would be that not all units use the system due to command preferences, however the classification is not a shortfall, the information can be shared.

(6) CI/I Ops WS, (AN/PYQ-7 (V) 1). The CI/I Ops WS is a BDE level and higher information management system designed to correlate and analyze intelligence sent to it from CI and HUMINT Soldiers using the CHATS and ITRT. It provides automation support to operational elements of military intelligence units with organic counterintelligence and interrogation assets and to the CI staff officer of the intelligence staff at division and above. CHAMS software will support the intelligence staff in performing database processing, message processing, intelligence preparation of the operational environment, situation display, operation order preparation, collection management, COA development, secondary imagery dissemination, and common applications. The CI/I Ops WS interfaces with the ASAS remote workstation, the ASAS CI/HUMINT single source workstation, the CHATS, and the ITRT. It is capable of communicating through ACUS, IEW special purpose communications, CNR, and through emerging Army communications systems. The CI/I Ops WS is accredited to operate at the secret level.

d. Decide

(1) Currently there are more than 150 C2 systems that don't easily facilitate joint operations or net-centric operations. Stove piped systems severely limit the capability to interact and collaborate in support of military operations. This limited access to products hinders the capability to search or browse databases and perform comparative analysis to rapidly and accurately support the commander's decision. The elimination of stove piped information systems will truly facilitate information becoming a real-time network centric enabler.

(2) By creating applications that meet the Soldier's demands for information sharing, a powerful tool to aid the commander in C2 decisionmaking is realized.

e. Act. The following section describes current act capabilities against adversary air, ground, CBRNE, information, electronic, and intelligence threats. These capabilities include the sub-functions of warn, and active and passive protection measures.

(1) *Air*

(a) Warning of an impending air threat is critical in protecting the defended asset and enhancing survivability of protected forces. Even a few seconds of warning against the RAM threat has shown a significant improvement in force survivability. Warning starts with the detection of the air threat, the assessment of which areas will be affected by the threat, a determination of protection required for that asset (some assets are more vulnerable to the air threat than others), and the accurate and timely dissemination of the warning to the affected area(s). It is imperative only the affected areas are warned, that the warnings are timely and accurate, and the false warning rate is minimal. Current AMD capabilities include the ability to defend against a small subset of the air threat. From a ground missile defense perspective, only a few radars are currently able to track long-range/intercontinental threats, and the ability to intercept these threats has not been successfully demonstrated. Current AMD forces can successfully defend against the short-range ballistic missile threat in a non-saturation attack. Current capabilities also focus on the ability to defend against the TBM threat or non-TBM threat, but not both simultaneously in an effective manner.

(b) The ability to attack and destroy the enemy's launch platforms prior to launch has not been effectively demonstrated during recent conflicts. Against the RAM threat, current AMD forces have demonstrated a limited capability to destroy the RAM threat in flight and alert ground forces of enemy RAM activity, thus preventing initial or follow-on RAM launches. The inability to effectively coordinate engagements with the JFs can lead to multiple engagements against the same threat platform which may cause the threatening RAM to go unengaged and / or causes missile wastage.

(2) *Ground*

(a) Current ground warning systems are stand-alone and, therefore, not integrated to provide a seamless protection system. Current explosive hazard warning systems consist of manual means and marking systems, based on mine field marking kits, local doctrine and standard operating procedures. The current warning doctrine to warn all parts of the unit is executed by data collection and daily operation orders. Maneuver control system allows the unit to input data gathered from the field and virtually mark any hazards, be it explosive or non-explosive. Once this data is entered, it is available to any units or echelons of the unit that have access to that unit's maneuver control system data. Other warning systems consist of actual marking systems based upon the universal mine field marking system, which is recognized across the JF. Current ground systems utilize active and passive measures in order to deter, deny, prevent, intercept, attack, or neutralize hostile actions.

(b) Today, the capability to prevent and counter the threat is severely limited due to technology and manning constraints. Active measures are manpower intensive most often include employing Soldiers to engage and defeat an activity in order to protect personnel, assets, and information. This takes Soldiers away from duties and mission; impacting their functional mission set that must be performed on the battlefield. Commanders are driven to this solution as they lack a fully integrated, intelligent, precise system of protective lethal and nonlethal effect capabilities. Passive defense measures are executed in order to deter, deny, prevent, and anticipate an adversary's attack.

(c) There are solutions, (such as integrated commercial intrusion detection system, access control package installation), that have been built to improve physical security with a design theme utilizing technology to avoid manpower constraints. However, generally, most of these solutions are heavy, manpower intensive, and do not provide the optimum stand-off capability to enhance UP capabilities. The ability to defend the ground threat provides the unit with the means to quickly dominate terrain, modify the physical environment to isolate enemy forces, deny key terrain and impede, deny, or canalize enemy movement. This protects friendly forces and their freedom of action while placing enemy forces in positions of disadvantage. Current forces utilize construction equipment to create berms and barriers, emplace mine fields, create fighting positions, and utilize an array of visual, motion, and seismic monitors to monitor cleared areas, execute hostile actions to deny enemy use of areas/facilities, fix enemy forces, disrupt enemy operations, and shield friendly forces.

(3) *CBRNE*

(a) *CBRNE act* focuses on active and passive measures to deter, prevent, and deny enemy actions. Active measures include WMD interdiction and elimination which takes away current and future use of CBRNE weapons and capabilities that could be used against U.S. forces and allies. ISR and CBRN information systems allow commanders to make decisions to *act* against CBRNE and TIM agents and hazards. Protection provides life sustain and continued operational capability in a contaminated environment. Once the commander decides to *act*, CBRNE protection occurs in the areas of individual and collective protection. Individual protection currently protects Soldiers against CBRNE warfare agents; however, technological advances can provide improvements to reduce the physiology burden of wearing protective equipment, extended durability, and reduce heat stress burden, which all cause reduced levels of performance. Individual protective equipment (IPE) provides individual protection from CBRN/TIM hazards by the proper use of masking devices (respiration and ocular) and wear of protective gear and clothing (percutaneous).

(b) Collective protection (air purification and shelter) is primarily used for transportable and fixed site application. Current capabilities are bulky, difficult to enter and exit, logistically intensive, and not available in the necessary quantities. Passive defensive measures include protecting equipment and supplies through the use of protective coatings, such as conformal coatings for electronics, chemical agent resistant paints for equipment, and chemical resistant packaging for supplies. *CBRNE act* also provides safe, efficient, and consistent collection and handling of all CBRNE/TIM samples, including those taken from personnel following exposure. Warning occurs during the *act* stage, and timely warning is critical to success and survivability.

The nuclear, biological, chemical, warning reporting system is the current system. As programmed, the joint warning and reporting network (JWARN) is a suite of hardware and software that should, once fully operational, provide adequate capability from a CBRNE information systems ISR standpoint. Until JWARN is fully operationally capable, limitations to CBRN information systems and processes include manual data receipt and entry, limited interface with COP, restricted information flow into the global C2 system, and limitations to real-time SA.

(4) *Information*

(a) Information *act* capabilities protect systems and information in storage, during processing, and transit from unauthorized access or modification. They also deny service to unauthorized users. Current capabilities include the ability to physically and electronically shield systems and information, and the ability to protect information while in transit or storage. These are primarily commercial applications are hardened and meet current military standards for encryption and information security.

(b) The conditions that limit these capabilities are outlined in information *detect* and information *assess*. Current information *act* capabilities used to warn users include the ability to broadcast warnings to users both manually and automatically, but are limited by the same conditions outlined in information *detect* and information *assess* capabilities.

(5) *Electronic*

(a) Current electronic protection *act* capabilities protect systems by hardening internal electrical components that may be exposed to EMP. Current capabilities also include counter IED devices used to jam or electronically detonate IED hazards.

(b) Future electronic protection *act* capabilities must serve as active protective systems that detect and then react to an electromagnetic spectrum EA threat.

(6) *Intelligence*. The intelligence capabilities will provide timely warning on enemy trends, intent, and activities.

(a) Analysis and Dissemination. Analysis capabilities include-

(1) Intelligence analysis personnel and ASAS at the BCT, SBCT, and MI BN. Technology has not reduced the fog of war. Analysts leverage national, theater, and tactical reporting to rapidly establish threat association and linkages; recognize threshold events, activity patterns, and anomalies; and within the continuing increasing volume of collected material understand the significance of information buried within the increasing amount of information.

(2) IMINT. Tactical exploitation system and the extended range multi-purpose UAV provides airborne IMINT with near real-time capability; it is day or night capable at extended ranges; provides persistent intelligence gathering capability (constant ISR).

(3) CI/I Ops WS, (AN/PYQ-7 (V) 1). The CI/I Ops WS is a brigade and higher level information management system designed to correlate and analyze intelligence sent to it from CI and HUMINT Soldiers using the CHATS and ITRT. It provides automation support to operational elements of military intelligence units (with organic counterintelligence and interrogation assets) and to the CI staff officer of the intelligence staff at division and above.

(4) CHAMS software will support the intelligence staff in performing database processing, message processing, intelligence preparation of the operational environment, situation display, operation order preparation, collection management, COA development, secondary imagery dissemination, and common applications.

(5) The CI/I Ops WS will interface with the ASAS remote workstation, the ASAS CI/HUMINT single source workstation, the CHATS, and the ITRT. It is capable of communicating through the ACUS, IEW special purpose communications, CNR, and emerging Army communications systems. The CI/I Ops WS is accredited to operate at the secret level.

(6) ITRT, (AN/PYQ-8 (V)). The ITRT is a portable, automation tool that provides counterintelligence and interrogation team Soldiers the capability to collect, process, and disseminate tactical intelligence information obtained through investigations, interrogations, collections, operations, and document exploitation. The ITRT is the entry level device into the counterintelligence and human intelligence automated collection and reporting systems architecture. Its primary function is to report intelligence of immediate tactical value to other reporting systems by direct local area network connection, CNR, or ACUS. This is accomplished through use of commercial and government furnished software designed to receive, process, and store formatted messages, digital maps, and digital imagery. The ITRT is accredited to operate at the secret level. Future developments may include a personal digital assistant. The ITRT provides the HUMINT collector SA and the ability to send real-time information.

(7) Biometric automated technologies/counter human deception detection. Advances in technology, especially in biometrics (physiological, neurological, thermal analysis) will enable future CI agents and HUMINT collectors to more accurately identify not only personnel for identification purposes, but will provide various types of signatures regarding indicators of deception.

(8) Related technological advances in information systems will provide Future Force CI and HUMINT with automated analysis and data sharing, in order to assist in identifying deception in subjects scrutinized for intelligence purposes (such as screening, investigations, source vetting, and collection).

(9) CHDD will surpass current polygraph techniques for measuring physiological signatures/indicators and the associated subjective analysis and evaluation. Additionally, these same technologies will develop physiological signatures which can be entered and tracked through biometric devices/databasing. This will aid in identification, tracking, and stand-off detection of personalities of interest whose profiles exist.

f. Recover. The following section describes current recover capabilities against adversary air, ground, CBRNE, information, electronic, and intelligence threats.

(1) *Air*. Current AMD forces have the ability to quickly reconstitute and reload missile launchers in preparation for additional air attacks against protected assets and friendly forces. The maintenance procedures and processes are in place to ensure minimal down time of equipment, and repair processes are in place to quickly bring equipment back to ready state as soon as practical and possible.

(2) *Ground*. Ground protection elements provide material and equipment to fulfill the requirements for replacing and repairing ground protection capability. These capabilities include the constructional equipment to create barriers, harden facilities, and re-establish the ground sensor systems as required.

(3) *CBRNE*

(a) Current military forces have a limited ability to reconstitute combat power and resources to full operational functionality. Plans and coordination for mission execution of decontamination not only include personnel and equipment (personal, weapons, vehicles, etc.), but also terrain and strategically significant facilities. Logistics procedures (supply, maintenance, transportation, and storage) must be constantly assessed to support decontamination operations. Materials used for equipment decontamination are super tropical bleach, high test hypochlorite, and the M100 Sorbent Decontamination System. Existing capabilities rely upon the physical application and rinse of decontaminants on contaminated surfaces. Existing systems are effective against a wide variety of agents, yet are slow, labor intensive, and present logistical, environmental, material, and safety burdens. Existing systems are also inadequate for sensitive equipment decontamination, deficient for large area, port, and airfield decontamination, and rely on water or bleach based aqueous systems.

(b) Currently, standards have not been established to determine "how clean is safe." Once a standard is set it would enable contaminated equipment and remains to return to the U.S. by transiting through other allied and friendly nations to the continental U.S. and be in accordance with the Occupational Safety and Health Administration and the National Institute for Occupational Safety and Health standards.

(4) *Information*. Current recover capabilities include the ability to manually (and to a limited degree automatically) reroute failed major network nodes and backup stored data manually or automatically at predetermined intervals. Current fielding levels of these capabilities, the number of separate non-interoperable systems, and unit "home grown" solutions do not provide the level of resilience or redundancy to guarantee an acceptable recovery of critical data or reestablishment of connectivity in the event of catastrophic failure. These capabilities are also limited by those conditions outlined in information *detect* and information *assess*.

(5) *Electronic*. There are no current systems or capabilities to *recover* from electronic attack of ground units or platforms.

(6) *Intelligence*. These ISR systems enable and support the unit protection.

(a) The Army Joint Surveillance Target Attack Radar System (JSTARS) Common Ground Station. JSTARS common ground station can receive, process, store, disseminate, and display radar data from the joint Air Force/Army JSTARS. JSTARS consists of a multi-mode radar on an Air Force E-8 aircraft and a surveillance control data link, which connects the air and ground stations. This radar system provides a near real-time radar display of the deep and wide “ground pictures.” Radar data provides the aircrew workstations and Army ground stations with moving target indicators, fixed target indicators, and synthetic aperture radar images. In the Army ground stations, signal intelligence reports from the integrated broadcast service intelligence networks, and imagery products and telemetry data from select UAS and Air Force airborne collection systems supplement this JSTARS radar picture. Collectively, these provide the Army commander an enhanced ability to conduct targeting, battle management, and intelligence reporting.

(b) The Joint Tactical Terminal. Joint tactical terminal is a key battlefield weapon system component for the reception and dissemination of threat warning and situation awareness information to support that warfighter during all levels of operations. Although not designed to engage targets, it provides access to key broadcast intelligence networks, thereby enabling commanders to accomplish assigned peacetime and wartime missions.

4-2. Spiraling Current Capabilities

a. This section describes current plans or determines if no plan is present for the spiraling of current capabilities to future optimum capabilities to support UP objectives outlined in this CCP. These capabilities are described in the *detect, assess, decide, act, and recover* UP functional context.

b. Detect. The following section describes spiraling plans for *detect* capabilities against adversary air, ground, CBRNE, electronic information and, intelligence threats.

(1) Air

(a) AMD systems will continue to use deployed ground and space-based sensors to detect the launch of ballistic missile from threat regions, cruise missiles, UAS, ASMs, RAMs, as well as the residual capability to detect FW and RW aircraft. The AMD capability will be greatly enhanced with the deployment of very accurate radars located on elevated platforms to overcome the limitations of line-of-sight and terrain. These radars will detect small radar cross section aerial platforms and support the engagement of the threat platforms out to the kinematical range of the AMD interceptors. The sensors aboard the elevated platforms will also provide 360° detection of cruise missiles, UAS, and FW/RW aircraft, thus overcoming some of the limitations of sectorized radars against this threat set and providing for continuous tracking of all aerial platforms (friendly and hostile) throughout the flight of the platform.

(b) The ability to detect short-range, medium-range, intermediate-range, submarine-launched, and intercontinental ballistic missiles from space-based sensors beyond the ascent and

boost phase of the ballistic missile's flight will be enhanced with the deployment of highly accurate space-based sensors and improvements to prediction algorithms. There will still be limitations in detecting the ballistic missile threat from 360° since the sensors used to detect the SRBM and MRBM threat will still be sectorized. The ability to detect an increased number of RAM launched at static and mobile protected assets will be greatly improved over the current capability and will include multi-purpose radars capable of detecting larger numbers of RAM while supporting counter-battery and air traffic control missions simultaneously.

(2) *Ground*

(a) The family of rapid response equipment (FIRRE) gives commanders an additive, modular, tailorable system of protection systems that provides the ability to configure the sensors and response system to the environment and threat target set increasing unit protection capabilities. FIRRE provides commanders an integrated force protection COP and C2 capability. Advance security technologies are the center piece of FIRRE. FIRRE will integrate with a unit's basic force protection capabilities providing a layered, seamless ground defense. This "systems of systems" approach will provide the SU necessary to make decisions faster and more accurately so the correct level of force, both lethal and nonlethal, can be applied to counter an enemy threat. FIRRE will reduce false and nuisance alarm rates and distinguish friend from enemy.

(b) Detection and assessment equipment will have to cover large land areas in all weather environments and will incorporate remotely operated sensor platform to include robotic and unmanned aerial systems. FIRRE supports a defense in depth by providing means to detect, assess, decide, and assist in deployment of graduated responses/scaleable effects to include security forces to defeat intruders. Intelligent mine system (IMS) and Spider technology (system software), give the commanders an integrated working tool which gives a constant detect capability along with protect and assess. The data gathered from the IMS can give the commander a picture of the hostile intent, the hostile capabilities, and if needed, the means to eliminate the threat by employing the munitions. Spider technology gives the commander a means to employ an array of sensors and protective munitions that can detect hostile and enemy movement on any perimeter or corridor. Smaller robotic platforms are being developed to give units the ability to search, detect, and mark explosive hazards, non-explosive hazards, and hostile intent, and will then be able to send this data to the information systems ISR.

(c) A family of clearance vehicles is being spiraled into the Future Combat System (FCS) program that can detect IEDs and other explosive hazards using stand-off, semi-autonomous, and autonomous methods. These vehicles will be airborne stand-off mine detection system platforms, ground stand-off mine detection systems, and handheld stand-off mine detection systems for hand-held or small robotic platform applications.

(d) FCS Spin-Out 1 includes two systems contributing to detection; the unattended ground sensor (UGS) and the IMS. UGS will enhance the commander's decision process and SA by incorporating operational environment sensing (from platforms, drones and forces) into operations planning and execution. Military operations on urban terrain and urban advanced sensor system UGS provides the heavy BCT commander an enhanced intelligence picture

through early warning, SA, and force protection in urban environments. The urban advanced sensor system UGS provides remote monitoring and warning capability for the current force small unit (platoon) in an urban operations terrain environment, such as tunnels, caves, sewers, structures, and inside of buildings. ISR UGS provide a recoverable, persistent sensing capability assisting the commander in attaining SU of the operational environment. The system is tailored to mission requirements and is hand-emplaced by a Soldier.

(e) ISR UGS provides the heavy BCT commander a sensing asset capable of monitoring vehicle traffic, foot traffic, and radiological/nuclear agents. The IMS primary purpose is force protection by providing antipersonnel and anti-vehicle protection while monitoring designated areas. IMS, with its integrated sensors/munitions, provides over watch of known enemy forces and potential routes that could interfere with friendly maneuver. It can engage, isolate in place, and prevent reinforcement of enemy forces. IMS provides a proactive means for the unit commanders to shape the operational environment, support the scheme of maneuver, and provide acquisition for fires.

(3) *CBRNE*

(a) Technology will continue to use intelligence and ground based systems, to detect CBRNE in land, water, and air. In the future, many fielded detectors will detect, quantify, and classify most, if not, all chemical warfare agents and some TICs. A number of sensor technologies are being optimized while alternative detection technology matures. Mid-term technologies are focused on developments to improve tactical detection and identification capabilities for both chemical and biological warfare agents. Technologies in improved chemical point detection will have the characteristics including all agent programmable automatic point detection, portable monitors, and miniature detectors for aircraft interiors, and wheeled and tracked vehicles. The joint chemical agent detector is an example of this family of improved point detectors.

(b) Another capability will be improved biological point detection. The joint biological detection point system will increase numbers of agents detected with increased sensitivity, offer lower false-positives, and its design will be smaller and lighter with increased reliability. Improved stand-off detection will be realized in CBRN reconnaissance and chemical biological remote/stand-off detection through the joint Service lightweight stand-off chemical agent detector increment I/II, joint Service nuclear, biological, chemical reconnaissance system P3I, and the joint biological stand-off detection system block I.² Gas toxic Draeger kits, joint Service lightweight stand-off chemical agent detector, and joint chemical agent detector will likely remain the main capabilities to detect TICs. The nuclear, biological, chemical reconnaissance vehicle along with the joint modular chemical biological detection system will provide an integrated chemical/biological detection, identification, and quantification capability and is expected to rapidly and reliably detect, identify, and quantify most chemical warfare agents and some TICs.

(c) Chemical, biological network warning system will combine point/stand-off detector systems and surveillance systems allowing detection of chemical filled munitions before impact.

² Blocks I, II, and III are terms used in the concepts/requirements COP to define increment delivery periods.

In addition the Chemical Corps is currently attempting to leverage UAS capabilities for CBRNE detection in the mid-term. Many detectors will not detect aerosols and agent concentrations that are expected to cause low level effects. Many detectors also will not have the capability to take samples for future analysis. There is no current plan to improve radiological detection capabilities.

(4) *Information*

(a) The DOD employs an information protection sensor grid to monitor DOD networks and detect potential information attacks against system vulnerabilities. The grid is a coordinated constellation of intrusion and anomaly detection systems (owned and implemented by various entities) deployed throughout DOD information systems and computer networks. The sensors report back to Service, theater, and joint information protection service providers. LandWarNet, as the Army's contribution to the GIG, must be part of the information protection sensor grid.

(b) Key enablers to this end will be the continued transition from separate stove pipe networks to a single Army network, the maturity of Army network operations (NETOPS) procedures and capabilities, and the ability to keep pace with technology. The joint network node to warfighter information network-tactical (WIN-T) migration strategy will provide the Army with the means to migrate away from separate networks, initially as a federation of networks. With the fielding of WIN-T capabilities, a single comprehensive Army network capable of synchronizing detection capabilities through automated NETOPS reporting down to the tactical platform level is achievable. The current strategy to transition from the current networks in order to set the stage for WIN-T technology is represented in figure 4-3.

	JNN	WIN-T (incremental)	WIN-T (future)
Network Capability	Better Capacity; retain Stovepipes	Improved Capacity; Integrates stovepipes	Improved Capacity Imbeds all systems into one platform
Mobility	No OTM Hours to Install (ATQH)	OTM Minutes to Install	Formations OTM
Operational Reach	Spts Distributed Ops Single point of failure Commercial SATCOM	Spts Distributed Ops Dynamic networking	Supports Fully Mobile Distributed Ops
Network Operations (NETOPS)	Not integrated COTS tools Complex management	Initial Integrated CDR's Intent into Policy Assured delivery	Integrated Assured Delivery OTM
Network Agility / Task Reorganization	Improved Agility Intervention Required To Enable Network Services	Dynamic Reorganization at all echelons ATIH: Agile Peer based	Dynamic Reorganization OTM
Level Of Support	BN HQ ATQH	BN OTM—(CO OTM Option)	CO OTM (PLT FCS)
Joint Interoperability	Joint at BCT	Joint at all CPs	Joint down to Company
Support to BC	Rigid System; Task Org Change difficult	Auto configure; support BC systems OTM/ATIH	Auto configure; support BC systems OTM/ATIH

Figure 4-3. Setting the Stage for WIN-T

(5) *Electronic*. Currently no plan exists regarding the spiraling of current electronic *detect* capabilities to future optimum capabilities.

(6) *Intelligence*

(a) HUMINT. Collectors (BCT and SBCT MI company, division MI BN, and theater intelligence brigade).

- CI elements will be capable of providing an agile, tailored, interoperable network of human sensors (CI elements and developed contacts), that contribute to the SA in the operational environment. CI forces may corroborate other intelligence discipline information, as well as cue other intelligence assets through the CI core competencies and technical services. The CI core competencies are collection, investigations, operations, analysis, and production. CI technical services include computer network operations, technical surveillance countermeasures, and CHDD. Future CI will focus on combating the significant adversarial intelligence threat targeting Future Force personnel, plans, operations, activities, technologies, and other critical information and infrastructure. CI organizations will be flexible, and capable of split based operations.

- HUMINT will be focused on and dedicated to the collection of data and information to ensure the commander has the best picture of the adversary and the environment. HUMINT collection will contribute to the development of SU through the screening, interviewing, questioning of indigenous persons, debriefing of friendly forces, tactical questioning, elicitation, surveillance detection, interrogation of detained persons (to include enemy prisoners of war), and the exploitation of multimedia. HUMINT will interface with other entities, for example, counterintelligence, MP, long-range surveillance, civil affairs, and psychological operations. Future Army HUMINT organizations and operations will be tailorable and flexible, manned and equipped with modular, scaleable, interoperable, and deployable teams and systems capable of deploying in the first lift. HUMINT collectors and systems will be tailored for split based, remote, and on the move operations. HUMINT operations must be capable of rapid inter-Service integration in support of joint, combined, and coalition operations.

(b) ISR assets require the flexibility to detect a wide range of emerging threats. While the ability to detect conventional military threats remains important, the ability to address the asymmetric, non-conventional threat gains importance. Tracking the location and activity and predicting the intent of individual threats is a new challenge at the tactical echelon. The following are future enhanced capabilities to address the future environment and will aid in the execution of the UP *detect* function.

- IMINT: Shadow Tactical UAS (SBCT MI company), division extended range multi-purpose UAS, Buckeye, JLENS, Mohawk MI system.
- MASINT: UGS.

c. Assess. The following section describes spiraling plans for *assess* capabilities against adversary air, ground, CBRNE, information, electronic, and intelligence threats.

(1) *Air*

(a) Improvements to space-based sensors and the algorithms used to predict TBM impact points and launch locations will significantly enhance the ability to assess the ballistic missile threat and provide support for attack operations and active/passive defense operations. Enhancements to sensor technologies to include non-cooperative identification and body and wingspan measurements will enable higher probability of correct classification and identification of aerial platforms. The netted and distributed architecture available during this timeframe and the enhancements to communications systems (bandwidth, speed of service, data quality, and completion rates) will enable the AMD systems to provide accurate assessments and recommendations to the AMD Soldier.

(b) Assessment limitations will still exist in the form of JIM ambiguities, as well as the enemy's attempt to morph and refine the asymmetric threat. There will always be a challenge to assess the threat's intent and to get inside the enemy's decision cycle, and the development and deployment of automated decision aids will go a long way in enabling this capability.

(2) *Ground*

(a) FIRRE provides an electronic means of accomplishing area intrusion detection, alarm reporting, display, and tracking, remote alarm assessment, and computer alarm assessment. FIRRE assessment capabilities provide the system operator automatic and manual controls necessary to make rapid and accurate assessments of sensor alarm indications in an effort to determine friend or enemy. FIRRE also provides the ability to use the mobility of unmanned vehicles to see and survey areas that have limited visibility or coverage by other sensor systems.

(b) Geospatial information provides the foundation upon which all other operational environment information is layered to form the COP. Geospatial information and services provides the JFC with current and actionable operational environment environmental data, collaborative decision support, and terrain analysis tools compatible with the network-centric environment. Geospatial information and services help the commander visualize the operational environment, effectively plan and execute the full ROMO, navigate, and accurately target the adversary. This capability provides the commander to platform level with real-time geospatial information and products (such as a modified combined obstacle overlay (MCOO) tied to a running mobility estimate). The separate operational level topographic battalion engineer company (echelons above corps) and the corps topographic engineer company is assigned to a topographic engineer battalion.

(c) The separate topographic teams include the topographic planning and control team; the topographic terrain direct support team, heavy division; the topographic terrain analysis team, heavy division; the topographic detachment, Force XXI Division; and the topographic terrain analysis team, light division. Each team is organic to their designated division and provides qualified personnel who collect, evaluate, and disseminates terrain data. Topographic capabilities are further enhance by producing terrain intelligence, as well as analyzing the effects of the terrain on military operations.

(d) ISR information systems assess data by inputting information into maneuver communications systems. This data can then be analyzed to determine hazardous areas, explosive hazards, and cleared or neutralized areas. The disadvantage of this system is the data has to be loaded into the system at the HQ level, after it has been gathered from lower echelon units, and thus increases the possibility the data may not be real-time.

(3) *CBRNE*

(a) In the future, improved warning and reporting will be possible via a network (JWARN block II/III). Improvements in hazards analysis will be realized given a robust network of integrated sensors and expert systems, such as the high altitude intercept analysis post engagement effects model, urban environment analysis, and the chemical, biological network warning system. The network warning system will integrate disparate sensor information to build a picture of a possible CBRN event, and it continues to improve assessment confidence as it complies and integrates more information.

(b) New databases will be needed to interface with the GIS to provide input to the COP to provide a clear and accurate picture of all CBRNE events/attacks/hazards in real-time. Automated field CBRNE intelligence systems will need to accept manual and automatic CBRNE/TIM event data input, and must be able to modify, retrieve, display, archive, and transfer data (such as intelligence, location of attack, source and sensor information) to repositories. In addition, these capabilities will need to interface with standard information systems ISR to effectively and rapidly accomplish threat assessments. These databases and intelligence system capabilities are continuing to be explored.

(c) Predicting and tracking CBRN/TIM events will be captured in the anticipated initial operational capability of the joint effects model Block I in FY2006, and the initial operational capability of the joint operational effects federation (JOEF) block I, increment I in fiscal year 2008. The joint effects model will provide a single, validated capability to predict and track CBRN and TIM events and effects. The JOEF will provide an operational requirements modeling and simulation system which accurately predicts CBRN effects on personnel, equipment, and operations. The JOEF will consider pertinent aspects of CBRN/TIM immediate and long-term health hazards and permissible exposure limits.

(4) *Information*

(a) Assessing and understanding the nature of an adversary cyber attack requires the ability to quickly and accurately determine the characteristics of the attack, including criticality and vulnerability of the systems against which an attack is directed, source of the attack, and purpose of the attack. By comparing the current attack characteristics to previous attacks and coordinating with other information protection providers to learn if they are similarly affected, a JFC gains understanding. A rapid assessment and employment of state-of-the-art event correlation and data reduction tools are critical to providing the JFC with predictions about the attack's effects on DOD networks and the operational impact on the JFC's courses of action.

(b) Until WIN-T has achieved full functionality across the force to automate the majority of NETOPS functions, the migration to a single comprehensive network will enable deployed organizations that are responsible for NETOPS to quickly pass critical information through the NETOPS reporting chain for assessment and action. Modular force design implementation will provide Soldiers trained with the necessary skills for assessing electronic attack of the deployed force's network and systems. These Soldiers will require a high level of technical knowledge to perform these complex tasks. The ability to provide the necessary training for these specialties will be provided through LandWarNet University.

(5) *Electronic*. There are currently no plans to spiral systems or capabilities that *assess* electronic targeting of ground units or platforms.

(6) *Intelligence*

(a) CI and HUMINT. Using reach systems, such as the distributed common ground system—Army (DCGS-A) will access theater, departmental, and strategic knowledge centers to satisfy their information requirements and report in real-time or near real-time size, activity,

location, unit, time, equipment, priority intelligence requirement and early warning of imminent hostilities data. Systems must be able to perform source and initial information analysis and have the communications capabilities to receive and pass data including digital imagery to analysts, consumers, and other HUMINT collectors in real-time and on the move.

(b) CI and HUMINT elements will require a centralized DCGS-A -like database that can be accessed at all echelons for collaborative information sharing. This National database requires gateways for information exchange by CI elements at all echelons. The database will contain multiple product libraries for text reports, scanned documents, photographs, video, and fingerprints. It will contain search engines and will cross reference related data between individual and multiple product libraries. The database will also have a restricted library that serves as a central source registry for CI and HUMINT sources and an operational reports archive.

(c) The source library will only be accessed by specified CI special agents, (such as the counterintelligence coordinating authority, CI staff officer or HUMINT staff officer on staff, and HUMINT operations cell personnel who serve in source management positions). The source library will be protected by user permissions or other security protocols to eliminate unauthorized access. The database will also contain a reference library containing all applicable intelligence directives, joint publications, service specific regulations, and doctrinal manuals. Multi-level and layered security will ensure exchange of information at different classification levels that produces system commonality and reduces equipment requirements.

d. Decide

(1) The ability of commander, staff, and Soldiers to decide, task, and monitor the operational environment will continue to develop through initiatives to integrate in the objective BCS, JC2 or FCS. The efforts will continue to build service oriented architecture, a network-centric environment, and migration to few integrated systems.

(2) Current roadmaps how battle command will spiral and develop into the BCSs of the future are depicted in figures 4-4 and 4-5.

e. Act. The following section describes spiraling plans for the act sub-functions of warn, and active and passive protection measures for capabilities against adversary air, ground, CBRN, information, electronic, and intelligence threats.

(1) *Air*

(a) Warning of TBM launches to the affected areas will continue to improve based on higher fidelity sensors and improved prediction algorithms. Warning of the individual platform or Soldier will enhance the friendly force survival rate and minimize loss of equipment and assets. Significant improvements to the warning of the RAM threat will also enhance the survivability of forward operating bases, as well as the capability to warn the force when in convoy operations.

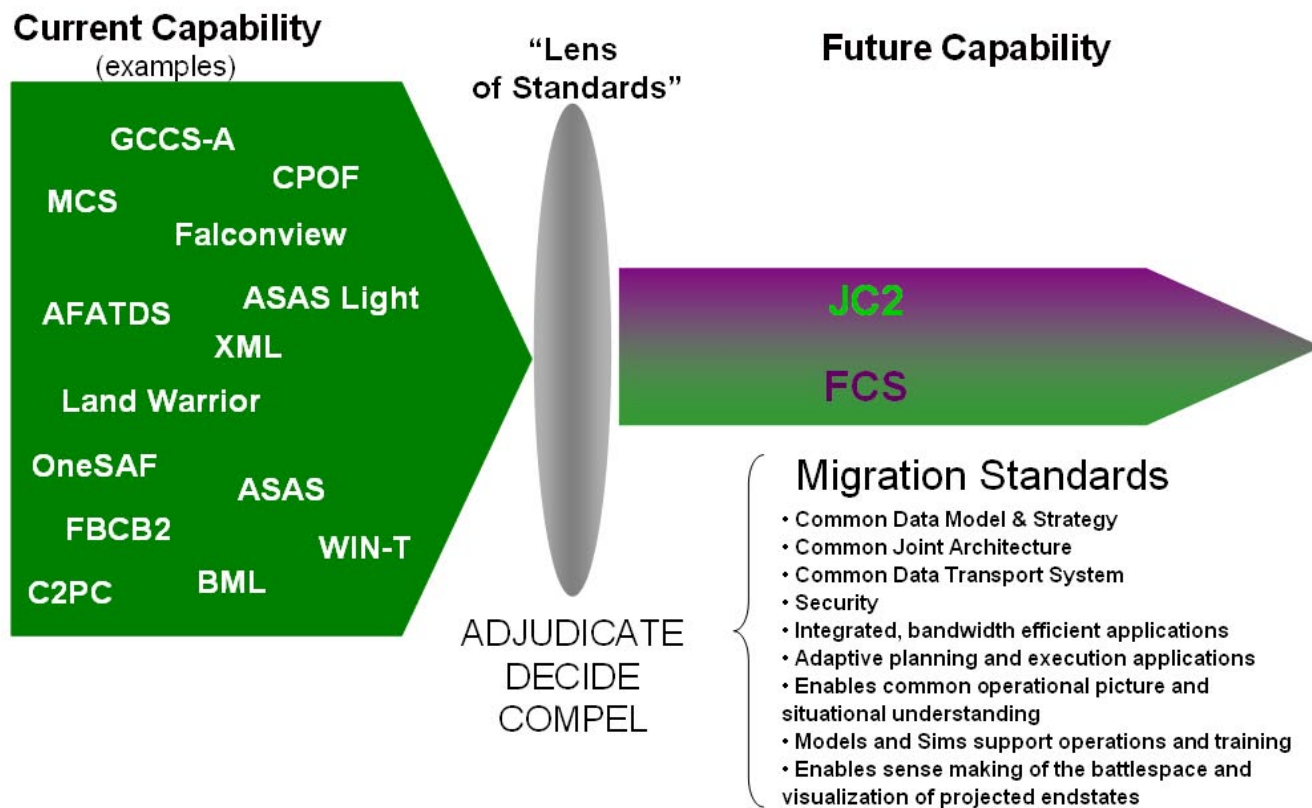
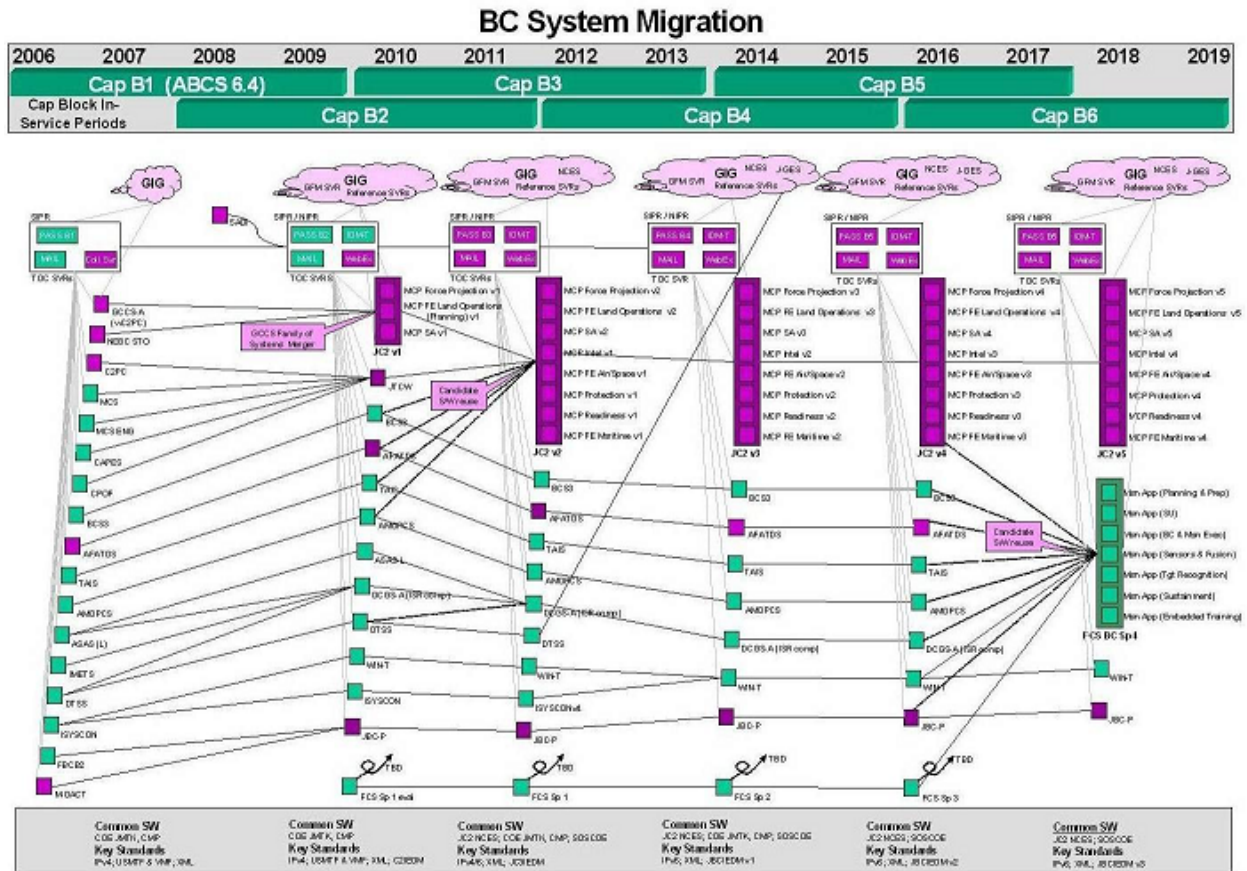


Figure 4-4. Battle Command Systems of the Future

(b) The ability of U.S. forces to dominate the third dimension while denying the enemy use of the airspace to perform reconnaissance, surveillance, targeting, and assessment will further allow the U.S. forces to exploit use of UAS and aerial surveillance platforms. The netted and distributed architectures available in this timeframe will allow for positive control, and identification and SA of the friendly UAS/aerial platform locations, thus enabling warning to U.S. forces while denying the threat forces exploitation of the third dimension. Spiraling AMD capabilities will be able to counter much more of the air threat. By this time, a modest amount of global missile defense forces and capabilities will be deployed in order to protect the U.S. against long-range or ICBM attack from rouge nations. The deployment of long-range surveillance and precision radars located on elevated platforms will enable U.S. AMD forces to engage the CM and UAS threat at significantly longer ranges. Additionally, these radars on the elevated platforms will allow for the tracking of U.S. assets, such as UAS and FW and RW aircraft, thus enhancing third dimension SA and friendly protection of these U.S. forces.

(c) The netted and distributed architecture deployed during this timeframe will enable engagement of enemy aerial platforms by providing the best data of all the available Army and joint sensors to the engagement platforms with the highest probability of kill against the threat platform. Better SA from the use of elevated sensors will enable the negation of launches from enemy ground positions prior to or immediately after the launch.



(d) The network will also enable joint “shooters” to engage enemy platforms using Army sensors thus expanding the engagement environment. The deployment of a greater number of AMD forces and systems will enhance the ability to negate the TBM threat in a saturation environment. Against the RAM threat, improvements to the sensors and effectors will enable AMD forces to protect larger areas with smaller AMD forces and will support the protection of friendly forces, both in static locations and convoy operations. Better engagement coordination with joint and allied AMD forces will reduce the number of multiple engagements against the same target, thus saving scarce missile resources and increasing kill probability.

(2) *Ground*

(a) FIRRE provides an integrated C2 capability, permitting warning information to be rapidly and accurately passed among security and force protection communities. It provides SU to commander dispatched response forces. Some intelligent remote control physical security systems exist today (such as, integrated commercial intrusion detection system) and will continue to be spiraled to protect the niche for which they were designed. Intelligent remote controlled systems are being developed and demonstrated as components of a system of protection system approach that will permit the commander to better develop a 360° protection capability, such as MATRIX, Spider, Sheriff, dynamic barrier system (graduated response

systems, FIRRE). The envisioned FIRRE systems will also enable remote command and automated activation of delay/denial devices (MATRIX, Spider) integration and execution. There are also ongoing efforts in the MP and engineer schools to reduce the bulk, size, and manpower requirements for passive physical security measures.

(b) The FCS Spin-Out 1 includes the NLOS launching station. The NLOS launching station provides extended-range precision attack against heavy and lightly armored stationary and moving point targets during day, night, and in adverse weather conditions. The NLOS launching station supports shaping, strike, and economy of force missions with limited logistical requirements. When employed in an urban environment; the NLOS launching station limits collateral damage. Launchers can be fired directly from their carrier vehicles, dismounted and fired from the ground, and even airlifted and emplaced for remote or local operation in forward areas. The ability to engage moving targets and to designate targets adds flexibility and complements existing indirect fire.

(3) *CBRNE*

(a) *CBRNE act* will continue to include active and passive measures. These measures will include proactive and reactive actions that combine preventive prophylaxis, such as vaccinations, medical screening, and pre-treating personnel, and treatments or medicines to return the injured to pre-contaminated health. There is no current plan to increase the chances of military working dogs surviving exposure in a toxic/infectious environment.

(b) The fielding of improved joint IPE joint Service lightweight integrated suit technology, joint Service aircrew mask, joint Service general purpose mask, and joint protective aircrew ensemble will continue to provide improved protection for the force. Moreover selectively permeable membranes will offer lighter weight protective garments and enhance aerosol protection for the joint protective aircrew ensemble. The IPE provides limited protection against TICs/TIMs, collective protective systems provide protection; however, efforts are being pursued to eliminate the limitations of large size, heavy weight, and substantial power requirements.

(c) The immune building system will provide shelter in place and preserve forensic evidence after an external/internal chemical biological release within the same building. Protective coatings, such as conformal coatings for electronics, chemical agent resistant paints for equipment, and chemical resistant packaging for supplies will continue to be researched. Within the *act* definition the warning measures will continue use the nuclear, biological, chemical, warning reporting system as the current system to warn American military forces. The improved warning system JWARN (Increment 1, initial operational capability) is projected for initial fielding to operational units in the midterm.

(4) *Information*

(a) The ability to take timely and appropriate defensive action is based on the JFC's ability to quickly warn users and make decisions that enable supporting commanders to effectively counter adversary cyber attacks. Effective information protection decisions must

include efficient and effective implementation of the information condition and the information assurance vulnerability management process for warning others of the cyber attack, determining the appropriate actions to mitigate the effects of the current attack, and selecting additional protection measures to preclude a future occurrence.

(b) WIN-T will provide the ability to implement and comply with DOD Information Assurance Vulnerability Alert Policy in accordance with Information Assurance Vulnerability Alert Policy Memo and all applicable DOD and Army Policies, such as AR 25-2, Information Assurance.

(c) The Army's current plan to migrate from several disparate networks to a single comprehensive network of networks, with the flexibility and security to be interoperable within a JIM environment will provide to the force, over time, the required act capabilities. The current spiraling of joint network transport capability spiral capabilities across the force will posture the Army for the advanced technology that WIN-T will bring to the fight. WIN-T will provide the means to actively defend the network through automated NETOPS capabilities.

(d) WIN-T, as the network transport and service provider to LandWarNet, will provide a multi-tiered architecture to protect and defend information and information systems, and support counter jamming measures against known external threats. WIN-T will provide a means to create and manage certificates for defense message system users deployed in tactical environments. LandWarNet will be protected by WIN-T perimeter protection capabilities to include firewalls, malicious code detection and blocking, and intrusion detection and protection at the WIN-T network boundaries. The WIN-T boundary is any instance where the WIN-T wide area network connects to a non-Army local area network, to include interface points with the GIG.

(e) In order to provide and sustain the efforts of NETOPS the technical composition must be considered (see figure 4-6). The center of the diagram illustrates the three NETOPS essential tasks, their relationships, and the desired effects once they are transformed into a tightly integrated NETOPS capability.

NETOPS MISSION AREAS

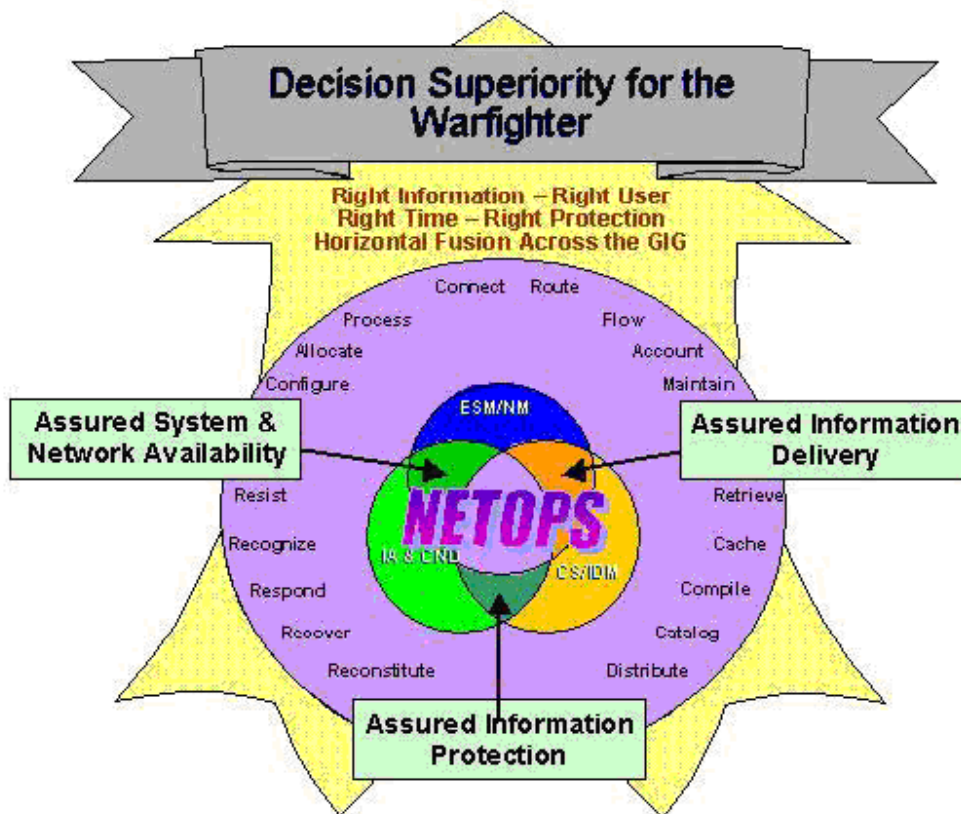


Figure 4-6. NETOPS Essential Tasks and Effects

(5) *Electronic*. Currently the only plan that is present for the spiraling of current capabilities to future optimum capabilities is Counter Remote Control Improvised Explosive Device Electronic Warfare – 2 (CREW-2) and the CREW family of systems.

(a) CREW, as a capability to defeat radio control IEDs, includes a variety of specialized systems. In its simplest terms CREW is a radio frequency jammer, which preempts the detonation of a remote controlled improvised explosive device (RCIED) by disrupting the radio signal of the initiating device. In order for any CREW system to be effective it must be programmed to jam the correct RCIED signal frequency and be in range of the RCIED to prevent the initiating signal from reaching the explosive device. All CREW systems support only a limited number of programmable frequencies and while some systems are more sophisticated than others there is no fielded technology that will dynamically identify a signal as a threat and jam that signal alone.

(b) CREW-2 will be employed across the operational environment in all areas where U.S. forces are vulnerable to RCIED attack. CREW-2 systems operate at either a fixed location or mounted/integrated with commercial vehicles and tactical military vehicles.

(6) *Intelligence*

(a) Understanding the ISR environment is the key to understanding how ISR elements will operate effectively. This environment places significant demands on sensors and processors and creates challenges faced by those who employ ISR systems to derive information and intelligence. Critical tasks for each echelon remain to carefully synchronize sensors to collect and report and then ensure collected data is turned into actionable intelligence by processors and analysts.

(b) In order to achieve SA during UP operations and enable the *act* function, these processes must work efficiently and in tandem.

(1) Translation Capabilities. The Sequoyah Foreign Language Translation System: English Target Language two-way speech-to-speech provides translation capability to enable non-linguists to conduct two-way speech communications with host nation and coalition personnel. This capability is currently being developed for Iraqi Arabic, Pashto, and Farsi.

(2) Integration and Dissemination. DCGS-A. All CI and HUMINT communications and information processing systems must be integrated with DCGS-A to allow tipping and cueing of other intelligence discipline information. The Human domain will correlate and integrate all human sensor open ended architecture to allow for expansion and compatibility with other service elements, government organizations, non-governmental organizations and coalition elements to effectively communicate during contingency operations. All information systems ISR will be vertically and horizontally integrated to be compatible across all battlefield operating systems and with current force elements. In many instances, forward deployed information centers and large staff elements of the current force organizations will be absent from the future Modular Force. Deployed forces and supporting intelligence assets will rely on sanctuary-based knowledge centers to provide information on the AO prior to deployment, during in-flight preparation and while conducting operations. These knowledge centers will be capable of providing information concerning all aspects of the target area, including cultural, geographic, socio-economic and political information, order of battle and biographic data. Knowledge centers will leverage multi-service, multi-agency and multi-national resources to provide elements and supporting intelligence assets actionable intelligence, while on the move.

- Analysis Capability: Intelligence Analysis personnel and DCGS-A at (BCT, SBCT, division MI BN).
- CI: Division MI BN and Corps.
- Translation.
- Sequoyah Foreign Language Translation System.
- English Target Language Two-Way Speech Translation System.
- Coalition Chat Line +: Two-Way Text Translation capability to enables non-linguists to conduct two-way written exchanges through e-mail and instant messaging for coalition coordination capabilities.
- The system also translates electronic documents from a target language into English and vice versa.

- Languages currently supported are Western European languages: French, German, and Spanish.

e. Recover. The following section describes spiraling plans for recover capabilities against adversary air, ground, CBRNE, information, electronic, and intelligence threats.

(1) *Air*

(a) Improvements to the logistic and supply system will improve the AMD forces' ability to quickly reconstitute and reload their missile launchers in preparation for additional air attacks against protected assets and friendly forces. The initial use of improved diagnostic and prognostic capabilities will greatly improve the AMD forces' readiness capability and reduce the repair times for the equipment.

(b) These systems will alert the operators and the supply system of impending failure or reduced operational capability thus speeding up the replacement or repair process. Use of virtual and electronic repair activities and capabilities will minimize equipment inoperable time.

(2) *Ground*

(a) Ground forces will continue to use rapid repair kits and concepts to restore functions and facilities. In the near term, new materials, construction methods, and equipment will enable recover in a fraction of the current time.

(b) As smart technologies mature, they will enable improvements in construction methods and product manufacturing significantly improving the ability of our forces to recover from an event. Smart materials and systems using sensing materials and devices, actuation material and devices, microchip controlled devices coupled with self-detection, self-diagnostic, self-corrective, and protective functions embedded in these materials and structures will enable ground forces to quickly restore critical functions and facilities. These materials and construction techniques will greatly reduce current dependency on equipment centric repairs for ground recover operations.

(3) *CBRNE*

(a) CBRN forces will continue to improve on the ability to reconstitute combat power and restore resources to operational functionality. The M17 Light Decontamination System is being replaced by the more efficient modular decontamination system. Decontaminants will require less or no water resources, be non-caustic, non-corrosive, easier to store and manufacture, and environmentally safe.

(b) Robotic decontamination, as well as decontaminants that do not damage sensitive equipment, are currently in the joint capabilities integration and development system, but will not be fielded until mid to far-term. Logistics procedures (supply, maintenance, transportation, and storage) are constantly being assessed to support decontamination operations. Hand-held and man-portable decontamination applicator systems will be available for operational

decontamination. Rapid large-scale decontamination capability for fixed sites will be available to reduce manpower and logistical burden and furnish non Two Way Text Translation -aqueous capability for electronics, avionics, and sensitive equipment.

(4) *Information*. The network's ability to update and restore operations as a result of an attack will provide the warfighter a self-healing network. The joint network node will provide an initial capability through current technology providing on demand reallocation of network assets, and recovery and restoration of data. WIN-T will provide this capability automatically, creating the self-healing qualities required of the future force.

(5) *Electronic*. There are currently no plans to spiral systems or capabilities that *recover* from electronic attack of ground units or platforms.

(6) *Intelligence Integration and Dissemination*

(a) DCGS-A is the ISR component of the future Modular Force battle command system (BCS) and will be the Army's primary system for ISR tasking, posting, processing, and using information about the threat, weather, and terrain at all echelons. DCGS-A will contribute to visualization and SA and SU, thereby enhancing tactical maneuver, maximizing combat power and enhancing the ability to operate in an unpredictable and changing environment throughout the operational spectrum. It will facilitate the rapid planning, execution, and synchronization of all battlefield operating systems resulting in the future Modular Force ability to operate within the enemy's decision cycle.

(b) DCGS-A will support future Modular Force operations with the ability to provide relevant information to support situational development out of contact, enabling the commander to maneuver to a position of advantage before enemy forces can be joined. DCGS-A will enable theater and national intelligence organizations to provide dedicated "intelligence over-watch" primarily from fixed locations through focused multi-discipline and all source fusion applications and analysis. This capability will provide the necessary IRS information to execute recover operations while maintaining SA.

4-3. Optimum Capabilities

This section describes desired future optimum capabilities to support UP objectives outlined in this CCP. These capabilities are described in the *detect, assess, decide, act, and recover* UP functions context.

a. *Detect*. The following section describes optimum *detect* capabilities against adversary air, ground, CBRNE, information, electronic, and intelligence threats.

(1) *Air*

(a) *Air detect* capabilities must be supportive of the four Army AMD mission sets; provide air and missile defense, contribute to third dimensional SA and SU, contribute to airspace management, contribute to operational force protection. The unit commander will require real-time aerial detection capabilities that provide point and wide area persistent

surveillance of the complete aerial environment. These sensors will integrate with a suite of UP FoS/SoS sensor capabilities.

(b) Sensors will provide stand-off detection of friendly and hostile aerial platforms. This capability includes the ability to locally detect or to receive the detection of the following through secure data feeds:

- TBM.
- SRBM.
- MRBM.
- Intermediate-range ballistic missile.
- ICBM.
- SLBM.
- CM.
- RAM.
- LCR.
- ASMs (to include ARMs).
- UAS.
- Manned platforms, FW and RW aircraft.

(c) The UP air detect capability must include the 360° detection of adversary missiles, manned and unmanned air platforms/objects of all sizes and RCS, provide data to support launch point designation, and execute continuous tracking through all phases of flight. Air detection must be supportive of integrated fire control, allowing the detection to trigger timely engagement with applicable weapon systems at NLOS/BLOS distances. Sensors and sensor capabilities must integrate with other UP SoS/FoS sensor and detection capabilities, and provide the ability for a commander to *see first*, through a 360° hemispherical COP.

(2) *Ground*

(a) UP detection systems must provide the desired effect of see first. Persistent and pervasive sensing, detection verification, tracking, and persistent surveillance are the foundation capabilities of a FoS/SoS that enable *see first*. The FoS/SoS must support the commander's ability to engage targets beyond the range of enemy weapons or hazards beyond their effects throughout the depth of the operational environment and develop situations out of contact. Capabilities must include total integration of all protection systems into a COP. Without such a capability, the element of surprise belongs to hostile forces. The detection capability will integrate ISR and dynamic sensors to build a "tunable" 3D sensor field that will automatically extract targets/hazards from the environmental background using integrations of multiple sensors while simultaneously tracking friendly blue forces.

(b) Future detection technology enhancements will provide stand-off, non-intrusively, on the move detection and tracking of personnel, vehicles, things, activities, and hazards (to include explosives). Persistent and pervasive detection improvements will empower the JFC to see into areas where a non-cooperative enemy does not expect them to have visibility. The FoS/SoS must have the ability to sense and report the presences of hazards to include explosive and

CBRN within an area, along a route, contained on, or within vehicles, as well as carried by personnel at stand-off. Area or point detection must be made with the fidelity to identify the precise limits of the hazard area and determine the composition of the hazard. This will enable response forces to intercept and neutralize intruders or mitigate or defeat the effects of the hazard prior to effecting friendly operations.

(c) Sensors such as seismic, magnetic, infrared, acoustic, radio frequency, diction, and other advanced sensor capabilities, whether static, hand-held, mobile, or networked UGS will be tailored to the environment and target on which they are collecting. These sensors capabilities when static, hand-held, mobile, or networked will be tailored to the target on which they are collecting. UGS will be small, low-cost, robust sensors, capable of operating in the field for extended periods of time. Self-organizing and self-healing sensors will organize into a web that is capable of target/hazard detection, location, tracking, and classification in real-time information. Sensors will be capable of autonomous cooperation with other sensors to eliminate operational environment ambiguities. Commonality of detection systems from FCS sensors to UP sensor to theater sensor will promote a high fidelity COP facilitating the commander's SU.

(d) UGS and unmanned vehicles (UVs) will provide the pervasive sensing capability required by the commander to see, survey, detect, track targets and hazards, and understand across the entire operational environment. Robotic support will be substitute for Soldiers in manpower intensive detection tasks and operating in environments where human beings have difficulty operating. Unmanned ground, air, and water vehicles will be capable of autonomous operations in a collaborative manner among themselves and with Soldiers. Robotic support also provides randomness, an important concept to successful detection and surveillance as a piece of protection operations.

(e) Current capabilities require protection units to have a FoS/SoS that gives the unit access to a variety of components that are all integrated into the information systems ISR and allow for a stand-off capability. The FoS/SoS must have the ability to predict, prevent, detect, report, and mitigate improvised explosive hazards prior to commitment of forces along a route (for example, ground movement, sustainment operations) or within the AO with the fidelity to identify the precise limits of the hazard area and determine the composition of the hazard. An explosive hazards coordination cell would be needed to provide pattern analysis and technical advice as it supports SA of explosive hazards within the units AO. The UP force will provide area clearance in order to restore its military use in support of theater entry operations, tactical/operational, ground/air movement, or sustainment operations. This set of requirements includes a FoS/SoS that will-

- Detect, report, and virtually/physically mark explosive hazards prior to commitment of forces into the area (entry operations, air movement, troop bed-down, and sustainment areas) with the fidelity to identify the precise limits of the hazard area and determine the composition of the hazard. FoS/SoS must have the ability to physically mark cleared areas within the hazard area and clearly mark the transition from one threat area to another.
- Neutralizes the full spectrum of explosive hazards present in an area to a level that restores and allows military use of that area. They must be capable of

neutralizing hazards with and without the aid of precision detection of individual explosive munitions within the suspected or confirmed hazard area.

- Deploys rapidly by air, ground, and sea to allow for rapid response into and within the theater. The capability must be scalable to efficiently and effectively handle small and large areas with a minimal logistics footprint.
- Survives against the effects of explosive hazards, but not necessarily the effects of direct and indirect fire.
- Contains seamless information systems ISR interoperability with the force it supports.

(3) *CBRNE*

(a) The UP CBRNE detect capability must provide the unit commander a real-time, persistent surveillance capability to sense and discern CBRNE threats. The CBRNE capability of detect inherently includes the joint CBRNE requirement to sense. This detection capability includes the ability to discern IED fillers, traditional and non-traditional CBRNE agent contamination, and WMD.

(b) The CBRNE detect capability must provide stand-off, point/wide area detection, and will use sensors (human, electronic, mechanical, chemical) to detect agents prior to and after release. Sensors will identify and assess agents (CBRNE or TIM) keyed to meteorological conditions and project downwind hazards and distances. UP CBRNE detect capabilities include but are not limited to-

- Real-time meteorological/other data.
- Battlefield ordnance.
- Cooperative, networked arrays (sensors, communication links, smart markers).
- Disparate (non-CBRNE specific) sensor technology integration.
- Stand-off traditional and non-traditional agents.
- 360° battlefield views (stand-off sensors coupled to real-time networked displays and change detection/other software).

(c) Improvements will be made to surface contamination monitors and the ability to detect chemical biological contamination in water. Automated, integrated detection of both biological and chemical agents in a sensor package will be available. The FCS will include CBRN manned reconnaissance and unattended CBRN sensors. A capability will exist for stand-off radiation detection and measurement. UAS CBRN detection capability and sampling capability will be mature. The ability to identify CBRN hazards from space-based systems will be available.

(4) *Information*

(a) The UP information detect protection must provide the unit commander a real-time capability to sense and monitor electromagnetic spectrum availability. This capability must provide the unit commander the ability to automatically de-conflict electromagnetic spectrum use across the protected force. UP *detect* information capabilities must detect failure of sensors

and sensor connections to the network in joint and Army applications. *Detect* capabilities must include the ability to automatically detect hostile network intrusion activity, EW, jamming, and CNA in real-time, and not rely on previously registered data.

(b) The UP information *detect* capability must have seamless visibility across all information systems ISR applications within the force it supports, giving the commander and all elements a real-time, complete 360° virtual picture of the operational area that provides relevant electronic information to the right people at the right time. The UP information detect capability must integrate with other UP FoS/SoS sensor and detection capabilities, and provide the ability for a commander to see first, understand first, act first, and reengage at will through a 360° hemispherical COP.

(5) *Electronic*. The UP electronic protection *detect* capability must provide the unit commander an effective passive early warning capability to detect and monitor electromagnetic threats. *Detect* capabilities must sense and monitor infrared, radio frequency, electro-optical, radar, and laser threats. Personnel, systems and fixed sites must be reasonably hardened to deny the effects of EMP and other directed energy weapons that have the ability to deny, disrupt, and destroy mission critical electronic components.

(6) *Intelligence*

(a) Integration and Dissemination. DCGS-A is the ISR component of the future Modular Force BCS. It will cross all UP functions and will be the Army's primary system for ISR tasking, posting, processing, and using information about the threat and the environment at all echelons. DCGS-A will contribute to visualization and SA and SU, thereby enhancing tactical maneuver, maximizing combat power, and enhancing the ability to operate in an unpredictable and changing environment throughout the operational spectrum. It will facilitate the rapid planning, execution, and synchronization of all battlefield operating systems resulting in the future Modular Force's ability to operate within the enemy's decision cycle. DCGS-A will support future Modular Force operations with the ability to provide relevant information to support situational development out of contact, enabling the commander to maneuver to a position of advantage before enemy forces can be joined. DCGS-A will enable theater and national intelligence organizations to provide dedicated intelligence over-watch primarily from fixed locations through focused multi-discipline and all-source fusion applications and analysis.

(b) Multi-ISR Sensor. The tactical unmanned airship communications intelligence surveillance reconnaissance will cross all functions. The airship will provide-

- Persistent, responsive communications and intelligence.
- Surveillance and reconnaissance for maneuver.
- Rapid strike and force protection 24/7.
- Intelligence will be integrated within DCGS process.

b. *Assess*. The following section describes optimum assess capabilities against adversary air, ground, CBRNE, information, electronic, and intelligence threats. UP assess capabilities will

integrate through FoS/SoS sensor and assess capabilities, and provide the ability for a commander to *understand first* and *act first* through a 360° hemispherical COP.

(1) *Air*

(a) The UP air *assess* capabilities must provide the unit commander the ability to determine air threat type, platform delivery, impact time and point, adversary delivery location, and jamming capability. Air *assess* must facilitate the AMD mission to contribute to third dimensional SA and SU and will include actions and capabilities that provide visualization and understanding of aerial activities or events occurring in the third dimension operational environment. SA encompasses the detection and knowledge of the airspace, and predicted and current aerial objects as part of a COP. SU is the product of applying this aerial analysis and judgment to the aerial intelligence preparation of the operational environment and the COP, in order to draw timely and relevant situational mission data and contributes to decision superiority.

(b) UP air *assess* capabilities must facilitate the AMD mission to *contribute to airspace management* and includes actions and capabilities that enable fires and manned/unmanned airspace users in a JIM environment while protecting friendly forces, ensuring the synchronized use of airspace, and enhancing the battle command of forces using that airspace. UP air assess capabilities must integrate with other UP FoS/SoS sensor and assess capabilities, and provide the ability for a commander to *understand first* and *act first* through a 360° hemispherical COP.

(2) *Ground*

(a) UP assessment systems will provide the commander the ability to *understand first*. From the clutter of the environmental background, the assessment system will combat identify targets/hazards using fused intelligence, ATR, interrogation, and individual assessment skills while simultaneously tracking friendly blue forces.

(b) ATR alerts the system operator of possible intruders or hazards. It keeps the alert under observation until combat identification is made and a response is culminated. ATR will be enabled by the commander's ability to rapidly fuse theater/operational and locally produced intelligence into a relevant database. ATR will allow the operator to tailor the assessment algorithms in accordance with the characteristics of the local or specific threats/hazards. In an effort to determine the intent of the suspected activities and behaviors, these ATR algorithms will perform automated three-dimensional characteristics, activity, and behavior analysis to classify, recognize, and identify hazards which will facilitate SU decisionmaking. An ATR enabled system will never completely remove the human-in-the-loop, but its goal must be to minimize workload and training requirements for protection personnel.

(c) If ATR cannot determine intent, then future intelligent, precision nonlethal effects and lethal effects used nonlethally will be remotely available to interrogate alerts. These intelligent effects systems will be use at stand-off distance and in increments to separate combatants from noncombatants.

(d) UVs will provide the stand-off, remote, visual assessment capability required by the operator to make rapid and accurate assessments of sensor alarm indications and interrogation actions. UVs will loiter over and on the target area for extended periods, continuously provide real-time information to the operator, and be used as a cooperative tool to help the operator with other types of actions, for example, engagement targeting.

(e) The assessment system, an integral part of C2, will provide a rapid assessment of alerts. This rapid assessment will enable the leadership to respond to prevent the approach and access into protected areas by unauthorized personnel, to neutralize intruders found in these areas, and to mitigate the effects of a hazard before they can impact friendly operations.

(f) UP needs to have a single topographic element as a mission module force with the capability to collect and process high resolution elevation data, produce terrain analysis products, and other geospatial data within the unit's operational area. The separate topographic teams of the current force need to be replaced by the geospatial planning cell that will have the capability to manage the theater geospatial database; generate and analyze terrain data; and prepare decision graphics, image maps and updates; and intelligence preparation of the operational environment overlays. The first imperative involves the collection and integration of geospatial, cultural, and enemy information (aided by automated mobility planning tools) to establish the mobility COP for the entire AO. This information allows quick development of the initial and follow-on, real-time MCOO that enables the maneuver commander to select the focused operating areas within the AO. The operating areas are smaller areas designated within the AO that allow the commander to focus collection assets and efforts. The MCOO is defined by the desired end state and will be updated with new information to reflect real-time mobility aspects.

(g) Knowledge of the existing obstacles and monitoring of existing traffic patterns are two examples that allow commanders to see the battlefield in near real-time. Knowledge of where obstacles are located is as important as where obstacles are not located. This information allows the commander to determine where to maneuver, what resources will be required to get there, and how the enemy may attempt to influence the maneuver plan. Providing mobility to the COP enables the maneuver commander to identify the operating areas in the AO and the associated mobility challenges. This imperative, linked to ISR operations, is critical, continuously updating the commander and leaders with real-time mobility visualization.

(h) Developing mobility input to the COP links the information element to the leadership element to provide SU. This functionality should be embedded with current and future joint battle command capabilities. It should address the battle command analysis and decision support tools needed to project precise unit protection effects into the operational environment in support of the JFs land component command. It should also include the systems, organizations, and procedures required for communicating across forces and reaching back to the home station operations center and other knowledge centers. This functional area establishes the conditions for all engineer capability elements to be successful in support of the joint task force commander. In order to provide mobility assessments, the FoS/SoS must include-

- Collection and fusion of high-resolution geospatial data and comprehensive operational environment environmental information that includes real-time

collection of new data, as well as supplementing existing data sets with more detail.

- Sensor cueing and placement.
- Stand-off wide area ISR.
- Tailored, digitized, and usable operational environment environmental data that is timely and compatible with the network-centric environment.
- Actionable and scalable visualization products to mitigate the threat's "home-court" advantage displayed either visually or in some other form that is compatible with the user needs.
- Computer aided analysis and reasoning tools that enable prediction and understanding, and provide actionable advice.
- Reach to national and other sources, when needed.
- Data storage, retrieval, and update capabilities.
- Digital interoperability with coalition/indigenous forces, indigenous populations, institutions, and international organizations, non-governmental organizations, and other government agencies.
- A layered network of advanced sensors that sense in multiple domains (for example, radio frequency, thermal, acoustical, electro-optical, infrared, and seismic) and operate independently, or as components of other systems/platforms. The other systems include dismounted Soldiers, manned/unmanned ground vehicles, manned/ UAS, satellites, and even cyber-based platforms.
- Networked ISR which is linked to all shooters.
- Mobile battle command which can achieve information dominance and facilitate the exchange of information between joint, allied, and coalition forces, as well as support the warfighter with integrated, reliable, real-time access to the GIG anywhere in the world.

(3) *CBRNE*

(a) New databases must interface with the GIS or similar future system to provide input to the COP to give a clear and accurate picture of all CBRNE events, attacks, and hazards in real-time. Joint effects model block III/IV, will have the capability for hazard prediction with high fidelity down to micro-scale event analysis. Additional information operations and intelligence system integration and incident management will be provided by the JOEF block II. JOEF is intended to provide a high level, strategic, and operational focus, planning tool via a massive data fusion effort with already existing but not federated data bases.

(b) Automated field CBRNE intelligence systems must accept manual and automatic CBRNE/TIM event data input, and will then modify, retrieve, display, archive, and transfer data (such as intelligence, location of attack, source and sensor information) to repositories. CBRNE hazards will have smart markers that are integrated into systems which populate the COP. With these systems commanders and staff will be able to display current COPs and efficiently execute "what if" scenarios and facilitate the evaluation of plausible adversary and friendly COAs, CBRNE employment, and TIM release other than attack. These systems will interface with standard information systems ISR to effectively and rapidly accomplish threat assessments.

(4) *Information*

(a) In order to provide Soldiers the ability to collaborate, retrieve, and store information, across the operational environment unhindered by terrain, weather, or hostile activity to accomplish their mission to *see first, understand first, act first, and finish decisively*, the UP information assessment capability must provide the unit commander the ability to assess network availability, vulnerability, and operational status down to the lowest tactical level, static or on the move. Capability must include the ability to *assess* adversary network capability.

(b) Information *assess* capabilities must include the ability to *assess* adversary EA and CNA capability and must include the ability to quickly and accurately determine the characteristics of an attack including criticality and vulnerability of the systems under attack, source of the attack, and purpose of the attack.

(5) *Electronic*. The UP electronic protection detect capability must provide the unit commander an effective capability to assess electromagnetic threats or an EA. *Assess* capabilities determine the danger of infrared, radio frequency, electro-optical, radar, laser, EMP, and other directed energy weapons threats to personnel, systems, and fixed sites.

(6) *Intelligence*. Provide interpretation of a foreign language and the assurance of accurate exchange of statements, ideas, intent, and assessment of the current populace attitude.

(a) Translation. Sequoyah Foreign Language Translation System which also applies to *decide* function.

(b) Language Systems include-

- English-Target Language Two-Way Speech Translation System provides the capability that enables non-linguists to conduct two-way speech communications with host nation and coalition personnel.
- English-Target Language Two-Way Text to Text Translation Capabilities for documents in written and electronic format.
- Target Language to English Speech to Text capability to automatically monitor, transcribe, and translate broadcasts to enable viewing and keyword search by non-linguists. This capability is planned for development in all strategic languages as determined by the DOD Foreign Language Steering Committee.

c. *Decide*

(1) Optimum UP *decide* capabilities will provide a commander battle command C2 capabilities that will have seamless information systems ISR interoperability with the force it supports. As a minimum, UP *decide* FoS/SoS capabilities will provide real-time SA allowing commanders, staff, and Soldiers to visualize the battlefield three dimensionally. This capability will display a shared common picture of the operational environment through FoS/SoS sensors.

(2) In addition, the UP *decide* capabilities will provide graphical displays, with friendly and enemy proposed and current unit locations, target/hazard identification, and tracking. These

systems will support the ability to task and synchronize the UP FoS/SoS sensors, act measures to include available networked fires and support, and as required, execute effective autonomous, sensor to shooter, precision-guided and intelligent munitions engagements that can quickly render targets and/or hazards harmless. The UP decide system will be an interactive, flexible, and adaptable system that provides an easy to use and understand interface capability; allowing for the decisionmaker's own insights. It must fuse large amounts of data into information that can be quickly acted upon and will support the decision support system

(3) The UP *decide* capabilities must provide effective in near simultaneous protection measures analysis required in UP operations. The *decide* function will additionally be supported by automated tools, mission planning and rehearsal, and joint mapping tool kit, which will support rapid COA analysis, and provide predictions about factors governed by the laws of physics. These systems must be capable to execute analysis of information which will present and organize information to support a decision.

d. *Act*. The following section describes optimum act capabilities, and discusses the act sub-functions of warn, and active and passive measures against adversary air, ground, CBRNE, information, electronic, and intelligence threats.

(1) *Air*

(a) The ability to execute detailed contingency planning and preparation is a fundamental aspect of the protection process. The unit commander will require the ability to provide aerial activity warning to applicable forces to enact sufficient protective stances and procedures. Air activity warnings will assist the commander in protecting personnel, assets, and information, and drive the development of courses of action and orders for execution allowing the force to responsively react. The UP air warn capability will provide precise warning to the affected area, a robust C2 system with means to coordinate the execution of plans, predictive intelligence, and a network of dissemination systems. The UP air warning capability will additionally provide the ability to execute nonlethal enemy (and unknown identity) warning to deter, interrupt, or cease further hostile (or possibly hostile) air activity.

(b) Active and passive air response capabilities must provide scalable lethal/nonlethal and kinetic/non-kinetic effects, and directed energy to destroy enemy air capabilities. The air act capability must provide integrated fire control which will include the ability to utilize all available networked sensors and shooters (ground and elevated), engaging air threats with the optimum, automatically selected weapon system. The sharing of sensors and shooters (launchers) via an integrated battle command capability must extend to joint engagement processes, and when necessary homeland defense agencies, and also populate the integrated AMD COP. These capabilities will ensure a more efficient engagement cycle, improve air space C2, and expand aerial protection. When coupled with ground sensors and shooters, and force application processes, these capabilities will aid the commander in executing an expanded engagement process and facilitate the integration of air and ground combat operations. These capabilities will provide the ability to execute *act* measures (see chap 3) and additionally expand current contributions to attack operations, active and passive defense operations, and AMD information systems ISR operations defense operations.

(2) *Ground*

(a) UP warn systems will provide the commander the capability to *act first*.

Commanders will finish decisively when the system is integrated with JC2 and facilitates timely warning to personnel and units of impending attack and tasking of individual and collective personnel protection measure to implement UP systems. Future systems permit the commander to engage target/hazards beyond the range of adversary weapons/effects and to destroy the target/hazard with precision fires at the time and place of choosing. The future system of protection systems will provide a fully integrate sensor and shooter system that will function equally, as well in both static and mobile environments.

(b) Active measures will provide at stand-off distances, the capabilities to-

- Deny personnel and vehicles freedom of movement outside a protected area with lethal and nonlethal remotely activate barriers integrated with C2 system.
- Rapidly and effectively engage stationary and moving targets to include vehicles and explosives within line-of-sight/BLOS/NLOS using intelligent, precise, lethal, and nonlethal effect systems to include vehicles and explosives.
- Tethered and autonomous unmanned ground vehicle with tailored mission packages will provide the capability to neutralize hazards (especially explosives) before they can impact the commander's mission. These UV systems will be capable of collaboration with other UV to successfully complete a mission.
- Provide the agility to automatically process personnel and vehicles at designated entry points.

(c) Passive defensive measures (*deny, deter, and prevent*) will provide at stand-off distances, the capabilities to-

- Deny personnel and vehicles access to and from facilities, to include movement within buildings, facilities, structures, airfields, key infrastructure and both natural and man-made terrain, hardened or buried targets with lightweight modular nonlethal protection systems which can be operated in a variety of ways, such as close/remote, on demand, and automatic activation at stand-off distances.
- Deter personnel and vehicles movement into a protected area with lethal and nonlethal remotely activate warning capabilities integrated with C2 system.
- Automatically and manual remote control lightweight modular effects protection systems, to include physical barriers, that mitigated the effects of enemy actions.
- Defeat enemy direct fires initiated at critical assets with autonomously acting lightweight modular effects protection systems.
- Deny personnel and vehicles freedom of movement outside a protected area with lethal and nonlethal remotely activate barriers integrated with C2 system.

(3) *CBRNE*

(a) CBRNE active and passive measures will require capabilities that include, proactive and reactive actions which combine preventive prophylaxis (vaccinations, medical screening,

and pre-treating personnel, military working animals, or equipment to defeat contaminants prior to their use); effective decontamination materials, processes, and techniques once contaminated; and treatments or medicines to return the injured to pre-contaminated health. Other capabilities include stand-off detection at Strategic distances; increased joint and coalition responsibilities in intelligence gathering; nonproliferation and counter-proliferation operations; monitoring and disrupting CBRNE/WMD developments; and WMD elimination at various points along the operating continuum.

(b) CBRNE *act* components, integrated across DOTMLPF domains, provide a single, overwhelming, force multiplier to all military missions. U.S. CBRN units, equipment, personnel, and practices are pivotal in maintaining friendly force viability despite natural or manmade CBRNE hazards. Attacks against U.S. and coalition forces using CBRNE weapons can disrupt, spoil, and defeat our offensive operations without leaving an enemy open to preemptive strikes or retaliation due to the nature of CBRNE/WMD mediums. Without skilled intervention, any third rate nation state, disaffected individual, or terrorist could wreak havoc on units and personnel executing a combatant commander's selected COA.

(c) U.S. CBRNE and WMD defensive operations, whether supporting an offensive, defensive, or stability mission, also includes the mission to safeguard U.S. military personnel or civilians (family members, civilian employees on installations, or inside government buildings). UP CBRNE *act* capabilities include but, are not limited to IPE/CPE, breathing capability on strategic delivery platforms, breathable filters, ingress/egress between CPE systems, or vaccines against biological agents (natural, industrial, or militarized).

(d) Within the *act* definition includes measures to warn. The unit commander will require CBRNE warning which will combine data derived from detecting and assessing sources (sensors, intelligence assets, verified agent release, etc.), rapid warning techniques, and protection means (IPE/CPE, decontamination, etc.) to timely warn Soldiers to take the appropriate protective posture. The UP CBRNE warn capability will provide potential target warning of a CBRNE or WMD event or attack. CBRNE warning capabilities will include a networked connection to the COP to report/warn of possible threats; multilevel agent confirmation; obscuration (physical/electronic/other) regardless of service or location, everyone receives the same information simultaneously. Indicators when protection is no longer required will also be available.

(4) *Information*

(a) Users throughout the force must be connected with adequate resources to allow reliable, near continuous access to enterprise information and services, both on the move and at the halt. UP information warn capabilities must include the ability to provide automated warning of network connectivity loss, interference, network intrusion, and CNA to vulnerable network users. Warning capabilities must provide alerts during degradation of network communications assets, and must provide the ability to disseminate precise warnings and actions necessary to isolate, repel, or mitigate the effects of a network attack. These capabilities must provide the ability warn of unauthorized access to sensor information and a capability that alerts user in real-time of failed sensors or sensor connections to the network.

(b) The purpose of UP information *act* capabilities is to safeguard critical information assets used to enhance decisionmaking and synchronize activities to accomplish the mission. The unit commander will require information *act* capabilities represented by an information network with the redundancy and security to protect it. Optimum capabilities include the ability to centrally and automatically repel network attacks at the enterprise level; the ability to transparently and automatically reroute priority information around degraded/compromised networks through terrestrial, airborne, and space communications assets; and the ability to locate, identify, and destroy (physically and electronically) adversary network attack/intrusion capability.

(5) *Electronic*. Active electronic protection capabilities should give the unit commander the ability to prevent collateral damage from electromagnetic spectrum EA threats. Active protection systems should allow the operator to detect and react to weapons and munitions using the electromagnetic spectrum.

(6) *Intelligence*. Enables the *act* function through information integration and dissemination. DCGS-A provides this capability (see chap 3).

e. Recover

(1) UP *recover* must provide processes that enable the rapid restoration of operational readiness for all affected detect, assess, decide, and act UP systems and processes and logistics capabilities, during and following attacks. These capabilities will enable, not hinder, the battle damage assessment and repair process. The utilization of embedded systems and technologies to enable self-recover processes and capabilities will require the advancement of self-healing technologies and components in the design of future systems. These designs should also utilize unmanned systems to enable capability restoration and leverage existing, and require additional improvements to sustainment functions.

(2) In addition, the UP FoS/SoS *recover* capabilities will provide additional unique capabilities to execute the decontamination of materials/systems while using decontaminants that do that do not degrade sensitive equipment (aircraft and electronics), improved decontamination materials and procedures (for example, distribution of CBRN decontamination unit capabilities to non-CBRN units) and operate within international standards and protocols for marking of contaminated areas. The future will require unmanned decontamination platforms and system with precision roll-on/roll-off delivery means to return the force to operational capability once agents are discovered. The UP and electronic *recover* capabilities will assess and repair electronic infrastructure at strategic, operational, and tactical levels and detect and recover lost or corrupted information.

Chapter 5 Army Unit Protection Operational Architecture

5-1. Army Unit Protection Operational Architecture Products

a. The primary purposes for developing the UP operational architecture products are to support the development of the UP CCP, and to describe how UP integrates with and performs as a part of the future Army.

b. Included in this CCP are the operational concept graphic and operational activity model (OV-5) operation architecture products. The activity model is a draft model that is under development and will be further developed as the UP concept capability plan matures.

(1) *Army Unit Protection Operational Concept Graphic.* The operational concept graphic consists of three views of the UP CCP, depicted in figure 5-1. The graphic presents a top level view of the interoperability requirements with the current and known future organizations and graphically illustrates how information will be exchanged as envisioned by the concept writers. It also illustrates potential operations supported by the UP capability mapped to specific timeframes.

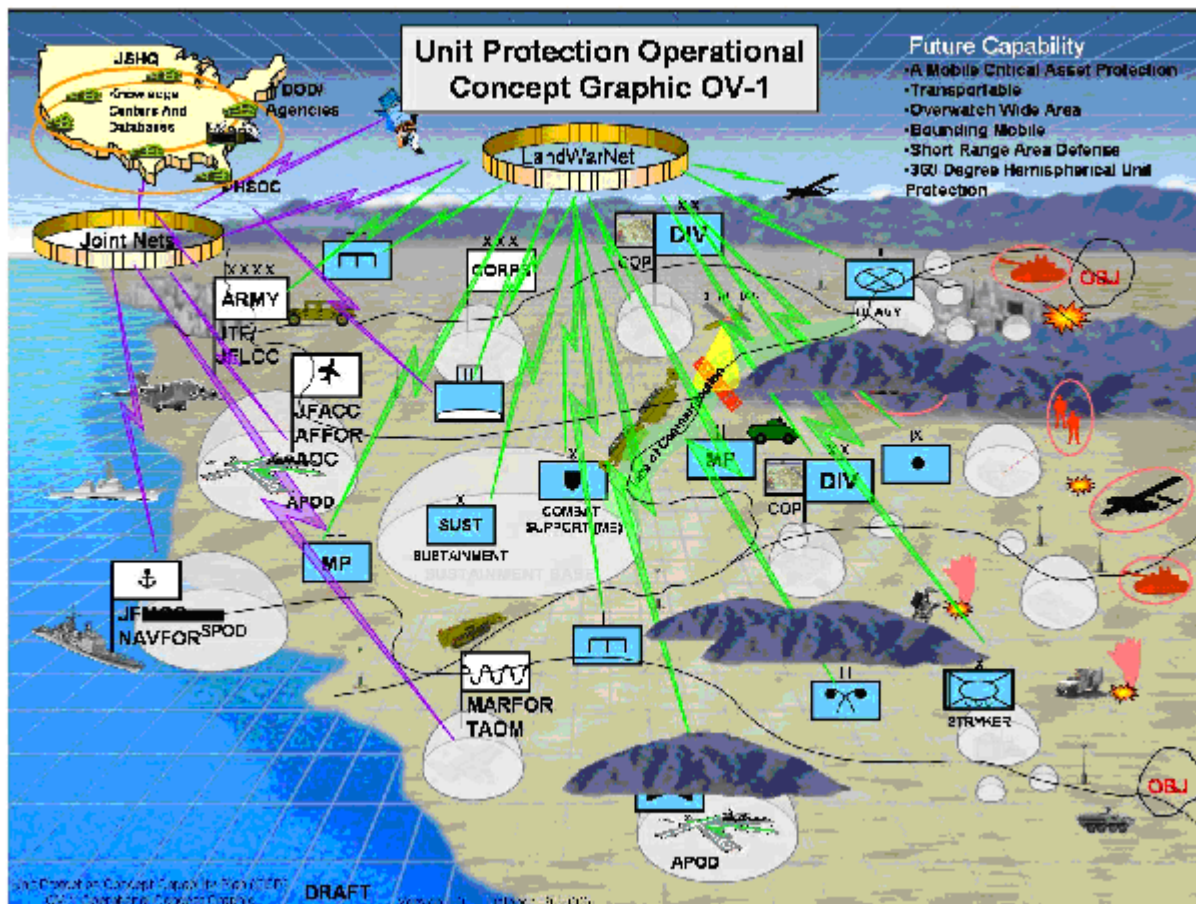


Figure 5-1. Operational Concept Graphic (OV1)

(2) The effects based intent of operational level UP in support of theater operations will ensure unimpeded projection and sustainment of forces; deter, preempt, or defeat enemy attacks; protect critical bases of operation; and enhance the commander's SA and SU. Fusing UP technologies and capabilities will provide a commander a 360° hemispherical protection capability during all phases of operations. Initially the protection will be limited to a static capability, which will eventually be able to provide a mobile critical asset protection capability. The BCS provides the integration of protection capabilities from different branches in the U.S. Army to include, but not limited to AMD, MP, chemical, engineer, military intelligence, and signal. These capabilities will be incorporated into joint protection processes across the land, air, sea, and space.

(3) The LandWarNet and various joint networks will be utilized to integrate these capabilities to enhance SA and SU, provide early warning, and support defense of protected assets from attack, and to preempt or defeat enemy asymmetric attacks. Increment I will be accomplished during the 2007/2008 timeframe. Increment II will be accomplished during the 2016-2017 timeframe and Increment III during the 2023-2024 timeframe.

(a) Increment I will provide increased SA and SU through the integration of two new systems; counter RAM and FIRRE. These systems will provide an integrated air and ground picture and active defense against RAM. The UP Increment I capability will be a static protection capability and is envisioned for use at forward operating bases. Connectivity between counter RAM and FIRRE will be through LandWarNet systems.

(b) Increment II will provide enhanced protection capabilities through the further integration of counter RAM and FIRRE, and other UP capabilities which enable a 360° hemispherical UP covering a stationary critical asset, such as aerial ports of debarkation, sea ports of debarkation, or an assembly area. Connectivity among units will be enhanced through anticipated improvements in LandWarNet and various JC2 networks.

(c) Increment III will provide a mobile critical asset protection capability. Further integration of UP capabilities will provide 360° hemispherical UP covering both stationary and mobile critical assets, such as a convoy on main supply routes. Connectivity among units will be enhanced through anticipated improvements in LandWarNet and various JC2 networks.

5-2. The Army Unit Protection OV-5 Activity Model

a. General

(1) The Army UP activity model defines and documents the information and resources used and consumed, the controls and constraints on the performance, and the outputs of the missions, activities, and tasks performed or supported by Army UP operational nodes and organizations.

(2) The OV-5 includes missions, activities, and tasks performed, or to be performed, by all Army UP nodes and organizations, depicted in figure 5-2. NOTE: In accordance with

guidance contained in *Commander Joint Chiefs of Staff Instruction 3170.01E*, the OV-5 will incorporate activities from the net-centric operations and warfare reference model.

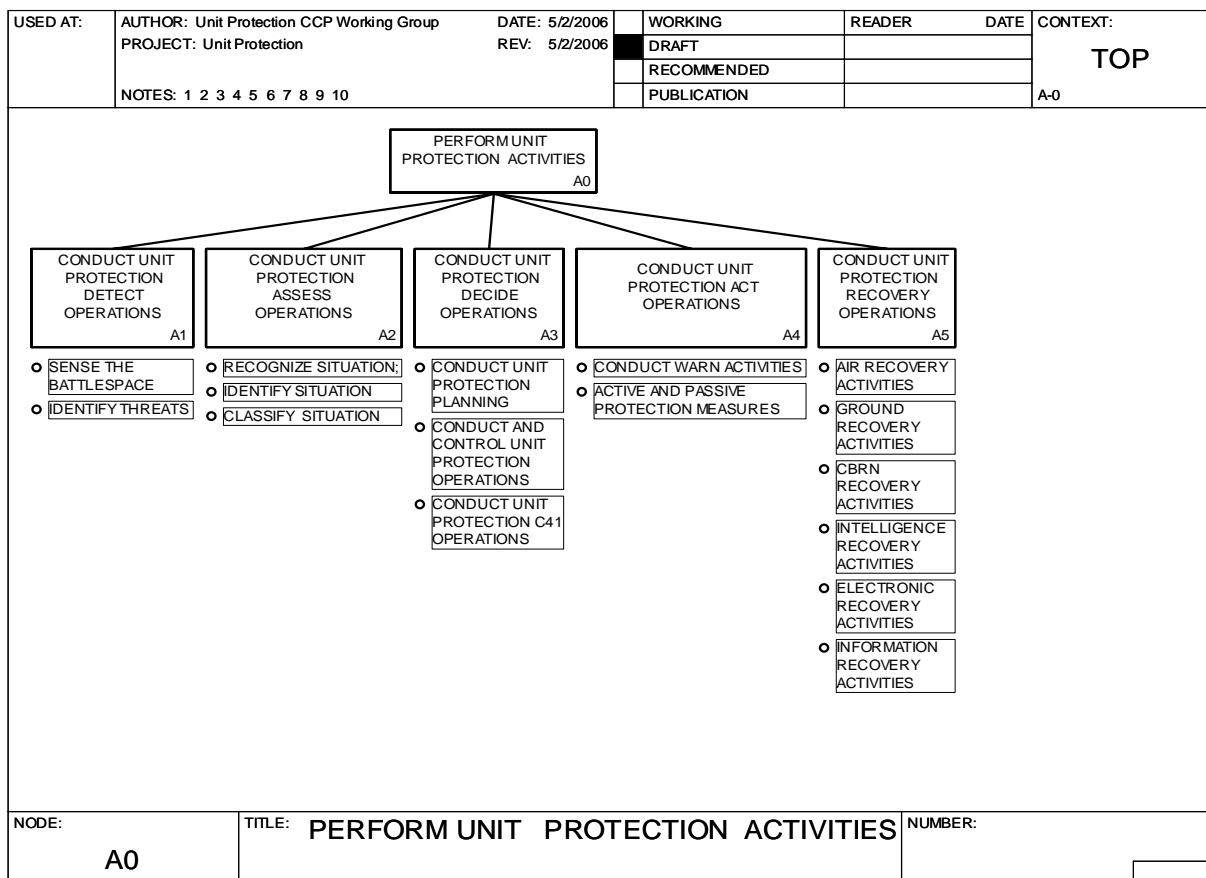


Figure 5-2. Unit Protection Operational Activity Node Tree

b. Activity Model Contents and Structure. The Army UP activity model is organized at its highest level into five major activities reflecting the primary categories of activities performed and supported by Army UP organizations, nodes, and systems.

c. Conduct Unit Protection Detect Operations. This portion of the model identifies the activities performed or supported by Army UP sensors, sensor nodes, and the sensor portion of some integrated weapon systems. The subordinate activities within this area include *sense the operational environment* and *identify threats*.

d. Conduct Unit Protection Assess Operations. This portion of the model identifies activities performed or supported by Army UP C4 systems, nodes, and the thinking and controlling components of Unit Protection systems including sensors, and integrated weapon systems. The subordinate activities within this area include *assess enemy situation*, *assess friendly situation*, and *assess environmental situation*.

e. Conduct Unit Protection Decide Operations. This portion of the model identifies the common set of C2 activities performed or supported by Army UP C4 systems, nodes, and the thinking and controlling components of UP systems including sensors and integrated weapon systems. The subordinate activities within this area include conduct unit protection planning, conduct and control unit protection operations, and conduct unit protection information systems and intelligence operations

f. Conduct Unit Protection Act Operations. This portion of the model identifies the activities to be performed by Army UP C4 systems, nodes, and the thinking and controlling components of UP systems including sensors, and integrated weapon systems. The subordinate activities within this area include conduct warning activities, and conduct active and passive protection measures.

g. Conduct Unit Protection Recover Operations. This portion of the model identifies the activities performed by Army UP C4 systems, nodes, and the thinking and controlling components of UP systems including sensors and integrated weapon systems. The subordinate activities within this area include air, ground, CBRNE, information, electronic, and intelligence recovery activities.

Chapter 6 DOTMLPF Implications and Questions Architecture

a. There are profound implications for the Army and the joint community as we evolve the UP CCP; consequently, synchronization across the DOTMLPF domains is required. Some study issues transcend the specific area of protection and should be examined fully as the Army and the joint community moves to an advanced form of UP. There is one unifying idea, the Army must become a learning organization to a greater extent than ever before and must better understand the cognitive processes as they apply to UP. Army concepts normally include a discussion of the implications of the concept capability plan for DOTMLPF. Those implications should be explicit enough to generate some action for change within the DOTMLPF domains by responsible offices.

b. The *primary* implications arising from the UP CCP, vice an exhaustive list, are described below. However, many of the items cited below will require additional analysis before comprehensive actionable recommendations emerge.³

- (1) What is the most effective organizational design for implementation of the UP plan?
- (2) What are the required objective and threshold capabilities for the UP plan?

³ The discussion of the DOTMLPF implications for UP is drawn from a similar discussion within the Protection Joint Functional Concept, the future Modular Force capstone concept, OM and TM, with minor clarifications and revisions. Any activity that crosses the threshold in cost or impact will require joint capabilities integration and development system review as outlined in the CJDSM 3170.01B and the CJCSI 3170.01E. As analysis brings DOTMLPF issues to the fore, it is probable there will be joint capabilities integration and development system implications either in addressing acquisitions or DOTMLPF Change Request.

(3) What operational and organizational challenges remain from today's conceptual efforts in the future?

(4) What UP capabilities does the Army have to provide to other Services in order for them to implement the UP plan?

(5) What UP training and training support capabilities does the Army have to provide to other Services or integrate with other services to implement the "train as you fight" concept?

6-1. Doctrine

a. Emerging doctrine will focus on the necessary capabilities to engage adversaries across the full range of operations with a JF that shares common systems, tactics, techniques, procedures, and doctrine. The doctrinal concepts necessary to initiate the organizational and cultural changes described in TRADOC Pam 525-3-1, *Future Force Battle Command (C4ISR) Concept* and TRADOC Pam 525-3-25, *Maneuver Support Concept* are promulgated in Field Manual (FM) 1, *The Army*; FM 3-0, *Operations*; and FM 6-0, *Mission Command: Command and Control of Army Forces*. As the future Modular Force nears operational readiness, these documents will evolve. Our system of doctrine production and dissemination will become more responsive.

b. The degree of modularity envisioned requires doctrine that is more synergistic and adaptive. Standardization of information management procedures is necessary to effectively execute a networked approach to operations. At the same time, tactics and operational doctrine must stress the art of war, and create flexible and adaptive solutions that depend upon human creativity. Doctrine principles provide an authoritative guide for leaders and Soldiers, but still provide freedom to adapt to circumstances. The evolution of organizations is driven by concepts and doctrine. New doctrine and tactics, techniques, and procedures will be required to effectively plan and manage battles collaboratively, and must seamlessly be integrated with joint doctrine to optimize planning and execution of warfighting operations at all levels. Doctrine questions include, but are not limited to-

(1) How does the Army conduct offensive, defensive, stability, and support operations in UP?

(2) What are the impacts of national rules of engagement, policies, and law during UP missions?

(3) What are the limits to interdependence among branch and Service functions?

6-2. Organizations

a. To effectively support future operations, organizations must transform into a more modular, scalable, mission tailorable organizations with multifunctional capabilities. They must become more versatile and agile to support joint operations and must process capabilities to adequately support the operations of maneuver and support forces. Joint mutual support

becomes the key factor in determining Service roles and missions and mission context will determine the apportionment of Army HQ and forces. The range of missions assigned to Army forces will force an alignment change from the traditional command echelons. Army HQ will support the combatant commander with the command structure appropriate for land operations. The rank of the commander and the functions of the HQ will not necessarily correspond to the numbers of forces assigned to it.

b. Higher HQ will be organized and equipped to exercise UP over highly flexible task organizations. In many operations, the number and composition of subordinate units will differ dramatically from industrial age warfare echelons. As each operation unfolds, the makeup of the deployed Army force will evolve, shifting in composition as the mission and circumstances require. While units that are stationed with the HQ may align for training and readiness, actual operational groupings will be based upon mission requirements. Organizational questions include, but are not limited to-

- (1) What does the appropriate organization structure consist of to enable effective UP?
- (2) Can current organizational structures be augmented to satisfy the capabilities of UP?
- (3) Is a complete new organizational structure required to achieve the required capabilities of UP?
- (4) What types and mixes of capabilities must reside in the UP construct? How should those capabilities be organized for UP?
- (5) How can the JF protection and sustainment system identify trade-offs between services force packages in terms of capabilities required by UP?

6-3. Training

a. In past operations, ad hoc task forces, whether multi-national or joint, usually relied on inventiveness and adaptability during operations to overcome a lack of prior collective training. Battle staffs should routinely engage in exercising varying force packages in difficult and demanding tasks that they will perform in war in order to identify and correct weaknesses and gaps in protection. As new military occupation skills are required and technologies emerge, the Army must be flexible enough to train, incorporate new technologies as they mature, and become available. We must adopt a joint and expeditionary mindset. The point is to build synergy and synchronization across disparate force packages that potentially could be mixed to accomplish ever changing national objectives. To ensure a lean deployed staff is effective with ever changing force structures, it must be continuously trained in complex joint and multi-national operations at the operational and tactical levels. This training is essential to build the basis for trust and rapport, leader development, and to build cohesive and responsive capability against emerging against adversary actions.

b. Training plans will incorporate the implications to support evolution of the future Modular Force. Implications include the implementation of a lifelong training paradigm; the

continued refinement of the train-alert-deploy approach; the linkage of training strategies between force stabilization and readiness within the managed readiness system; and the accommodation of training tasks emerging from expanding mission for Army forces in the future joint operational environment, without a corresponding increase in time. As a means to frequently train the skills and techniques associated with C2 of tailored force packages, the future force BCS must provide embedded training modules supported by low-cost, low-overhead simulations.

c. Army embedded training modules shall complement new equipment training, battle staff training, home station sustainment training, and institutional training and approach the quality and standards of the combat training centers. Embedded training shall also provide the tools to assess operations and evaluate individual and collective task performance based on mission training plans, so lessons are captured and focused retraining may occur. Small unit training will remain the bedrock of readiness and effectiveness, and will be supported by Army applications in their operational mode. Training questions include, but are not limited to-

(1) How does current training and leader development enable UP? How can the Army adapt its training to better enable current forces to engage in UP operations as integral parts of joint and combined arms teams, and independently, when and as necessary?

(2) How will evolving technologies and ongoing or planned changes in organization affect the ways in which Army units and leaders operate, and what are the training implications of these changes to support UP operations?

(3) What training designs will develop units and leaders that can capitalize on the full range of UP capabilities and fully contribute their own capabilities as members of the joint team?

(4) What is the proper training required for contractors and DA civilians on the battlefield who support UP missions?

(5) What type, scope, and frequency of training must the future Modular Force conduct to enable effective UP operations?

6-4. Materiel

a. Resources are always limited. Lack of materiel restricts the unit's ability to execute missions. Modernization and sustainment ensure that baseline capabilities are maintained and future capabilities are pursued within funding and resourcing levels. Unit sustainment and the supporting logistics structure must be planned in detail. Realization of the future Modular Force UP concept is dependent upon the development and incorporation of advanced technology on the battlefield. Protection materiel solutions must proceed along a top-down, joint-driven path. In a networked, distributed operational approach to warfare, the optimization of the entire system is more important than the strict optimization of a single weapon, staff element, or past program. The potential operational benefits of these advancements in technology will be profound. Distributing UP capabilities among multiple distributed units and enabling multi-echelon collaborative planning from joint to tactical levels will eliminate much of the sequentially in

today's planning and allow streamlining of the military decisionmaking process. Planning in concert, commanders and staffs at successive echelons will have a clearer, common understanding of intent and fuller appreciation of the implications of planning decisions across units and formations.

b. Expanded SU and multi-echelon collaboration will facilitate the use of mission orders and expand span of control, enabling greater decentralization and simultaneity. Access to a COP or common information environment will enable subordinate commanders to self-synchronize their actions during UP operations and make adjustments in response to changing situations. The sum of these technological advancements will enable Soldiers on the battlefield to anticipate more reliably and apply force more precisely and effectively, simultaneously shaping the future battle while conducting current UP operations, across the spectrum of conflict. Materiel questions include, but are not limited to-

- (1) How will units establish tiered, multi-echelon, and multidimensional ISR, fires, and maneuver that are fully networked to assure over-watch in lethality and information during UP missions?
- (2) What are the required roles and capabilities for unmanned systems on the battlefield during UP operations?
- (3) How will sensor to shooter linkages enable lethal over-watch by engaging enemy target sets near instantaneously?
- (4) What combined vertical and inherent horizontal maneuver capabilities enable units to support UP operations as directed by the commander?
- (5) How will units have the ability to maintain freedom of movement during UP operations?
- (6) How will units enable dominant SU continuous throughout the tactical UP operations?
- (7) How will units be assured of a tailorable, networked BCS for use in UP?
- (8) How will units maintain a real-time UP focused family of interoperable operating pictures, including a single integrated air picture, through multi-path communications with air and ground forces and fire support?
- (9) What mix of passive and aggressive capabilities is required to provide timely UP combat information?

6-5. Leadership and Education

a. One of the keys in enabling effective UP will be the development of leaders and staffs who can perform effectively across the ROMO in a complex, uncertain, and dynamic operational

environment. Leaders must be educated, trained, and developed to be self-aware, innovative, and adaptive throughout training and operations. They must think strategically, as well as tactically, possess a joint and expeditionary mindset, and successfully apply the joint operational art across the range of UP operations. Leaders will also need joint/interagency and multi-national education and experience early in their careers. Doctrine will provide intellectual foundation, educational opportunities will prepare leaders for how to think, and robust and realistic training coupled with operational and experience will convert knowledge into operational competence.

b. Our system of leader development must focus on the human qualities of initiative, mature judgment, mature judgment, flexibility, trust, and teamwork to realize the full benefit of UP. The Army must instill audacity in our leaders and condition them away from passivity in the absence of certainty. As previously noted, a leader's staff must also be educated, trained, and developed. Consequently, changes that impact the mix and capabilities of staff specialists and generalists are significant. The rapid evolution of automated systems and capabilities require a change in leader development to ensure future leaders can leverage these new tools. Emerging technology will help leaders focus on critical decisions, highlight opportunities for initiative, and facilitate teamwork.

c. Future Modular Force leaders must be trained to aggressively manage information and instill trust in the output of decision support tools that automated systems provide. Other major implications include adoption of a lifetime of education paradigm and the creation of knowledge centers configured to support professional leader education. Leader development questions include, but are not limited to-

(1) How do we develop leaders ready to deal with the complexity of the contemporary operating environment, threats, and interagency implications?

(2) How can we develop more adaptive leaders, versatile in UP operations?

(3) How do we provide collaborative, distributed training problem solving and decision aids that empower battle command to support commanders, as well as staffs to advising commanders during planning, preparation, rehearsal, and execution of UP exercises and operations?

(4) How are leaders enabled to know the terrain and weather and appreciate their tactical implications for tactical concealment, employment of weapons, mobility, and seeking positions of advantage?

(5) How are leaders empowered to understand the operational environment as well as, or better than, the threat in order to execute UP detect, assess, and decide functions?

(6) How will units enable leaders to know the enemy, friendly unit locations, and their capabilities?

(7) How will units adapt to emerging UP situations more quickly than an adversary?

6-6. Personnel

a. Soldiers are the Army's greatest resource and the most important factor in maintaining and effecting unit readiness. Implementing force stabilization policies that reduce personnel turbulence better supports a lifetime training and education paradigm, and reduces the redundancy that occurs in some training cycles is also important. The personnel management system must adapt to force stabilization and undergo analysis regarding continuing in its current form to ensure that it provides the career paths needed to fully prepare leaders for the future Modular Force. The dependence on reserve component mobilization and deployments to meet operational requirements also force the inclusion in the analysis and adaptation of the personnel management system.

b. The modular and distributed nature of the UP capabilities proposed will require new combinations of uniformed and non-uniformed personnel. New organizational constructs will rely on experienced civilian personnel to provide the expertise needed to support training readiness and global operations. The right combinations of Active Army, Reserve Army, DA civilian and contractor attendants can only be determined through research and exercise. Personnel questions include, but are not limited to-

(1) How do units share and integrate critical and selected operational data (platform level) required to support the commanders human resources requirements to build, generate, train, and sustain combat power during UP operations?

(2) Do certain individuals have innate skills at cognition, problem solving, and rapid decisionmaking under conditions of uncertainty, ambiguity, complexity, and stress? How do we identify these individuals? How do we refine and or duplicate these skills to support UP operations?

6-7. Facilities

a. Improving strategic response will require upgrades of Army facilities infrastructure. The facilities and infrastructure of the Army will require significant investment of resource to train, sustain, mobilize, and deploy forces in accordance with future force concepts. These facilities will have varying capabilities of training, projection, reach, and knowledge. Installation information facilities will enable distributed information sharing among the sustaining base and deployed forces during all phases of operation.

b. Prior to deployment, fixed facilities on the installation can collect, process, and analyze large volumes of data such as terrain databases that must be pre-positioned down to platform level. Installations will require suitable facilities for skilled civilian personnel supporting a military staff to leverage supporting UP operations. Installations will also need to consider facilities needed to co-locate protection enablers in order to cultivate necessary live fire and field training relationships that supplement virtual battlefield training sessions. Additionally, the future force must support the concept, "train as you fight" and strive to create a realistic training environment for Soldiers and their organizations. Specific implementation resources, plans, and

procedures must be initiated with sufficient lead to reach maturity with the future Modular Force. Facilities questions include, but are not limited to-

(1) Are there adequate facilities available to Soldiers, leaders, battle staff, non-uniformed personnel, and units sufficient to allow, attain, and maintain acceptable levels of training effectiveness for UP operations?

(2) What infrastructure is required at forts/installations to adequately support UP missions in both training and operational constructs consistent with Army, joint, and multi-national concepts and as specified JNTC attributes?

(3) What infrastructure is required in theater to support UP missions?

Chapter 7

Wargaming and Experimentation Study Questions

a. The Army is pursuing the most comprehensive transformation of its forces since the early years of World War II. This transformation is happening while the nation is at war. The urgency of supporting the current fight blurs the usual dichotomy between the current and future Modular Force. The Army must seek to accelerate inculcation of select future Modular Force capabilities into the current Modular Force to support today's fight, while simultaneously ensuring that today's lessons learned are applied to future Modular Force developments, and timing.

b. This transformation encompasses more than materiel systems. Adaptive and determined leadership, innovative concept development and experimentation, and lessons learned from recent operations produce corresponding changes in the DOTMLPF domains. Experimentation, wargames, and experience are the methods the Army uses to mitigate risk while considering and improving capabilities for the future Modular Force.

7-1. Introduction

a. Hypothesis testing experiments are the traditional type used by individuals to advance knowledge. This occurs by seeking to falsify specific hypotheses (specifically if...then statements) or discovering their limitations. In order to conduct hypothesis testing experiments, the experimenter shall create a situation in which one or more factors of interest can be observed systematically under conditions that vary the values of factors thought to cause change in the factors of interest, while other potentially relevant factors are held constant.

b. Simulations and modeling are often called upon to make an assessment. Vignettes are built to look at one or more sets of conditions that will best help to evaluate these hypotheses, but the raw data is often not conclusive or requires reasoned review by seasoned subject matter experts to confirm the reliability of these simulation/modeling efforts.

c. Concept development and experimentation is fundamentally a risk reduction activity; failure to conduct effective development and experimentation significantly increases developmental risk for the Future Force and operational risk to the current Modular Force.

Specific actions to reduce these risks are operational risk to the current Modular Force and development risk for the future Modular Force.

(1) *Operational risk to the current force.* Increase the capabilities of the current Modular Force through prototype experiments that test the compelling solutions and develop DOTMLPF capability packages to support the spiraling forward of future Modular Force capabilities to satisfy critical current force operational needs.

(2) *Developmental risk for the future Modular Force.* Reduce future Modular Force development risk by developing concepts and capabilities that meet the needs of the future JFC through rigorous concept development experimentation.

d. *Army Testing.* Wargaming and experimentation to support this CCP for UP and its impact on DOTMLPF sets will be tested and studied using standard vignettes, except where the set of standard vignettes will not allow for reasonable testing. In that case, additional vignettes may be recommended or other methods found to evaluate aspects of UP. Experimentation will help define how the capability requirements (see chap 3), can best be implemented in the ground, air, and EW realms.

e. *Joint Testing.* Joint organizations and operations will be tested and modified as mission requirements change during experimentation. Vignettes selected for simulation will provide an illustration of how organizations will conduct or support operations throughout the deployment cycle while supporting the full ROMO. Although the vignettes will be based on a hypothetical theater, they will test the new modular organizational structure and how all organizations will execute UP functions while performing their assigned missions. Logical excursions will then be conducted to evaluate what the results might be if they were performed in a different theater or varying set of factors for mission, enemy, terrain, troops, time, civil considerations.

7-2. Past and Future Experimentation

a. *Past Experimentation.* TRADOC and its proponent schools have conducted extensive experimentation that has implications on the UP CCP. The following is a list of major experiments conducted over the last two years:

- (1) TRADOC Integrating Event series of events, such as Omni Fusion.
- (2) Convoy Protection IPT studies.
- (3) Maneuver Enhancement Brigade Study #1.
- (4) FBCT focused events on Fires, Explosive Hazards, Urban Operations.
- (5) Unified Quest.
- (6) Sea Viking Joint exercises.

b. *Future Experimentation*

(1) The following experiments will further assist in defining the UP CCP:

- (a) Urban Resolve 08.
- (b) Nonlethal CEP.
- (c) Joint Robotics Modeling and Simulation Center efforts.
- (d) Unified Quest 07.
- (e) Joint Functional Protection Experiment.

(2) In addition to these listed events, there are many small analysis events and experiments that occur throughout various installations which will also provide insights to further refine this CCP.

7-3. Study Questions

Questions which support future experimentation include-

- a. What are the identified UP capability shortfalls?
- b. In a distributed operation environment, what unique protection capabilities are required for support and sustainment forces, systems and associated LOCs?
- c. What are the best organization and capabilities to develop and conduct an integrated, UP campaign?
- d. What are the new organizational solutions required to manage the complex activities comprised within UP operations?
- e. What new of integrated UP missions are the responsibility of AMD, MP, chemical, engineers, military intelligence, and signal?
- f. How are responsibilities for security of bases, base clusters, lines of operations determined and tasked?
- g. How are UP operations executed? What are the required tasks? Who communicates with whom/what in UP missions? What challenges would the UP configuration have across all mission sets?
- h. What advanced training tool sets are required to support adequate Soldier training and development for UP missions?
- i. What constitutes a sufficient level of knowledge/information to enable freedom of maneuver operations?

- j. How should information be managed and disseminated to maximize a shared level of SA among all echelons?
 - k. What is the training impact of each new system/equipment, to include short-term transformation and long-term sustainment?
 - l. What are future Modular Force vulnerabilities to technology failures?
 - m. What is the appropriate mix of UP technological capabilities for air and ground assets, manned and unmanned?
 - n. What critical assets are required in each unit to enable UP?
 - o. What are the primary implications of noncontiguous, high-tempo, distributed, networked UP operations for battle command?
 - p. How do integrated UP capabilities provide sufficient near real-time SU to support self-synchronization during UP operations?
 - q. What are the current critical UP capability shortfalls for near term, midterm, and future?
 - r. What technologies are so compelling as to warrant immediate prototyping? What prototypes are under development?
 - s. How do emerging technologies introduced in Spiral 1 (the first grouping of provided capabilities) increase effectiveness for successful UP operations? What is the best mix of these technologies?
-

Chapter 8

Alternative CCP

- a. The UP CCP is an Army specific document that attempts to provide a plan for integrated protection, by conceptualizing a future protection FoS/SoS that will integrate protection capabilities across different protection related proponents, and develop separate capabilities into one integrated protection capability. UP is not force protection, although the application of protection capabilities will positively affect force protection. By integrating the protection capabilities outlined in this CCP, a commander, and consequently, the force will be offered superior protection abilities.
- b. There were many concepts referenced in the development of this document. There are numerous references (see app A), which detail the numerous capabilities researched and the mission areas that were studied either prior to or during the formulation of the UP CCP. One such example is the CSB operational and organizational (O&O) plan. The CSB O&O addresses specific proponent missions and the mission areas of those units assigned or attached to the CSB (many of those units are the same proponents that are addressed in this concept). The CSB O&O

additionally addresses the protection related missions of the units assigned or attached, and details that the missions may be performed under the command of the CSB senior leader and staff. The CSB O&O does not address the integration of these capabilities into a FoS/SoS capability that will provide integrated protection to a commander.

c. Each proponent of the UP Plan has its own branch based future concept, for example, the AMD concept, and plan for how it will operate in the future, or a concept driving future operations based upon a specific capability, such as LandWarNet. Additionally, there are individual TRADOC and/or DA supported working groups that address problems and solutions for certain threats, for example the sustainment force protection and the IED defeat working groups. While these concepts and working groups are necessary for the development of proponent specific capabilities, most do not fully address the ability to integrate with other, protection type mission capabilities. While all of the specific proponent protection capabilities are viable and provide capabilities that the force (current, spiral, and future) needs, they are stove piped and ill-equipped to support an integrated future force; they lack a common capability underpinning the theme of DOD transformation the ability to integrate and interoperate (see chaps 2 and 4). Spiral and future protection capabilities should not continue to develop on separate paths, but should develop as an integrated capability envisioned in the UP CCP.

d. The UP CCP and follow-on analysis should serve as a rallying point for emerging protection capabilities. Newly developed protection technologies and capabilities should fall under the UP capability/umbrella. The UP CCP and its resulting 360° hemispherical protection capability should serve as a benchmark for the development of additional protection capabilities that will give the future force an advantage on the battlefield.

Appendix A
References
Required Publications

Department of Defense Protection Joint Functional Concept.

TRADOC Pam 525-2-60

Military Operations: The Operational Environment and Threat, a View of the World to 2020 and Beyond.

TRADOC Pam 525-3-0

The Army in Joint Operations the Army's Future Force Capstone Concept 2015-2024.

TRADOC Pam 525-3-1

U.S. Army Operating Concept for Operational Maneuver 2015-2024.

TRADOC Pam 525-3-2

U.S. Army Operating Concept for Tactical Maneuver 2015-2024.

TRADOC Pam 525-3-5

U.S. Army Functional Concept for Protect, 2015-2024.

Section II
Related Publications

Army Comprehensive Guide to Modularity.

AR 25-2

Information Assurance.

Bridge to Future Network, Capability Production Document.

Bridge to Future Network, Concept of Operation.

The Chemical, Biological, Radiological, Nuclear Defensive (CBRND) Functional Area Analysis Document.

The Chemical, Biological, Radiological, Nuclear Defensive (CBRND) Functional Needs Analysis / Functional Solution Analysis.

CJCSI 3170.01E, Joint Capabilities Integration and Development System.

CJCSM 3170.01B, Operation of the Joint Capabilities Integration and Development System.

CJCSM 3500.4D, Universal Task List.

TRADOC Pam 525-7-1

DCGS-A Capability Development Document.

Department of Defense Chemical and Biological Defense Program Annual Report to Congress
March 2005.

Department of Defense Chemical and Biological Defense Program Annual Report to Congress
March 2005.

Department of Defense Command and Control Joint Integrating Concept, Version 1.0.

Department of Defense Force Application Functional Concept.

Department of Defense Force Management Joint Functional Concept, Version 1.

Department of Defense Functional Concept for Battlespace Awareness.

Department of Defense Global Strike Joint Integrating Concept, Version 1.0.

Department of Defense Homeland Security Joint Operating Concept, Version 1.

Department of Defense Integrated Air and Missile Defense Joint Integrating Concept,
Version 1.0.

Department of Defense Joint Command and Control Functional Concept.

Department of Defense Joint Forcible Entry Joint Integrating Concept, Version .92A3.

Department of Defense Major Combat Operations Joint Operating Concept, Version 1.

Department of Defense Net-Centric Joint Functional Concept.

Department of Defense Net-Centric Operational Environment Joint Integrating Concept,
Version 1.0.

Department of Defense Seabasing Joint Integrating Concept, Version 1.0.

Department of Defense Stability Operations Joint Operating Concept, Version 1.

Department of Defense Strategic Deterrence Joint Operating Concept, Version 1.

Information Assurance Vulnerability Alert Policy Memo.

Joint Concept of Operations for Global Information Grid: NetOps.

JNN to WIN-T Transition Brief to VCSA.

Joint Pub 3-01
Joint Doctrine for Countering Air and Missile Threats.

Joint Pub 3-05.1
Joint Tactics, Techniques, and Procedures for Joint Special Operations Task Force Operations.

JSTARS Common Ground Station Operational Requirements Document.

Joint Tactical Terminal Operational Requirement Document.

Maneuver Enhancement Brigade Concept of Operations and Organization.

Special Text, 2-22.7 Cdr's Hand Book on Tactical Counter Intelligence and Human Intelligence.

TRADOC Pam 525-2-1
U.S. Army Functional Concept for See, 2015-2024.

TRADOC Pam 525-3-3
U.S. Army Functional Concept Battle Command, 2015-2024.

TRADOC Pam 525-3-4
U.S. Army Functional Concept for Strike, 2015-2024.

TRADOC Pam 525-3-6
U.S. Army Functional Concept for Move, 2015-2024.

TRADOC Pam 525-4-1
The U.S. Army Functional Concept for Sustain, 2015-2024.

TRADOC Pam 525-66
Military Operations Force Operating Capabilities.

TRADOC Pam 525-93
The Air and Missile Defense Concept.

Warfighter Information Network – Tactical, (WIN-T), Operational Requirements Document.

Warfighter Information Network – Tactical, (WIN-T), Capability Development Document.

Glossary

Section I

Abbreviations

ABCS	Army battle command system
ACUS	Army common user system
AOR	area of responsibility
ATR	aided target recognition
AMD	air and missile defense
AO	area of operations
ARCIC	Army Capabilities Integration Center
ARM	anti-radiation missile
ASAS	all source analysis system
ASM	air-to-surface missile
BCT	brigade combat team
BDE	brigade
BLOS	beyond line-of-sight
BN	battalion
C2	command and control
CBA	capabilities based assessment
CBRN	chemical, biological, radiological, nuclear
CBRNE	chemical, biological, radiological, nuclear and high-yield explosive
CCJO	Capstone Concept for Joint Operations
CCP	concept capability plan
CHAMS	counterintelligence and human intelligence automated management system
CHDD	counter human deception detection
CHARCS	counter intelligence and human intelligence automated collection and reporting systems
CHATS	counter intelligence and human intelligence automated tool set
CI	counterintelligence,
CGS	common ground system
CI/I Ops WS	counterintelligence/interrogator operations workstation
CM	cruise missile
CNA	computer network attack
CNR	combat network radio
COA	course of action
COP	common operational picture
CPE	collective protective equipment
CSB	combat support brigade
DA	Department of the Army
DCGS-A	distributed common ground system-Army
DOD	Department of Defense
DOTMLPF	doctrine, organizations, training, materiel, leadership and education, personnel, and facilities
EA	electronic attack
EMP	electromagnetic pulse

EW	electronic warfare
FCS	Future Combat System
FIRRE	family of rapid response equipment
FoS	family of systems
FW	fixed-wing
GIG	global information grid
GIS	geographical information system
HQ	headquarters
HUMINT	human intelligence
ICBM	intercontinental ballistic missile
IED	improvised explosive device
IEW	intelligence electronic warfare
IMINT	imagery intelligence
IMS	intelligent mine system
IPE	individual protective equipment
IRBM	intermediate-range ballistic missile
ISR	intelligence, surveillance, and reconnaissance
ITRT	individual tactical reporting tool
JC2	joint command and control
JF	joint force
JFC	joint force commander
JIC	joint integrating concepts
JIOC-I	joint intelligence operations capability-Iraq
JIM	joint, interagency and multi-national
JOC	joint operating concept
JOEF	joint operational effects federation
JSTARS	joint surveillance target attack radar system
JTF HQ	joint task force head quarters
JWARN	joint warning and reporting network
LCR	large-caliber rockets
LOC	line of communications
MASINT	measurements and signatures intelligence
MCO	major combat operation
MCOO	modified combined obstacle overlay
MI	military intelligence
MOUT	military operations on urban terrain
MP	military police
MRBM	medium-range ballistic missile
NETOPS	network operations
NLOS	non-line-of-sight
O&O	operational and organizational
ORD	operational requirements document
OV-5	operational activity model
RAM	rockets, artillery, and mortars
RCS	radar cross section
ROMO	range of military operations

TRADOC Pam 525-7-1

RW	rotary-wing
SA	situational awareness
SBCT	Stryker brigade combat team
SIGINT	signal intelligence
SLBM	sea-launched ballistic missile
SO	stability operations
SoS	system of systems
SRBM	short-range ballistic missile
SU	situational understanding
TBM	tactical ballistic missile
TIC	toxic industrial chemical
TIM	toxic industrial material
TRADOC	U.S. Army Training and Doctrine Command
UAS	unmanned aerial system
UAV	unmanned aerial vehicle
UGS	unattended ground sensor
UP	unit protection
U.S.	United States
UV	unmanned vehicle
WIN-T	warfighter information network-tactical
WMD	weapons of mass destruction

Glossary

Section II

Terms

act first

The combat battalion acts first, initiating decisive combat at its chosen time and place. Wide dissemination of mission-type orders that enable decentralized operations within the commander's intent coupled with broad access to the COP provide unprecedented opportunities for subordinate initiative to exploit enemy vulnerabilities as openings present themselves. To act first, leaders, systems, and units must have information dominance and be capable of moving, shooting, and reengaging faster than the enemy with assured first round kill potential.

adversarial intelligence

Any entity that focuses collection efforts on collecting information or material concerning U.S. personnel, activities, operations, plans, equipment, facilities, publications, technology or documents, either classified or unclassified without official consent of designated U.S. Release authorities, for any purpose that could cause damage or otherwise adversely impact the interests of national security or the U.S. or its ability to fulfill national policy and objectives. Threats include, but are not limited to any (U.S., allied, coalition, friendly, competitor, opponent, adversary or recognized enemy) government or non-government organizations, companies, businesses, corporations, consortiums, groups, agencies, cells, person or persons; terrorist, insurgent, guerrilla, criminal affiliated and non-affiliated entities whose demonstrated actions, views or opinions are inimical to U.S. interests. (Not approved in doctrine and policy, but used in CAR, DCD conceptual documents instead of the old HOIS (hostile intelligence services) or FIS (foreign intel services)).

beyond line-of-sight (BLOS)

An extension of traditional direct fire that extends the range to the next terrain compartment. BLOS enables standoff engagements at greater ranges and also opens up fields of fire previously denied to firing elements due to the restrictions of intervening terrain, adverse weather effecting LOS engagement or range to the target. The sensor, decider and shooter are resident within the same echelon, typically company level and below. BLOS is still direct fire in that the gunner pulling the trigger sees the target directly through a sensor. The crew can identify the target, clear ground fires to prevent fratricide, and is responsible for avoiding collateral damage and complying with rules of engagement. (FCS ORD).

blocks I, II, III

Blocks I, II, and III are terms used in the concepts / requirements COP to define increment delivery periods.

chemical, biological, radiological and nuclear (CBRN)

Pertaining to all of the individual aspects of persistent and non-persistent chemical warfare agent attack, intentional or unintentional toxic industrial chemical release, biological warfare agent or toxin attack, release of non-fissionable radioactive material, and nuclear bursts.

classification

The systematic arrangement in groups or categories according to established criteria. When you reach the second level of acquisition, you can place the object within a category. For instance you may detect a potential target and know it is a tracked vehicle, but nothing else. (JP1-02).

command and control (C2)

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1-02).

common operational picture (COP)

A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 1-02).

computer network attack (CNA)

Operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 1-02).

concept capability plan (CCP)

Describes the application of elements of joint and Army concepts to selected mission, enemy, terrain and weather, time, troops available, and civilian conditions. It is typically more illustrative and descriptive than a concept, and more focused in its purpose. A CCP includes one or more illustrative vignette(s) for a specific scenario and a set of distinguishing principles applicable to a particular operation. It may include multiple illustrative vignettes for specific mission, function, or operation from the range of military operations. The CCPs provide architecture data to support experimentation and the continuous refinement of the concept and architecture. The CCPs have the narrowest focus of all concepts in order to derive detailed required capabilities and operational architectures. The CCPs include the required details to initiate the capabilities based assessment within the joint capabilities integration and development system. (TRADOC Reg 71-20).

enemy warn operations

Enemy warning may be executed through specific nonlethal capabilities that interrogate, challenge, and warn an enemy that further action (hostile or presumed hostile) will result in increasingly lethal U.S. counter action. These enemy warnings will be effective against air, ground, CBRNE, electronic and intelligence threat capabilities. (UP CCP).

family of systems

A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation. (Mission Need for Future Combat Systems (AROC); (JROC) CJCSI 3170.01B, Requirements Generation System).

finish decisively

Small units and subordinate teams of teams finish decisively by well-timed tactical assaults, then transition rapidly to exploitation or the next engagement without allowing the enemy time or opportunity to regroup or continue the fight. All this must be done against an enemy who will know our capabilities and be imaginative and adaptable in seeking to counter every action we take. Application will be neither easy nor according to formula.

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. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. The GIG supports all DOD, National Security, and related intelligence community missions and functions (strategic, operational, tactical and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. (Defense Information Systems Agency definition contained in DOD Chief Information Officer Guidance and Policy Memo No. 11-8450, DOD GIG Computing Signed by the Deputy SECDEF).

hemispherical

A 360 degree lateral and 180 degree vertical half sphere of space over a platform or point on the operational environment. Like an upside down bowl. (FCS ORD).

identification

The process of determining the friendly or hostile character of an unknown detected contact. In arms control, the process of determining which nation is responsible for the detected violations of any arms control measure. In ground combat operations, discrimination between recognizable objects as being friendly or enemy, or the name that belongs to the object as a member of a class. (JP 1-02).

information assurance

Information operations 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 1-02).

information management (IM)

The provision of relevant information to the right person at the right time in a usable form to facilitate situational awareness and decisionmaking. It uses procedures and information systems to collect, process, store, display, and disseminate information. (FM 3.0).

information operations

Actions taken to affect decisionmaking processes, information and information systems of adversaries and influence those of others, while protecting friendly decisionmaking processes, information and information systems.

integrated capability development team

An integrated team made up of people from multiple disciplines formed to develop a CCP, perform the CBA to identify capability gaps, identify non-materiel and/or materiel approaches to resolve those gaps, and develop an ICD and/or DCR, when directed. (TRADOC Reg 71-20).

joint functional concept

Joint functional concept applies elements of the CCJO solution to describe how the future JF, 8-20 years in the future, will perform a broad military function across the full range of military operations. The joint functional concept identifies the capabilities required to support JF operations as described in the JOCs. It also identifies the attributes to compare capability alternatives and measure achievement. Joint functional concepts provide functional context for JOC and JIC development. (CJCSI 3010.02B).

LandWarNet

LandWarNet is the Army's contribution to the GIG that consists of all globally interconnected, end-to-end set of 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 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.

modularity

An organization or piece of equipment designed with standardized sizes or dimensions for flexible usage. The characteristic of the future Modular Force that enables it to attach and detach current, SBCT, and/or objective subordinate elements without sacrificing operational momentum or flexibility. (Webster's Dictionary).

near real-time

Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02).

network operations (NETOPS)

An organizational and procedural framework for integrating Network Management (NM), Information Dissemination Management (IDM) and Information Assurance. (FCS ORD).

nonlethal effects

The capability to incapacitate, suppress, disperse, or engage personnel, places, or things; deny personnel access to, use of or movement through a particular area / point / facility; deny vehicles access to, use of or movement through a particular area / point; alter terrain / environmental

conditions to favor “blue”; influence actions of others; and, separate combatants and noncombatants.

nonlethal weapons

Weapons that are explicitly designed and primarily employed so as to incapacitate personnel or material, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment. (JP 1-02).

non-line-of-sight

The sensor, decider, and shooter are not, in some combination, part of the same echelon. The sensor detects a target, the decider tasks the shooter, and the shooter shoots. This type of engagement assumes no exposure of the shooter to the target.

operational environment

Composite of all conditions, circumstances, and influences which affect the employment of military forces and bear on the decisions of the unit commander. (JP 1-02).

real-time

Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. (JP 1-02).

recognition

The determination by any means of the individuality of persons, or of objects such as aircraft, ships, or tanks, or of phenomena such as communications-electronics patterns. In ground combat operations, the determination that an object is similar within a category of something already known; for example a tank, truck, or man. (JP 1-02).

reengage at will/transition to subsequent engagements

Capability of the force to maintain relentless pressure on the enemy. Keeping the enemy continuously engaged deprives him of the opportunity to reconfigure effectively, conduct counterattacks, or reconstitute forces. In addition, it is a critical means for thwarting the enemy’s likely strategy of attrition to prolong battle, delay decision, and avoid disintegration. Each successful successive engagement can further serve to accelerate higher-level decision. Several conditions must be met to permit the force to conduct sequential engagements without pause. First, the initial engagement must itself be completed rapidly (reinforcing the significance of the tactical disintegration possible through shock, surprise, and speed—the ambush dynamic). Second, through exploitation of higher echelon fires and effects, maneuver forces must preserve sufficient combat power and on-board consumables to permit an immediate subsequent engagement. In addition, higher tactical commanders must already be shaping favorable conditions for the subsequent engagement, including sharing the burden of planning and analysis and extending the tactical infosphere and situational understanding required for the force and subordinate echelons to rapidly complete planning and execute immediate follow-on missions.

see first

The future Modular Force will possess the capability to see first by detecting, identifying, and tracking the individual components of enemy units.

shaping operations

Shaping operations at any echelon create and preserve conditions for the success of the decisive operation. Shaping operations include lethal and nonlethal activities conducted throughout the AO. They support the decisive operation by affecting enemy capabilities and forces, or by influencing enemy decisions. Shaping operations use all elements of combat power to neutralize or reduce enemy capabilities. They may occur before, concurrently with, or after the start of the decisive operation. They may involve any combination of forces and occur throughout the AO. (FM 3.0).

situational awareness

The perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the future. In generic terms the three levels of situational awareness are level 1 (perception) level 2 (comprehension) and level 3 (projection). There is both individual and group (sometimes called Team) situational awareness.

situational understanding

Achieved when a decisionmaker or other human-in-the-loop analyzes the SA and is able to use that information to appreciate and comprehend the state of the battlefield and future adversarial courses of action, branches, and sequels. It is the product of applying analysis and judgment to the COP to determine the relationships among the factors of mission, enemy, terrain, troops, time, civil considerations. (FCS ORD, 30 June 2004).

stability operations

Stability operations promote and protect U.S. national interests by influencing the threat, political, and information dimensions of the operational environment through a combination of peacetime developmental, cooperative activities and coercive actions in response to crisis. Regional security is supported by a balanced approach that enhances regional stability and economic prosperity simultaneously. Army force presence promotes a stable environment. (FM 3.0).

system of systems

A set or arrangement of systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. (CJCSI 3170.01).

understand first

Understand first with combat information on terrain and weather, the future Modular Force will develop the situation out of contact, and establish a dynamic tactical information sphere in order to determine when and where to fight on favorable terms, set conditions (isolate and shape) for one or more engagements, and maneuver rapidly on separate axes to positions of advantage,

from which tactical units can move quickly to envelop without the need first to fix the engaged enemy force.

unit protection

Is the integration of active and passive capabilities and processes, provided to operational and/or tactical units, across the ROMO to protect unit personnel, assets, and information against traditional, catastrophic, disruptive and irregular; ground, air, CBRNE and electronic hostile threats, in order to conserve unit fighting potential so it may be applied by commanders at the decisive time and place. (UP CCP).

