

ARMY SCIENCE BOARD

FY2000 SUMMER STUDY

FINAL REPORT



DEPARTMENT OF THE ARMY
ASSISTANT SECRETARY OF THE ARMY
(ACQUISITION, LOGISTICS AND TECHNOLOGY)
WASHINGTON, D.C. 20310-0103

“TECHNICAL AND TACTICAL OPPORTUNITIES FOR REVOLUTIONARY ADVANCES IN RAPIDLY DEPLOYABLE JOINT GROUND FORCES IN THE 2015-2025 ERA”

VOLUME III INFORMATION DOMINANCE PANEL REPORT

Distribution Statement:
Approved for public release; distribution is unlimited

DISCLAIMER

This report is the product of the Army Science Board (ASB). The ASB is an independent, objective advisory group to the Secretary of the Army (SA) and the Chief of Staff, Army (CSA). Statements, opinions, recommendations and/or conclusions contained in this report are those of the 2000 Summer Study Panel on "Technical and Tactical Opportunities for Revolutionary Advancements in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era" and do not necessarily reflect the official position of the United States Army or the Department of Defense (DoD).

CONFLICT OF INTEREST

Conflicts of interest did not become apparent as a result of the Panel's recommendations.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Hwy, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington D.C. 20503.			
1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE April 2001	3. REPORT TYPE AND DATES COVERED Army Science Board – FY2000 Summer Study	
4. TITLE AND SUBTITLE Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era - Volume III - Information Dominance			5. FUNDING NUMBERS N/A
6. AUTHOR(S) Information Dominance Panel Chairs: Dr. Philip C. Dickinson, LTG John W. Woodmansee (USA, Ret.) , Gen James P. McCarthy (USAF, Ret.) Panel Members: Mr. John Cittadino, Dr. Derek Cheung, Ms. Christine Davis, Dr. James R. Fisher, Mr. Jerome S. Gabig, Ms. Dixie Garr, Mr. Gary Glaser, Dr. Lynn Gref, Dr. John Holzrichter, Ms. Suzanne Jenniches, Dr. Don Kelly, Mr. Kalle Kontson, Mr. David Martinez, Dr. Rey Morales, Dr. Prasanna Mulgaonkar, Dr. Sam Musa, Dr. James A. Myer, Dr. William Neal, Mr. John Reese, Dr. Stuart Starr, Mr. Alan Schwartz, Dr. Nick Tredennick, Dr. Robert Ziernicki			N/A
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(ES) EXECUTIVE SECRETARY Army Science Board SAAL-ASB 2511 Jefferson Davis Highway Arlington, VA 22202-3911			8. PERFORMING ORGANIZATION REPORT NUMBER N/A
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) GEN JOHN M. KEANE VICE CHIEF OF STAFF UNITED STATES ARMY 201 ARMY PENTAGON WASHINGTON, DC 20310-0201 GEN JOHN G. COBURN COMMANDING GENERAL UNITED STATES ARMY MATERIEL COMMAND 5001 EISENHOWER AVENUE ALEXANDRIA, VIRGINIA 22333-0001 MG CHARLES C. CANNON, JR. ACTING DEPUTY CHIEF OF STAFF FOR LOGISTICS UNITED STATES ARMY 500 ARMY PENTAGON WASHINGTON, DC 20310-0500 GEN JOHN N. ABRAMS COMMANDING GENERAL U.S. ARMY TRAINING AND DOCTRINE COMMAND FORT MONROE, VIRGINIA 23651-5000 LTG JOHN COSTELLO COMMANDING GENERAL U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND 1941 JEFFERSON DAVIS HIGHWAY, SUITE 900 ARLINGTON, VIRGINIA 22202			10. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A
11. SUPPLEMENTARY NOTES N/A			
12A. DISTRIBUTION/AVAILABILITY STATEMENT Approved for Public Release; distribution is unlimited			12b. DISTRIBUTION CODE A
13. ABSTRACT (Maximum 200 words) The Army Science Board was tasked to seek revolutionary possibilities for improving deployability as well as effectiveness of future joint ground combat forces. The study focused on the possibilities inherent in the Future Combat System(FCS) and also considered enhancements possible through the Future Transport Rotorcraft (FTR). Study efforts were conducted by four major Panels analyzing: Operations, Information Dominance, Sustainment and Support, and Training. The study concludes: 1) the FCS concept is sound, but senior level attention is required to ensure technologies are ready for 2006 FCS EMD; and 2) Key technologies will significantly improve force projection and combat power. The Information Dominance Panel was tasked to: 1) Assess required sensors at National and Theater level; 2) Assess the technological opportunity to provide necessary bandwidth for data, voice and video requirements; 3) Ascertain the requirements to deny the threat necessary voice and data information; 4) Assess the ability to link all via internetted non-line-of-sight communications systems. The Central Recommendation is to develop a Tactical Infosphere (TI) for the Objective Force. Subordinate recommendations include: Develop DTLOMS to support the Tactical Infosphere; Establish a program to demonstrate and evaluate TI operational concepts & determine technology shortfalls and system needs; Establish a test unit, a Bn slice of the Objective Force; Establish a simulation test bed; and, Build on current digitization capability.			
14. SUBJECT TERMS Information Dominance, Global Information Grid, GIG, Battlespace Infosphere, Tactical Infosphere, sensors, communications, Information Management, UAVs, C4ISR, Position, Navigation, Time, Pos/Nav/Time, RSTA, Future Combat System, FCS, Situational Awareness, Systems Engineering, Organic Sensors, ATR			15. NUMBER OF PAGES 230
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THE PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT None

FY 2000 Summer Study Report Format

The FY 2000 Summer Study has been published in 5 volumes.

- Volume I - Executive Summary**
- Volume II - Operations Panel Report**
- Volume III - Information Dominance Panel Report**
- Volume IV - Support and Sustainment Panel Report**
- Volume V - Training Dominance Panel Report**

If you received only the Executive Summary, the additional volumes may be reviewed and/or downloaded by visiting

<http://www.saalt.army.mil/sard-asb/> and clicking on “Studies.”

Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

Information Dominance Panel Report

Table of Contents

Information Dominance Panel Report	1-43
Appendices	
Appendix A: Terms of Reference	A-1
Appendix B: Participants List	B-1
Appendix C: Organizations Visited	C-1
Appendix D: Information Management	D-1
Appendix E: Communications	E-1
Appendix F: RSTA	F-1
Appendix G: UAVs	G-1
Appendix H: Pos/Nav/Time	H-1
Appendix I: Protect and Counter	I-1
Appendix J: System Engineering and Integration	J-1
Appendix K: Technology Assessment	K-1
Appendix L: Acronyms	L-1
Appendix M: Final Report Distribution	M-1



Information Dominance through



Tactical InfoSphere



The Thrust of the TOR

To provide information dominance through ..
an advanced "Central Nervous System"
to meet our force needs and
deny the threat its basic information needs.

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 2

The Terms of Reference (TOR) challenged the ASB to define a new solution to the command and control of the Objective Force. The TOR is included at Appendix A.

The operative phrase of the TOR is the statement quoted above - define an advanced "central nervous system" for the Objective Force, circa 2010 to 2015. In analyzing this problem we have derived a "Central C4ISR System" dubbed the Tactical InfoSphere (TI). The panel believes that the TI can provide a capability to the Objective Force analogous to the central nervous system of the human being. In the body of this report, we outline the components, capabilities and the processes to achieve the TI.

The membership of the study panel is given in Appendix B and included a rich mix of technicians, active duty and retired operators as well as senior retired Army and Air Force flag officers. The ASB members were augmented and assisted by senior technicians from the Army ARDECs, the Department of the Army and the TRADOC.

Appendix C identifies these offices and agencies with which we interacted over the course of the study. We appreciate the open discussion afforded these many groups and sincerely appreciate their support.



Structure of This Report

- **Introduction of the Problem**
- **An overview of the Tactical InfoSphere**
- **Challenges and solutions***
 - Information management
 - Communications
 - RSTA
 - UAVs
 - Position location, Navigation and Time
 - Protect and Counter
 - System engineering and integration
- **Technology Assessment**
- **Overall Observations and Recommendations**

* Each Area is expanded in an Appendix

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 3

This report is structured into four major sections.

First, the problem is outlined, as the panel understands it. Our solution derives from the recent Chief of Staff guidance as it impacts the realm of C4ISR.

Next the TI is defined and examples of its impact on operations are articulated. The seven technical areas defined above are addressed in a brief overview within the body of the report. In addition, each area is discussed in detail in Appendices D through J.

A brief review of the enabling technologies is included in "stop light" form. It clearly conveys the message that either the technology to support the objective force is in hand or achievable with some focused effort. However, the programmatic to support the technology development and funds to engineer the system are sorely lacking.

Finally, a series of recommendations are presented which define the necessary processes to acquire the TI.



Information Dominance



$$\text{Information Dominance} = \frac{\text{Blue Information}}{\text{Red Information}} \gg 1$$

- **Locate enemy targets in a timely and efficient manner.**
- **Deny the enemy the ability to locate and identify our Forces in a timely manner.**
- **Get the right information to the right echelons in the right format at the right level of detail at the right time.**
- **Deny the enemy's ability to attack our information systems and employ cover, concealment and deception**

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 4

To obtain Information Dominance on the battlefield, our forces must have much better information and knowledge than that available to the threat (i.e., the ratio of blue information to red information should be considerable greater than one). When this condition occurs, it can lead to rapid and effective decision-making, which in turn can ensure that our forces have operational dominance.

Information Dominance is not a "part time job," rather, it is a necessary condition - day, night and in inclement weather. The capability to locate enemy targets quickly and reliably with the complementary ability to deny the threat an accurate picture of our forces and their disposition, can greatly increase the lethality and the survivability of the Objective Force. However, the capability to do effective RSTA pays off only if the targets detected are reported to decision-makers and weapons, essentially instantaneously. Finally, the actions to deny the enemy's ability to attack our TI, to disrupt his information systems and his capability to employ cover and deception are essential to maintaining our information dominance.



C4ISR in the Objective Force

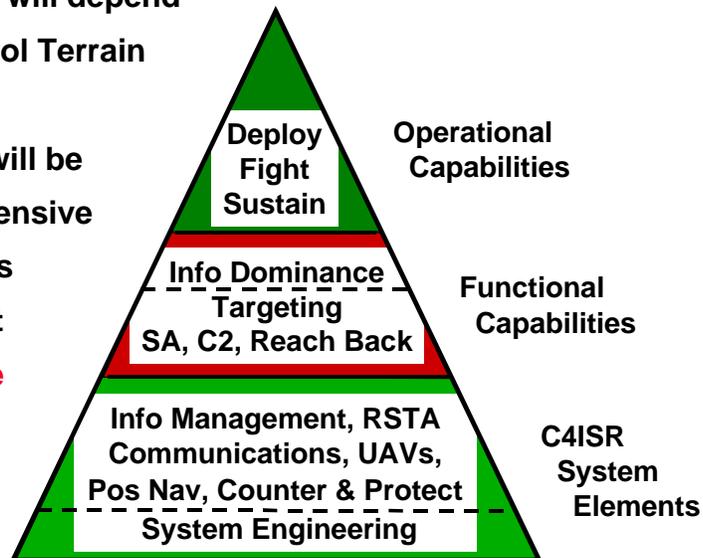


- **Operational Force will depend on C4ISR to Control Terrain and to Survive**

- **Adequate C4ISR will be complex and expensive**

- **Recommendations are extensive, but**

The Objective Force Requires a Robust Solution



Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

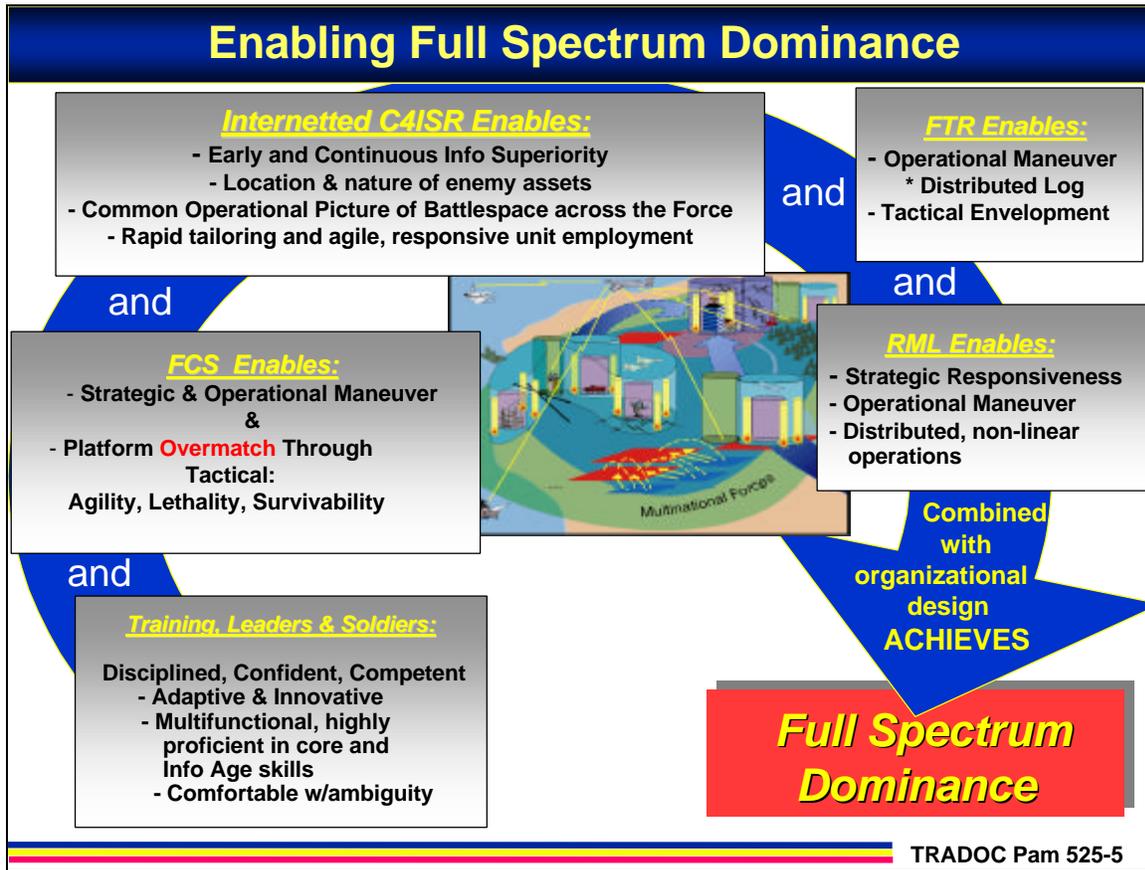
Page 5

As implied by this figure, C4ISR will be the foundation of the Objective Force.

The Chief of Staff has challenged the Army to develop an Objective Force with the unique capabilities to deploy, fight and sustain. Underlying these operational capabilities are supporting functional capabilities that include information dominance, targeting, Situational Awareness (SA), Command and Control (C2), and reach back. Information dominance is an integrating concept that argues that we must have superior information on enemy disposition and activities relative to his knowledge of us. Targeting is the process which supports determining potential target sets, recognizing and tracking them on the battlefield, matching firing systems with targets, delivering munitions and assessing the results. Situational Awareness (SA) is the integration of friendly and enemy dispositions, force status, and environmental factors such as weather, terrain, and civilian population. Command and Control (C2) supports decision-making, leading, and control of the force. Reach back refers to those processes that support access to assets outside the theater or in sanctuary that can directly support operations inside theater.

Underlying these functional capabilities are the technical systems, which enable C4ISR. These systems have been subdivided to facilitate analysis of each component. They include Communications, Reconnaissance Surveillance and Target Acquisition (RSTA), Unmanned Aerial Vehicles (UAVs), information management, counter C4 and C4 protection, position location and navigation, and systems engineering. Each element incorporates existing programs in the C4ISR development community as well as important new capabilities. Placing system engineering at the foundation connotes a need to orchestrate these disparate elements into a single integrated system to meet these challenging operational needs. Each of these elements is further defined and discussed in the Information Domination report.

C4ISR will play a critical role in the Objective Force, but the solution will be complex and expensive. This report offers recommendations directed toward the implementation of a robust, integrated solution.



Taken from TRADOC Pam 525-5, Draft, this chart illustrates the role of C4ISR as a force enabler.

Interestingly this graphic summarizes all the elements of this Summer Study, highlighting training, logistics, both the FCS and the FTR, as well as C4ISR. Thus, the TRADOC has articulated the importance of C4ISR as an element of the Objective Force supporting the FCS and FTR. This report defines an integrated set of C4ISR systems as the TI. Our analysis indicated that the TI is as important as the FCS and FTR to the success of the Objective Brigade. The presence of networked communications together with real time sensor capabilities can indeed provide the "Early and continuous Situational Awareness" call for by the TRADOC. By developing the C4ISR as a full partner to the weapons platforms, the TI will be much more effective than if these capabilities are added to the force as afterthoughts on a piece meal basis.



Assessment: Planned Systems For Fielding Against 2010 Needs



Army Vision 2010 Needs	Echelon		
	Corps & Above	Division	Brigade & Below
Communications (Advance MILSATCOM Architecture)	G	G	R
ISR (FIA; IOSA II)	G	Y	R
Weather & Terrain (NPOESS)	Y	Y	R
POS/NAV (Modernization; NAVWAR)	G	Y	Y

G = Satisfactory
Y = Marginal
R = Inadequate

ASB space Study 98

Communications, ISR and Met data were judged to be Red below brigade... and the requirements for the Objective Force just got a lot tougher!!

Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

Page 7

This chart comes from the 1998 Army Science Board Summer Study: "Prioritizing Army Space Needs". The time frame for that study was an objective force in 2010. The study looked at Space services in the four categories shown in column one: Communications; Intelligence, Surveillance and Reconnaissance (ISR); Weather and Terrain; and Positioning, Navigation and Timing (PNT).

An overall conclusion of the study was that Space "services" in general were satisfactory (and highly desirable) at the higher echelons (CINCS, JTF and Corps), but that they provided little support to the lower echelons. The three principal drivers creating this phenomenon were:

- The time line requirements at the upper levels were in the order of hours or fractions of hours vice minutes and seconds in the maneuver units;
- Infrequent, non-continuous coverage and limited throughput capacity of space assets will be limited for the foreseeable future; and
- Upper echelons, Corps, ARFOR and the JTF will invariably exercise their command prerogative to address their own needs with these scarce resources.

In the analysis of each of the categories, the study panel assumed that all of the improvements and additions contained in the FY99 Army POM and DOD Space Master Plan would be completed as planned. Then the panel examined the situation at three echelons: Corps and Above, Division and Brigade and Below. The analysis indicated (as shown as red on the chart) that a marriage of projected Space capability to planned terrestrial capability still produced significant deficiencies in Communications, ISR and Met/Terrain Data at Brigade and Below (B&B).

This current panel has reviewed the results of the space study and has found that the Army has proceeded to make many of the planned improvements, but the 1998 assessment remains valid today. Satellite capacity is still limited below the Brigade, timelines for intelligence and sensor data are too long and local weather and terrain data is not sufficiently accurate for many of the Brigade tactical operations. The panel notes that the original assessment was done against the Force XXI Army and that the operations postulated for the Objective Force are far more challenging.

Enabling Tactical Information Superiority

- **Locate the Enemy,**
 - Mix of Sensors
 - Report Automatically
- **Communicate,**
 - New Radios
 - Integral Routers
 - Airborne Relay
- **Synthesize Reports,**
 - Minimize clutter,
 - Highlight Threats
 - Display Relevant Real Time Tactical Information
- **Airborne, UAV, Ground Sensors, Robust GPS,**
 - SIGINT, FOPEN, MTI/SAR, Retro-Optic, etc
 - Automatic Target Detection, ATR (?)
- **Enable Real Time distribution to all users**
 - Increased Bandwidth to Handle Traffic
 - Manage Traffic flow, Minimize Latency
 - UAVs to Support Communications BLOS
- **Deliver Tailored Combat Information**
 - Flush data outside the Area of Interest,
 - Correlate like Reports, Fuze information
 - Relate to terrain, maps, DTED >4
 - Interface to the Warfighter

Without a “System” Dedicated to the Tactical Warfighter, the Picture Will Be Late and Incomplete!

Information superiority will be critical to the Objective Force and will prove to be a challenge to define, develop, field and train.

The solution depends on a chain of events - all of which are critical to meeting the needs of tactical operations. Meeting the timelines inherent to the mobility of the Objective Force will require the move from the classic approach to battlefield intelligence to an automated process dedicated to the tactical force which produces *Combat Information*. Technology has advanced to the point where it is not necessary for analysts to evaluate imagery and other sensor products to produce useful information, and intelligence personnel are not required to assist in the processing of sensor data and operational reports to produce an adequate picture of the battlefield.

The process defined includes three principal capabilities; 1) the ability to find and automatically report the presence of likely / potential enemy elements; 2) the capability to route these reports over the battlefield to all warfighters in the vicinity with essentially no delay; and 3) automated processes capable of condensing a rich and rather noisy stream of information into a coherent picture of the battlefield. The intense nature of the close battle requires information in near real time, *in seconds at most, not minutes*.

Find and Report

The problems associated with finding a dispersed enemy whose forces may wear blend into the environment or who move about the AO in armed pickup trucks has faced our forces in Vietnam, Somalia and Bosnia. The irregular nature of many threats and the unforgiving terrain in which they operate requires a rich mix of sensor capabilities.

- SIGINT systems have the capability to detect, and locate to some degree, and usually identify radio and radar transmitters. The ability to detect and provide a line of bearing to a forward

observer (who may be the local farmer) who is sending a spot report or calling for preplanned fires, can improve force survivability.

- FOPEN Radars have progressed to the level where they can detect and determine the overall dimensions of metallic objects in heavy foliage. They are unlikely to be able to identify these objects. This level of warning might be likened to the radar warning on an aircraft - one may do additional scouting in the area or may make the decision to avoid an unnecessary encounter.

- MTI and SAR Radars have the ability to monitor large areas for movement (MTI: Moving Target Indicator) and to provide day / night all weather imaging capability to "check out" suspicious entities on the battlefield.

- Retro-Optic sensors employ a low power laser to scan for optical systems that are pointed toward the sensor. When the sensor detects an optical system it can produce very accurate azimuth, elevation and range to the device.

- Automatic processing of the sensor data can convert an identified radio signal, or an image into a SALUTE like report (at this time there is an object at location x, y), in digital form, for transmission to the troops. The level of description of the target will vary from a SIGINT report that it has found a Gun-Dish radar associated with a ZSU-23 4, to a FOPEN radar which might report a tank sized blob.

Communicate the Results

To route critical information across the battlefield in near real time will require much greater bandwidth than that afforded by current radios. A wideband version of the JTRS radio will be necessary with an embedded router to support the direction of traffic to those who need it. To connect elements of a dispersed force beyond the line of sight, radio relay packages on UAVs will provide the connectivity. This communication network is an evolution of the current two-dimensional digitized battlefield into a three-D configuration.

The traffic routing on this network will rely on Internet protocols, with extensions to accommodate the fact that the entire network is moving. This contrasts with the fixed infrastructure of the commercial world.

Synthesize Reports

To minimize the clutter and noise presented to the warfighter a number of automated functions must be performed. At the combat platform level all incoming reports will be screened with the following possible outcomes:

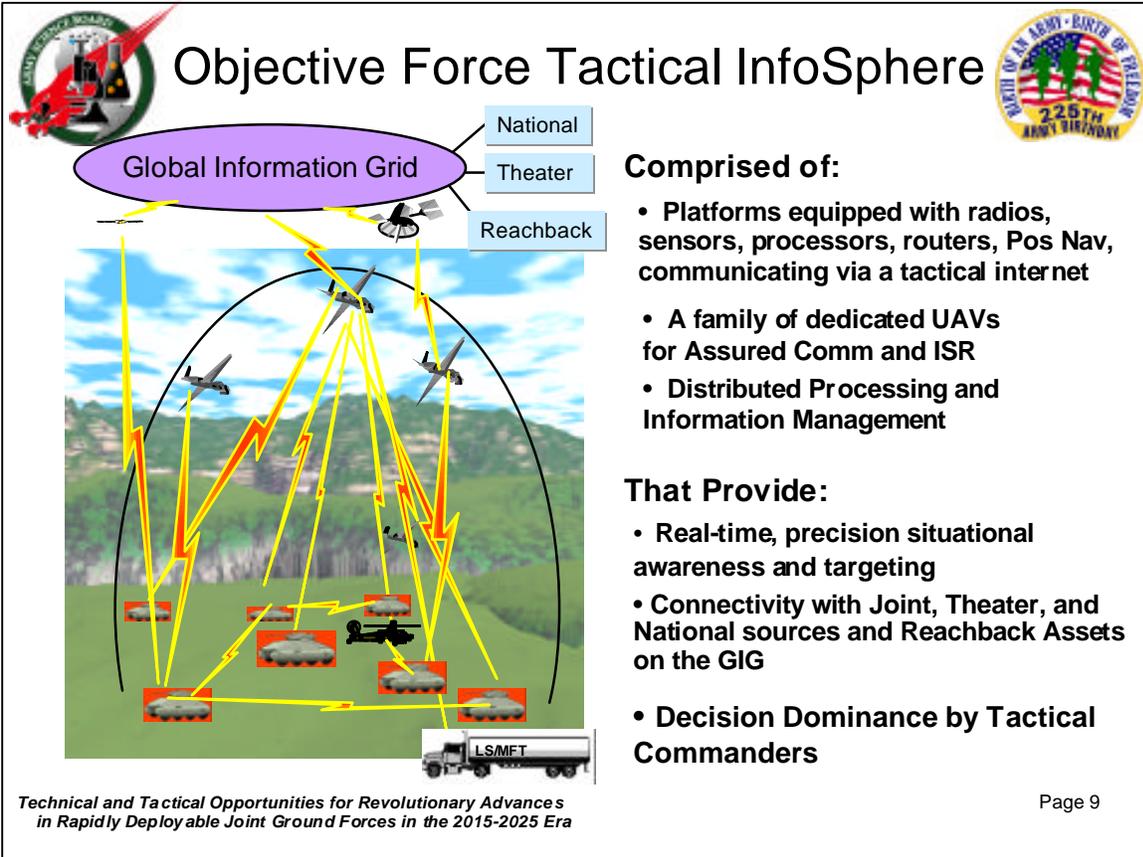
- If the event reported lies outside the operators predefined area of interest (more than 5km away) or if it is an event he has "instructed" the system to ignore, it will be discarded.

- If duplicate or repetitive reports are received they are correlated into a single record and shown as a single icon on his display. The record supporting the icon might include the fact that the air traffic control radar at the airport has been on for the past three days, it has been collected 500 times, its location is known and it was last seen 2 seconds ago.

- Groups of reports which fit predefined "templates" might be grouped to indicate that the vehicles and radios detected are representative of a Battalion Command Post.

An operator-defined composite of these reports would be displayed in a situation display, which would provide the option of showing digital terrain, rectified imagery and / or military maps. The object is to display the disposition of forces in a form that has the most meaning to the individual operator in the given situation.

Finally, and the most difficult, the situation must be presented to the operator in a manner which he can rapidly assimilate, with minimal intrusion into his already complex environment. This is an area that deserves a great deal of attention.



The TI is a robust set of C4ISR capabilities organized to support Army or Joint forces in the accomplishment of their tactical mission.

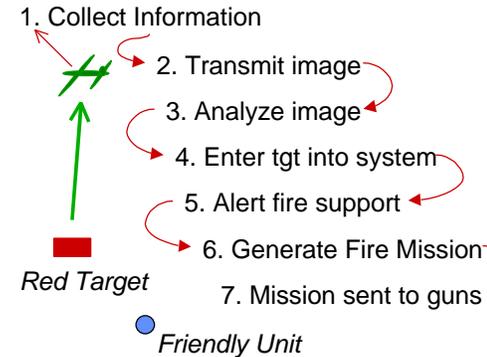
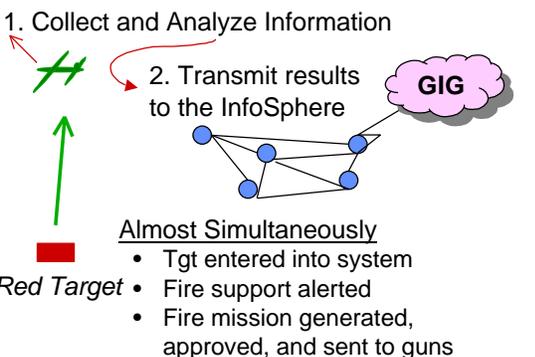
It consists of organic and dedicated sensors, a robust command and control system, rules for rapid distribution of information through the InfoSphere, and all the communication nodes of the tactical units assigned to the force concerned. This figure shows the operation of the elements of the InfoSphere.

The TI is linked through the Global Information Grid (GIG) to organizations and resources that will support the operations outside the InfoSphere. These would include tactical units and higher staffs operating in sanctuary locations; supporting National and theater assets; logistic organizations charged with pushing supplies forward; and training resources supporting mission rehearsal and maintain peak readiness while awaiting employment. The TI thus consists of any platform, on the ground, in the air, or in space, that is equipped with a radio, sensor, processor, router, and location device that participates in the information gathering and distribution for the warfighter. The information that passes throughout the TI informs, contributes to Situational Awareness, identifies the combat elements, and provides (and assists) targeting. The presence of the GIG with satellites, large high flyers, etc. will supply the connectivity to link the tactical battlefield communications with commands located in CONUS and in theater. They serve to inform lower echelons in theater of developments and intelligence information derived from high echelons.

As depicted, the TI provides an umbrella of dedicated communication relays and sensors on UAVs that will move with the tactical force. Throughout the TI, every entity on the battlefield that collects and transmits information (i.e., a sensor), moves and shoots (e.g., a tank), or provides a command function is an active node in the TI - down to and including the Future Objective Warrior.

Rules are established within the TI which permit automatic engagements when sensor-shooter conditions are met. Dedicated UAV borne sensors will have their coverage prioritized to support the critical tasks of the units within the InfoSphere. These allocations are made by the tactical commander, supported by the TI. The TI, in addition to providing the tactical force with distributed situational awareness, and rapid fire support capabilities, provides automatic engagement reports along with vehicle status reports. As an FCS unit engages an enemy force, the time, location of engaging and engaged force, the ammunition and fuel expenditure and vehicle systems status will be automatically reported. This provides near-real-time logistics status on each vehicle. If the Army decides to provide biomedical sensors to each soldier, the status of each of our fighters could also be part of the instantaneous picture. The TI is a dynamic system in which rules, sensor allocations, and databases can be accessed quickly, and modified to suit the current mission.

The presence of the TI, tied into the GIG can provide Blue Tactical Commanders Decision Dominance!

 <h2 style="text-align: center;">Legacy Systems vs. InfoSphere</h2> <h3 style="text-align: center;">Current (FXXI)</h3> <ul style="list-style-type: none"> • Some networked, many point-to-point communication; limited GIG access • MSE limits bandwidth, manually aimed and vulnerable • Stovepiped, vulnerable databases • Human intensive analysis and data transfer 	 <h3 style="text-align: center;">Future (InfoSphere)</h3> <ul style="list-style-type: none"> • Fully networked communications with GIG access at the lowest tactical levels • Wider bandwidth, robust, self-organizing, self-healing communication architecture • Integrated, distributed, virtual database • Computer intensive, smart routers and multiple levels of security
 <p>1. Collect Information</p> <p>2. Transmit image</p> <p>3. Analyze image</p> <p>4. Enter tgt into system</p> <p>5. Alert fire support</p> <p>6. Generate Fire Mission</p> <p>7. Mission sent to guns</p> <p>Red Target</p> <p>Friendly Unit</p> <p><i>Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era</i></p>	 <p>1. Collect and Analyze Information</p> <p>2. Transmit results to the InfoSphere</p> <p>Red Target</p> <p>GIG</p> <p><u>Almost Simultaneously</u></p> <ul style="list-style-type: none"> • Tgt entered into system • Fire support alerted • Fire mission generated, approved, and sent to guns <p style="text-align: right;">Page 10</p>

As an example of how current and future capabilities could differ, compare the operation of the ABCS system with the potential of the future TI.

The current system is human intensive for both analysis and information transfer. An Imagery analyst visually scans imagery and identifies potential targets. They must then manually enter the target data in a machine readable form for transmission to the Army Tactical Data System (ARTADS). These human interactions create unacceptable delays in the targeting / situational awareness processes. Future systems must be machine-intensive; using automated analysis to detect and report potential targets. Likewise the routing of the message must be fully automated, capitalizing on the multi-routing, multi-address capabilities of the Internet.

The current system has multiple, unique, stovepiped processes which have limited interoperability from one BFA to another. Future systems must capitalize on the broadcast nature of the TI to insure near real time information to all "local" warfighters. The current system makes extensive use of point-to-point communications that are minimally networked. Future systems will be totally networked, with "instant" data flow among echelons and to components over the Global Information Grid.

The current targeting process begins with manual analysis, manual data input, relay through multiple OPFACs and results in sensor-to-shooter time lines on the order of 5 to 10 minutes. Within the TI it should be possible to automatically detect a target onboard the UAV, generate a SALUTE (size, activity, location, unit, time, equipment) like, machine readable message, and route that report to: multiple fire units, a fires decision point if needed, and to all combat units in the vicinity as a situational awareness report. With current technology, there is no reason to believe the process should be longer than 5 seconds - sensor to shooter and to all local war fighters.



Structure of the Analysis



Each Element of the Solution Set Was examined in terms of Objective Force Needs:

- **Operational Challenge - nature of the problem**
- **Innovation and limitations**
- **Solution sets / examples**
- **Technology needs**
- **Recommendations**

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 12

Each of the system elements were analyzed and reported in terms of their impact on the operational capability of the force. An overview of each area is presented in the body of the report and an expanded analysis is included in appendices.

First, the nature of the problem was explored in terms of current capabilities and current programs. From this analysis certain shortcomings are identified. These problems were then evaluated in terms of the commercial and military technology to determine opportunities for innovation. Potential solutions or examples for the application of new technology are presented. The technology shortfalls were considered along with the risk associated with fully developing that technology by the Objective Force time frame. Finally, the panel presented recommendations on science and technology investments, or programmatic strategies that the Army should pursue.

Clearly, within the time and resource constraints of this study, not all these recommendations will prove to be the best course of action. Rather, they illustrate problems that severely limit the abilities of our forces today and are within the realm of a reasonable solution.



Information Management



The Tactical InfoSphere will direct relevant information to the right place at the right time in a form which facilitates decision making.

Nature of the Problem

- **Legacy systems are:**
 - Stovepiped, limited interoperability from BFA to BFA
 - Human intensive, point-to-point
- **Managing the InfoSphere:**
 - Information flow may not mirror the chain of command

Solutions

- **Information Management in the InfoSphere should be characterized as:**
 - Integrated, processing intensive, totally networked, joint through the GIG
- **Selected logic and processes of ABCS will transition to the InfoSphere:**
 - Communication, fire direction, information fusion, C2, logistics, ...
- **Need to simplify the “Business rules!” - A Requirements Challenge**

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 13

The management of Information within the TI is a major challenge in its implementation. The goal of the InfoSphere must be to direct and present relevant information to the warfighter to support decision with minimum delay.

In the interval in which the computer has had the potential to support military operations, the development of automated systems to assist battle management has proven to be very allusive. Most tactical automation has been developed as stove piped systems supporting a single battlefield functional area (BFA) with limited interoperability between these BFAs. Their operation has been characterized as human intensive. Data is often input to the system manually by an operator. The transfer of information from one system to another frequently requires an operator to reenter data into the receiving system. These delays are unacceptable in support of the tactical warfighter. These problems are further acerbated by communications systems, which are configured as BFA specific nets with limited net-to-net interoperability. The TI must enable information to flow to users in any BFA, independent of the source of the information.

One result of this shared data is the fact that information flow will quite often not duplicate the chain of command. For example a Battalion sensor flying over a Company team may detect a target in the Co area and simultaneously report its existence to the Bn, the Co and the subordinate elements of the Company in the vicinity of the target. This simultaneous "broadcast" of real time threat information is key to providing current continuous SA to the tactical elements of the Objective Force.

The objective of the TI must be an integrated communication system in which a message can automatically flow from node to node without human intervention. To achieve this capability, an intensive processing environment must implement the logic of the internet in which the router of each node "keeps book" on its connectivity to adjacent nodes and is able to determine a route or

multiple routes for information to flow. These processes are at the heart of the internet, but the TI brings an additional burden in that it is not a fixed network, but rather a mobile set of nodes connected by radio links. This radio-enabled mobile grid brings problems which are unique to the military and will require R&D to fine tune the COTS internet. The ability to reachback to units at higher echelon and to facilities in the CONUS will be enabled via the Global Information Grid that will be implemented with the compatible Internet protocols.

The unique connectivity of the TI can support unique battlefield capabilities. For example, an element of the enemy force which is found and reported by a sensor can be automatically routed simultaneously to the fires elements and to the all maneuver elements in the vicinity. This direct distribution of information then demands the development of sorting, correlation and fusion algorithms for each force element. By giving the warfighter the ability to sort out pertinent data he might define his area of interest - "show me threat activity within 5Km - that meets certain other criteria." The correlate function insures that repetitive reports of the same item - the TV transmitter in Grosnia is still on - are compressed into a single record/icon which contains the information that the transmitter is at x,y, that it has been in operation since 0600 and it was last detected 2 seconds ago. The operator sees only the icon, but can check the history if necessary. The ability to fuze the data permits the inference of larger organization or entities. For example, the Gundish radar implies the presence of a ZSU - 23-4 anti-aircraft weapon.

The Army has struggled with the problem of defining the required functionality of its battle field automation system. To achieve the realtime capability demanded of the Objective Force it will be imperative that the functional requirements be scrubbed ruthlessly to simplify the processes - and all "Bells and Whistles" must be eliminated. The focus must be on a realtime processing of critical combat information.

Success will only be achieved with new simplified business rules for the Objective Brigade. We recognize this is a very real requirement challenge.

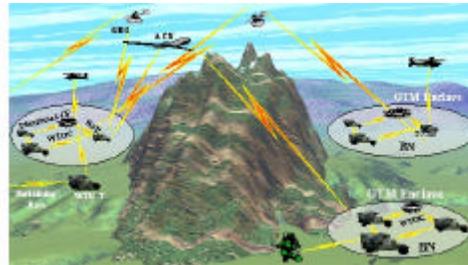


Communications

Fully networked, multi-layered, space, airborne, and terrestrial, compatible with the GIG

Nature of the Problem

- **The current communications network is:**
 - Line of sight, point-to-point, limited bandwidth
 - Multi-net with many interfaces
 - Modest Quality Of Service



Solutions

- **Every platform a Communications node**
- **Build on COTS technology, augmented by Army/DARPA R & D: mobile internet infrastructure, encryption,...**
- **Robust, self directing, self healing networked communications**
- **Refocus programs to support Tactical InfoSphere concept**
 - JTRS - Replacing SINCGARS, EPLRS, NTDR,
 - Redirect to meet Future Needs - Wideband/high data rate waveform
 - Fix Immature Hardware design concepts, Software constraints
 - MSE++/WIN-T- fully internet based
 - Integrate radios and routers on combat platforms and UAVs
 - Eliminate dedicated communications platforms below brigade

Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

Page 14

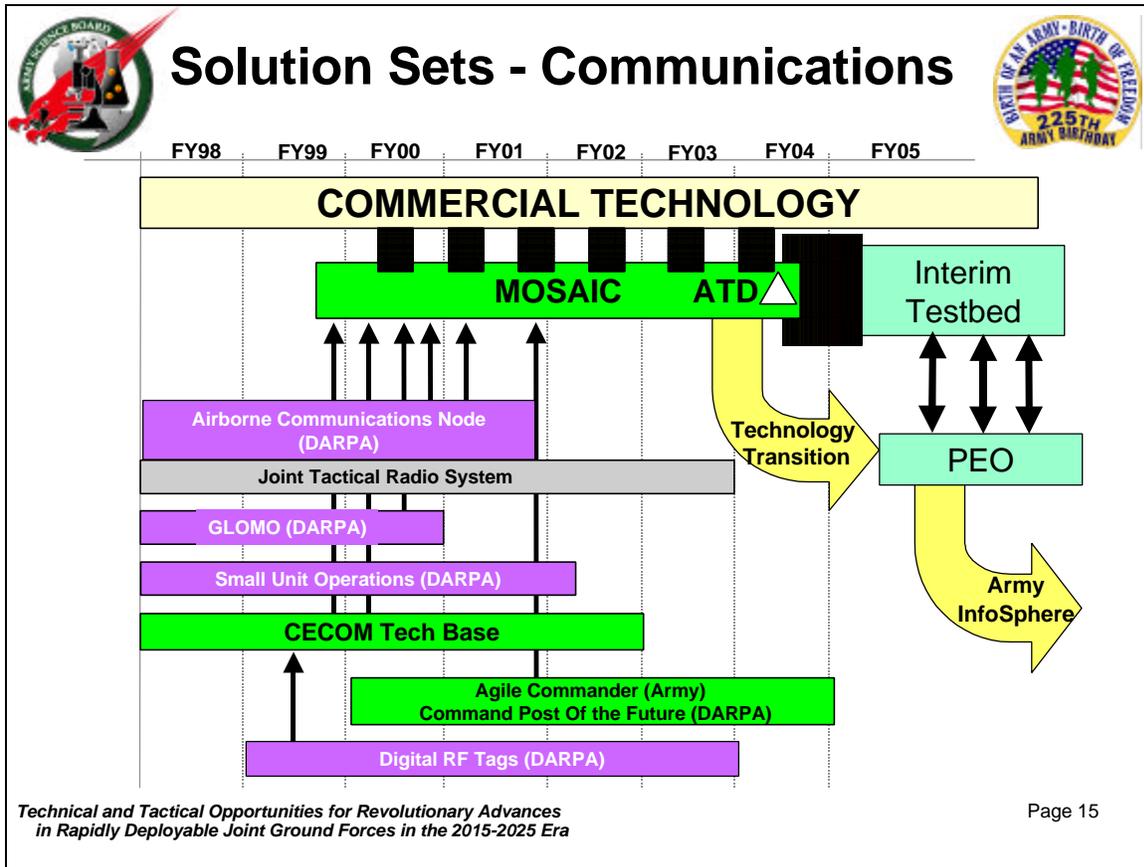
There are enormous challenges, and opportunities, in creating the communications system needed for the Objective Force.

In March 2000, the Deputy Secretary of Defense issued a Guidance and Policy Memo on the Global Information Grid. This memo described the GIG as “a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.” The next generation of communications and information systems will be designed to provide the military a networked capability largely based on the commercial Internet. The Army challenge is to develop a mobile network, compatible with the GIG, which includes the characteristics discussed below.

Existing and programmed Army communications, although adequate at the higher echelons, are woefully inadequate to support the Objective Force. Current Army terrestrial communications systems are limited to line-of-sight (LOS), point-to-point communication links. (SATCOM terminals have been issued to the Brigade, but operational experience shows that transponder access is rarely allocated at this level. Furthermore, existing data radios are severely limited in bandwidth (data throughput), are stove-piped (vertically integrated), and often have prolonged latencies resulting in missed or late messages. These limitations constrain mobile information distribution and command and control today, and are hardly adequate for the additional demands for real time SA and sensor to shooter communications.

The communication system for the Objective Force needs to be fully networked and multi-layered. The networks for this communications system will be self-directing (ad hoc) and self-healing. It must provide flexible, scalable bandwidth (data throughput) to support the information flow within the tactical AOR as well as having the reachback capability for the support of functions such as

sustainment and intelligence. By being compatible with the GIG, issues of Joint and Coalition interoperability, if not completely solved, become workable. Future JTRS radios for this system will need: built in network management, IP network compatible, wider bandwidth (data throughput), low probability of intercept and detect (LPI/LPD) waveforms, and capability to maximize and adapt the frequency of operation for any geographical region. Commercial telecommunications technologies will provide the core technologies, but must be integrated with Army/DARPA technologies and engineered to service the TI.



The adoption of COTS Internet technology to provide secure, mobile tactical communication system will require a focused effort to match the aggressive timeline of the Objective Brigade

The Army CECOM has initiated an Advanced Technology Demonstration (ATD) Program, Multi-functional On-the-move Secure Adaptive Integrated Communications (MOSAIC). The focus of MOSAIC is to demonstrate the integration of adaptive, networked communications to support a seamless flow of multimedia information across a layered (terrestrial, airborne and satellite) communications architecture. MOSAIC will: be IP-based, utilize open system standards to support maximum use of COTS products, incorporate the Joint Tactical Architecture (JTA) standards, and be fully compatible with the Global Information Grid (GIG). The goal is to accommodate the mobility of tactical elements of the Objective Force. The resulting wireless network will support: Quality of Service (QOS) for streamed services; ad-hoc networking; bandwidth management; traffic scaling and multimedia applications. MOSAIC will build on a core of commercial technology and standards that will be augmented with military capabilities (i.e., security, mobile infrastructure,) developed under Army and DARPA programs.

CECOM has released a Broad Agency Announcement (BAA) on MOSAIC and the industry response has been overwhelming. As shown, the ATD is planned for FY04. Transition to a PEO for the TI can be accomplished during FY05 with EMD decision in FY06 to match the FCS program. MOSAIC appears to provide a unique opportunity to develop the communications foundation for the Objective Force Brigades.

The MOSAIC ATD provides a roadmap for developing the communications network of the TI. KDARPA programs will directly contribute needed technology. The Airborne Communication Node (ACN) is a collection of high technology communications translation/relay capabilities targeted to become a payload for Global Hawk. DARPA has recently decided to eliminate the flight demonstration and will terminate the program with laboratory demonstrations of the developed

technology. Additional funding would allow the Army to integrate and fly the ACN payload in MOSAIC.

DARPA's Small Unit Operations (SUO) is developing advanced, military, "smart-radio" technology that will be directly integrated into MOSAIC. Important technologies being developed in SUO are: Ad hoc networking algorithms and software; LPI/LPD waveforms; mobility protocols; user terminal for Dismounted Warrior and co-site interference mitigation. Phase III will be completed in FY02 and could provide radio prototypes to MOSAIC. DARPA's GLObal MOBILE (GLOMO) Communications Program can provide key technologies in network management; routing protocols; Quality of Service (QoS); security-information assurance; survivability (self-healing algorithms and anti-jam); and dynamic channel access.

CECOM's Agile Commander and DARPA's Command Post of the Future are developing concepts in support of command and control which eliminate the "tyranny of the TOC," by enabling dispersed staff functions. These concepts and products can be integrated with the communications elements of MOSAIC to demonstrate mobile, tactical C2 and Battlespace management.

The Objective Force will require new, wideband digital radios with much greater bandwidth to support realtime battle management, The Joint Tactical Radio System (JTRS) is an OSD mandated program governing the acquisition of all future DOD radios. Current plans call for some early JTRS radios to be provided to MOSAIC. These radios will provide throughput equivalent to NTDR and will also include some built-in networking features. However, a major shortfall in the current JTRS is the lack of direction that JTRS radios be either IP or GIG compliant.

MOSAIC can be an important contributor to the development of the TI. It will require program support from the Army and can benefit from "adult" supervision in the form of an industry lead "Grey beard" panel to insure the technology in the program stays in sync with the future of the Internet.



Reconnaissance, Surveillance, and Target Acquisition



“Timely, Sufficient Knowledge” rather than “Perfect, Late Information”

Nature of the problem

- FCS Platform survival will depend on avoiding “surprise encounters”.
- National, joint, and services’ RSTA not available/continuous below Brigade
- Existing Single sensor, standalone product development rather than a total battlefield awareness solution which inhibits “plug and play”.

A Systems solutions incorporates all available sensors

- Shared Information - Automated SA, targeting, ordnance awareness
- Self protection based on dedicated UAV borne and on-board sensors for continuous coverage, “instant” detection and location of threats.
- Challenges - FOPEN, mine detection, urban terrain and sensor fusion.
- A mix of sensors - RF location, retro-optics, UHF radar, SAR / MTI radar

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 16

Fighting and winning on the tactical battlefield is all about knowing where your forces are, where the enemy is and having a superior combat force. The TI will provide *Timely, Sufficient Knowledge* to enable the Objective Force to win decisively. It is not intended to provide *Perfect Late Information*.

The survivability of light, mobile FCS platforms will be enhanced by near real time situational awareness that will reduce surprise encounters. When potential threat forces are located the force will have the option of probing carefully with scouts or micro UAVs, or if it better suits the mission, bypassing the threat.

The advent of theater level reconnaissance and National Tactical Means (NTM) in the 70's and 80's has provided the JTF and the Service component commands with a robust and varied capability to manage the battle at the strategic and operational levels. However, these same capabilities do not well serve the tactical warfighters. The problem is three fold.

- The tasking process flows from the company / battalion up through the Corps and thence to the JTF where it competes with the other Service needs and the CINC's demands. This process is not real time and the needs of the tactical user seldom make the cut. Further - the platform may not be available at the desired time.
- None of these collectors operate in a real time mode. A variable time delay occurs because there is either a human and / or a ground station in the loop.
- As noted earlier, the stated need is for *continuous SA*. The NTM does not now provide this staring capability and Discover II seems unlikely to be fielded to solve this problem. The theater level air breathers are seldom available in sufficient numbers to provide continuous coverage of the theater, let alone focus on current tactical operations.

Each major sensor system tends to consider itself the "solution" to the RSTA problem. This singular viewpoint builds closed systems, which limit the flexibility of the Force in the sense they are not really plug and play.

The solution to the tactical dilemma builds on the principle of shared real time information. By building the SA picture and determining targets from a dedicated group of collectors operating under the control of the tactical commander, he can avoid surprises. An essential ingredient is a mix of sensors, some on the combat platforms and others on UAVs, under the operational control of the tactical commander. These sensors need to include the ability to find the threat in foliage (FOPEN), to locate radios and Radars with SIGINT, retro optics to locate the "forward observer" and SAR / MTI for targeting beyond line of sight.

Each of these sensor systems must be enabled with an automatic targeting process, which converts the sensor data into digital information - suspected target, this location, this time. These reports are then routed automatically by the information management process to the platforms in the area where they are correlated and fused into the SA display. This process must take all available information from dedicated sensors or onboard sighting systems, and automatically share it with other members of the force. The connectivity of the tactical force to the GIG will permit the higher echelons to benefit from this realtime collection capability.



Unmanned Aerial Vehicles

Support Continuous Sensor Coverage and Radio Relay over the AO



Nature of the Problem

- Organic and dedicated UAVs are critical to the implementation of the Tactical InfoSphere
- COTS will provide the high altitude platforms and components for the medium altitude
- The family of UAVs will not be available for the Objective Force without strong proponentcy



Solutions

- Organic UAVs operating at low, medium, and high altitudes under the direct control of tactical commanders
- Focus Army S&T on cost reduction, self-protection, autonomous operation, and MEMS sensors and actuators



Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

Page 17

The dynamics and high mobility of the FCS battlefield leads to the requirement for rapid, responsive, organic sensing and communications capabilities. Such capabilities can only be provided by airborne platforms under the direct control of the commander. A multi-tier family of unmanned airborne vehicles (UAVs) is a critical enabling technology for the objective force. This suite of UAVs is expected to be organic to the commander at the Brigade level (Bde) and below.

UAVs can be categorized into three operating zones: high flyers with the capability to fly autonomously at 55,000 ft or beyond; medium altitude flyers, typically considered tactical UAVs operating in the 5,000 -15,000 ft altitudes; and low flyers in the 0 to 5,000 ft regimes.

Examples of high flyers are the USAF Global Hawk and the HELIOS electric powered platform. HELIOS is under development by AeroVironment Inc., with sponsorship from NASA. The high flyers will have the capability to support multiple functions within the context of C4ISR, including over the horizon communication, area and staring sensing, and satellite links. Highflying UAVs are likely to be joint assets, linking information to multiple units in the tactical battlefield.

The mid-tier of UAVs operate up to 15,000 ft of which Predator is the best known example. Another UAV under development by DARPA is the long endurance Hummingbird A-160. The Hummingbird program has a range of 4,800 km as a goal, with on station endurance in excess of 40 hrs. A medium altitude platform can provide over the horizon sensing, but will also be able to focus its field of regard much precisely on valuable targets than a high flyer UAV. On the other hand, the high flyer UAV will be able to search a much larger field-of-regard region.

Both the high and mid altitude UAVs can have sufficient mission duration to permit the platforms to be staged from bases outside the area of conflict. This mode of operation would allow

long duration, dedicated support to a tactical commander with no burden to the deployed unit. One might even consider contract support for this "sky hook."

The lowest tier of UAVs is the Micro Air Vehicles (MAVs). These platforms typically operate at very low altitudes. They would be carried and launched by a company and scout platoon. The troops can afford to lose several of them in battle due to their expendable design. Most of this development effort is under the auspices of DARPA. They will be able to be used in both defense and offense tactics. In a defense mode, the Micro UAVs will focus reconnaissance and surveillance over a much smaller region than either the medium or high flyers, but at a much lower latency in providing information to the tactical fighter. In an offensive mode, the MAVs can carry small munitions, and also serve as jamming sources to the enemy electronics.

There are many other factors that the Army needs to address to make multi-tier UAVs operational. The need for miniaturized ISR and communications relay payloads are paramount. The survivability of these UAVs is also a critical issue to maintain reliable C4ISR for real-time continuous operation for the tactical echelons.

The main impediment to the adoption of UAVs in the Army has been the lack of a focused community advocating these platforms. Currently, advocacy for tactical UAVs comes from the intelligence community. As the Army transitions to the objective force, the multifunctional capability of UAVs must be recognized and supported if an effective capability is to be fielded. Presently the Army does not have stated requirements, nor does it have an organization to develop and field an integrated package of communication relay and RSTA on UAVs.

The Army should establish a program office to oversee the development, integration, experimentation, and fielding of a suite of UAVs to support the TI. Likewise, the TRADOC must provide consolidated Mission Need Statements for these multi-purpose platforms.

Position/Navigation/Time

GPS Precision Pos/Nav/Time is THE enabler for precision targeting, coordinated maneuver and secure communications

Nature of the problem

- **GPS is deficient in:**
 - Robustness - vulnerability to enemy jamming, exploitation
 - Performance - limited coverage in complex terrain / heavy foliage
 - System integrity - upgraded constellation IOC 2015, FOC in 2017
- **The Army owns 86% of DoD GPS receivers**
- **DoD no longer has control of GPS program**

Solution

- **Consolidate Army Pos/Nav Activities to Focus on the Objective Force**
- **Expand Army Battlespace Tactical Navigation program**
 - Augment current GPS constellation with **Psuedolites**
 - Develop GPS receiver and antennas to enhance anti-jam performance
 - Develop MEMs inertial systems to augment GPS
 - Transition DARPA GPS Psuedolite technology to Army
- **Establish an Operational Capability - A Joint Problem!**

Precision positioning/navigation/time (Pos/Nav/Time) is critical to all dimensions of ground combat. It supports:

- Coordinated maneuver - the ability to navigate over featureless terrain,
- Precision targeting - the use of guided weapons, in all weather conditions, day or night,
- Precision attack - GPS guidance to maximize effect and minimize collateral damage,
- Enhanced secure communications - synchronizing encrypted communications; supporting higher speed services needed for network operations on the battlefield.

This Pos/Nav/Time capability is provided by a system-of-systems. The core capability is provided by GPS, which provides global Pos/Nav/Time service that is seamless, consistent, and uniform, with precise global timing. To highlight the importance of GPS precision Pos/Nav/Time, note that the Army owns 86% of the DoD user equipment.

However, there are a number of areas in which GPS does not fully satisfy the Army's requirements.

- GPS has significant limitations in robustness. It is extremely vulnerable to jamming. Further, an adversary is able to employ the system to satisfy his own needs for precision Pos/Nav/Time.
- GPS is unreliable in complex terrain in which the Army operates, including urban canyons, forests or jungles.
- The satellite constellation is currently in a fragile state with 60% of the on-orbit satellites having single-string failure mechanisms. Although a number of replenishment satellites are available, future high powered replacements with improved jamming resistance will not begin deployment until 2009, with FOC achieved in 2017.
- Finally, DoD no longer has sole control of GPS. There has long been tension between the military and civilian users of GPS in the area of exclusivity vice availability. On 2 May 2000, this

was resolved in favor of the civil aviation community's demands for an accurate, global capability. The Selective Availability feature, which degrades the accuracy of the GPS signal to both threat forces and the civilian community, was turned off.

There are several actions that the Army should take to ameliorate these deficiencies.

- Multiple offices within the Army are involved in the R&D, acquisition and operation of GPS. Combining these activities can maximize the benefit derived from limited resources.
- To increase the resistance to jamming and to enhance coverage to our forces, GPS should be augmented with Psuedolites. These Psuedolites would transmit higher power signals that are less susceptible to jamming, and could add Selective Availability to the theater of combat to degrade an adversary's use of GPS.
- To enhance resistance to enemy jamming, several technologies are available to upgrade GPS user receivers and antennas. These technologies, which are laid out in the Information Dominance Report, should be applied to Army combat platforms.
- To mitigate selected coverage and performance issues, complementary navigation systems should be developed and deployed (e.g., inertial systems employing micro-electromechanical systems (MEMS); time of arrival (TOA) processing in the Joint Tactical Radio System (JTRS)). These options are discussed in Appendix H.

GPS is a Joint Problem! It has become the ubiquitous means of navigating on the modern battlefield and as such it is critical to all US forces and to our allies. This issue must be raised in the Joint arena and a common solution developed to ensure reliable support to future US warfighting missions.



Protect and Counter

Protect Blue C4ISR assets and information Degrade and counter Red C4ISR



Nature of Problem

- Parity of C4ISR COTS/GOTS available from global arms trade
- Ability to understand and deal with new technologies, e.g. proliferated cell phones, smart landmines, wireless sensors
- Ability to impose and verify C4ISR Asymmetry in Blue favor
- Increased Signatures resulting from Blue C4ISR operations
- Red "Home Court" advantage

Solutions

- **A Red Team** - Establish an independent Organization to challenge the Tactical InfoSphere, using modeling, simulation, exercise and training
- Focus intelligence to document GOTS/COTS technologies available to Red Forces to support development of responsive countermeasures
- **Assess COTS/GOTS and develop techniques to:**
 - Harden Blue C4ISR components
 - Attack Red C4ISR components / systems

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 19

Information Dominance has two elements. The first, is Blue's ability to acquire, process and move information on the Battlefield. This must be accomplished in spite of Red's attempts (Red offensive Information Operations (IO)) to confuse, degrade and delay the information timeliness and quality. The second is Blue's ability to prevent Red (Blue offensive I.O.) from acquiring, processing and moving critical information on the battlefield.

The current revolution in telecommunications technology has complicated our usual technical advantage over a lesser nation. The availability of "world class" sensors and sensor products (satellite imagery), communication technology as exemplified by the cell phone, super computer class PCs and software tend to level the playing field. Further, potential adversaries have the unique advantage that a smaller, less bureaucratic defense establishment can quickly outfit an elite force with state of the art technology, which we are unable to match. The ability of our forces to deal with an ever-widening spectrum of technology stresses our ability to equip and train our forces. For example new technologies like the cell phone, wireless unattended sensors, automated C2 and smart mines are now posited as elements of a future threat. We must continue to search for, evaluate and learn to counter these advanced technologies.

Success in Protect and Counter is based on our ability to impose an asymmetric C4ISR capability on the battlefield. One of the challenges to maintaining this asymmetry is the need to measure the impact of our counter operations on his force.

As we move to a thin distributed force with increased reliance on wireless communications we inherit the concomitant burden of increased radio emissions and the signature that these radios produce. We must work to both minimize the transmissions to that which must be sent and to reduce the actual signature of the radios, with low probability of intercept waveforms.

Finally in an era of "come as you are wars" the threat force will almost always enjoy a home court advantage. He knows the terrain, the infrastructure, the hide positions, and all the other detail we attempt to generate in doing IPB. This inherent knowledge puts a unique demand on our intelligence units to quickly, accurately and as completely as possible, generate the IPB product.

Red offensive information operations will attempt to attack those vulnerabilities of the US Army's TI which have not been hardened and protected. These vulnerabilities, if not corrected in development, test or with feedback from exercises, will result in the US Army losing timely and critical decision support information on the battlefield. Similarly if the US Army fields the appropriate systems to counter the adversary's information infrastructure the impact on the adversary's ability to make good battlefield decisions can be severely degraded.

To build a Force with extraordinary information dominance capabilities will demand attention to the entire spectrum of the transition process. The elements of the TI must be selected and tested to insure they are as robust as possible. Doctrine and Tactics, Techniques and Procedures (TTP) must be developed and honed to insure our troops are ready and able to deal with the ambiguity of information operations on the battlefield. This approach of challenging the solution must also extend to training exercises - both in the schoolhouse and in the field. By establishing highly competent, independent Red Team, the Army will be able to challenge the development process to field robust hardware and software as well as providing a surrogate world class information warfare OPFOR. The ARL Survivability, Vulnerability Analysis Directorate, (SLAD) has the nucleus of such an organization. Today it does not have the breadth of charter or the resources to achieve the necessary level of effectiveness.

If our forces are to operate globally in the future, the intelligence community must focus their energies on the definition of potential threat C4ISR systems to a level of detail that permits the tuning of our offensive capabilities to overmatch the threat. For example, it may be important to know if their C2 was based on Windows 95, or Windows 98 or perhaps on SAP's e-commerce software. Only with detailed *a priori* knowledge, can our offensive tools be configured to insure overmatch.

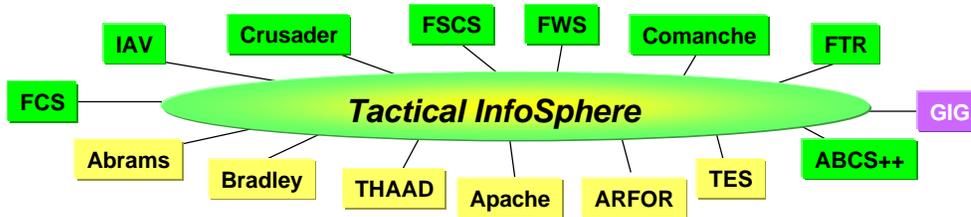
Finally the Red Team must be used to evaluate the vulnerabilities of our COTS C4ISR equipment and evolve the 'fixes' to reduce these vulnerabilities. Further, this evaluation process can also drive the development of techniques to counter the threats use of similar equipment and software. The challenge and respond nature of Information warfare has not changed in principle, but the rate of change is markedly higher than it was prior to the micro processor revolution.



Systems of Systems



Every platform in the Objective Force will be a node in the Tactical InfoSphere - a complex system of systems



Nature of the Problem

Need to Develop an Architecture, Engineer a Solution and Integrate -

- C4ISR for each weapon system / platform (e.g., FCS, Crusader. ...)
- Each C4ISR system (e.g., ABCS ++, TES, GIG, ...)
- The Objective Force - composite of weapon and the Tactical InfoSphere
- Incorporate Open Standards and Interfaces to GIG
- Designed to accommodate the future upgrade of legacy platforms

Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

Page 20

The TI must incorporate every C4ISR system used in the Objective Force. Embedded C4ISR capabilities on-board each weapon platform will act as a node of the TI. The computers, communications, networking and sensors on-board FCS vehicles, Crusader, Future Scout and Cavalry System (FSCS) and other platforms will be included in the TI. Program managers (PMs) for these weapon platforms must cooperate in enabling the TI. C4ISR systems and platforms such as the next generation Army Battle Command System (ABCS), Tactical Exploitation System (TES) and Tactical Unmanned Aerial Vehicle (TUAV), will also be included. PEO C3S, PEO IEW&S, and Army Space Program Office will be major players in the TI cooperative. Digitization lessons learned have highlighted the need to deliberately plan for the C4ISR system-of-systems comprised of all weapon platforms and C4ISR systems. Objective Force access to and interoperability with Joint and coalition forces will be accomplished through the GIG. Seamless integration of the TI and the GIG is crucial. Units provided with the communications, information management, RSTA, UAV, counter C4 and PNT capabilities previously recommended must be able to interoperate with other units provided with legacy systems. Developments for the TI must accommodate a minimum level of interoperability without demanding upgrades to legacy systems.

The current Army RDA organization involves many independent PMs and other organizations in developing the individual systems that will comprise the TI. The potential for ten or more organizations providing major systems for the TI presents a formidable management challenge unmatched in scale or magnitude. A holistic management approach with enabling processes and strategies is needed to cohesively unite all elements of the TI.



The Way Ahead: A Serious Management Challenge



Solutions

- **Operational Architecture and Requirements** - Prescribe warfighter needs, and acquisition priorities
- **Systems Engineering** - Conduct architecture design, systems engineering, prioritize R&D, and oversee systems integration
- **Models, Simulations, and Test Beds** - Provide the environment to explore operational needs and technology development for the Tactical InfoSphere
- **Vulnerability Assessment** - Independent Red Team to challenge the Blue Tactical InfoSphere in development and in the field
- **Acquisition Strategy** - Orchestrate PEO efforts, and develop a master plan focused on leveraging commercial technologies and processes

The unprecedented need for integration of platform and C4ISR systems Demands an Enterprise Wide Organization and Processes!

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 21

Meeting the Army's goal of fielding the Objective Force by 2010/2012 will stress every element of the RDA process.

The TRADOC will need to develop an Operational Architecture (OA) for the TI and document the requirements for the system. The OA must recognize that in a TI enabled force the information flows may bear little or no resemblance to the current BFA structure. A guiding principle must be to keep the processes simple! It will be critical that these documents be flexible enough that the development community is able to capitalize on the "best" available technology over the life of the Operational Requirements Document (ORD). One does not want to be in the position of buying lunch box size cell phones when the current models weigh 10 oz. The technology is so dynamic that the requirements must be free of constraining language and preordained solutions. Since these products drive the development process it is critical that they be available soonest. About right is good enough to get the process started.

Given a draft definition of the OA, the System Engineer must develop a Systems Architecture to identify the elements of the systems, their interrelationship and identify candidate technologies to enable the system. This process will uncover areas in which the commercial technology is not adequate to meet the Army needs and R&D will be needed. These "need" lists can then be used to focus the Army tech base expenditures.

Among the tools available to help the processes described above are modeling, simulation and live test beds. The Army enjoys a world class capability in modeling and simulation, but it is generally deficient in the areas of C4ISR and will need work to adequately model the TI. The application of these models and the networked simulations can support early experimentation with streamlined "business processes." As the system architecture matures and candidate technologies are identified and made available, it will be highly desirable to begin field trials to determine the

efficacy of the candidates and to identify their shortfalls and weaknesses. Critical areas include: the performance of sensors and their ATR processors, the ability of the internet to function on the move, the implementation of information management rules which will determine the availability of information to the user and the level of fusion available to declutter the warfighters displays.

The Red Team will play a critical role in forcing a robust solution to the TI. Their activities will commence in the requirements and early experimentation phase. They will be partners with the PM during the implementation of the system and will support the development of an Information Warfare element of the OPFOR for field trials.

The acquisition strategy, which brings together all the elements of the InfoSphere will touch the products of the PEO's for CSSCS, UAV, IEW, platforms and probably others. The focus of this effort must be on capturing commercial standards and products and insuring the total integration of the many products into a "seamless whole."

The many elements of the RDA process must perform in lock step if they are to meet the ambitious transition goals. The mechanism to achieve this level of coordination is lacking today.



Technology Assessment to Support Objective Force Capabilities



Core Capability	Technology	EMD Risk (Tech Readiness Level ³⁷ at FY2006)		
		Required	Technology	Programmatics
Info Mgmt	Intelligent Data Mgmt	<input checked="" type="checkbox"/>	Green	Yellow
	Common Operating Picture	<input checked="" type="checkbox"/>	Yellow	Yellow
	Human Machine Interface	<input checked="" type="checkbox"/>	Yellow	Red
Comm	Secure Mobile Networks	<input checked="" type="checkbox"/>	Green	Yellow
	Radios (DSP, waveforms, networks, etc.)	<input checked="" type="checkbox"/>	Yellow	Red
RSTA	EO, IR, Radar, RF, LIDAR Sensors	<input checked="" type="checkbox"/>	Green	Yellow
	Micro-acoustic, seismic, etc. Sensors	<input checked="" type="checkbox"/>	Green	Yellow
	Sensor Fusion – deconflict, Template	<input checked="" type="checkbox"/>	Green	Red
	Multi Sensor Fusion	<input checked="" type="checkbox"/>	Red	Red
	ATR-Detection and Recognition	<input checked="" type="checkbox"/>	Yellow	Red
UAV	Long Endurance	<input checked="" type="checkbox"/>	Green	Red
	Medium Endurance		Green	Yellow
	Mini/Micro		Yellow	Red
Pos/Nav	Receivers	<input checked="" type="checkbox"/>	Green	Red
	Antennas	<input checked="" type="checkbox"/>	Green	Red
	Pseudolites	<input checked="" type="checkbox"/>	Green	Red
Counter & Protect	Counterspace		Yellow	Red
	Information Assurance	<input checked="" type="checkbox"/>	Yellow	Yellow
	Sensor CM (RSTA)	<input checked="" type="checkbox"/>	Green	Yellow
	Offensive I.O.	<input checked="" type="checkbox"/>	Yellow	Red
RDA	Modeling, Simulation and Test Beds	<input checked="" type="checkbox"/>	Yellow	Red

Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

Page 22

The technology to build a TI can be available to enter EMD in 2006, if and only if, significant resources are applied to maturing the areas shown in yellow and red in the technology column. However, many of the critical technologies are not in the current program as indicated by the red in the programmatics column.

The panel was asked to provide an estimate of the maturity of the technology required to implement the TI. The details of this evaluation are included at Appendix K.

This matrix examines the maturity and the resources available to bring these technologies to the level where they could enter EMD in 2006. The chart is organized by the seven system elements addressed in this report. Each of the seven areas is further divided into critical technologies.

The chart should be interpreted as follows:

- The required column presents our judgement as to the necessity of fielding the particular technology with the initial elements of the Objective Force.
- The technology column gives our estimate of the current state of maturity of the technology and addresses the question, "Can this technology be ready to enter EMD in 2006 if sufficient R&D resources are made available?"
- The programmatics column indicates to the best of our knowledge, the adequacy of the current and / or planned program addressing this technology.

The message of this display is clear -

Significant resources will be required to mature these critical capabilities to a level of maturity suitable to enter EMD in 2006 to enable fielding by 2010 to 2012.



Overall Observations

- **Creating a Tactical Infosphere will provide our forces with superior situational awareness and robust communications**
- **But, we must also be able to degrade the Threat's C4ISR to achieve Information Dominance**
- **Training the Force and Developing the leaders to operate within the Tactical Infosphere will be a challenge**
- **Systems Engineering and Program Management will be daunting tasks**
- **Difficult Technology achievements remain - to include UAVs, software, remote mine detection, etc.**
- **The Tactical Infosphere, can and should serve The Army**

Current Organizations and Processes will not achieve the key Capabilities necessary for the Tactical InfoSphere

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 23

The TI can enable a new battlefield dynamic, but its development will be a major challenge!

The advantage gained by the Army from Information Dominance through the TI will be measured in terms of increased lethality and survivability. Superior knowledge of the battlespace derived from timely situational awareness information and the ability to instantaneously deliver that information as needed, throughout the force will be key. Links to joint and national sources of information over the Global Information Grid will ensure Army and Joint Force Commanders can interoperate effectively. Key to this concept is the ability to provide real time, detailed "combat information*" to the warfighter, while at the same time keeping higher echelons advised of the situation, and benefiting from their non-real time intelligence resources.

While the TI delivers unparalleled levels of critical and timely information to Blue Forces, achieving information dominance requires degrading opposing force C4ISR capabilities, either before or during operations. Since Red Forces likely will enjoy a "home court advantage", the challenge to Blue Forces will be to attack and degrade Red's C4ISR capabilities. Increasingly, COTS technologies - radios, computers, Software, commercial satellite imagery, UAV's and ground sensors will be available to compromise Blue's operational security. In addition to investing in enhancements to Blue situational awareness, the Army will need to consider and develop a range of Force Protection capabilities, ranging from IW to Space Control, to degrade Red's C4ISR.

Training leaders to command Army forces in the information environment of the TI will be a complex and multi-disciplinary endeavor. As forces become more skilled in working with these information technologies, commanders will be able to hone their organic and supporting sensor collection capabilities to provide them with unprecedented levels of information, allowing them to decisively dominate opposing force actions.

Due to the complexity of the TI discussed earlier, the means by which the Army engineers and manages the development will present major challenges in both combat and materiel development. The recommendations that follow outline a proactive approach to mitigate many of these challenges. While the management and systems engineering challenges with acquiring the TI are daunting, there are a series of technical challenges, as addressed on Chart 22, that remain. These range from UAV development, to Automatic Target Recognition, to Information Management software, etc.

The TI, providing combat information to the warfighter and connecting Army forces into the Global Information Grid, can provide Information Dominance on future battlefields.

* The term Combat Information was coined by General William DePuy, the first Commander of the TRADOC. As DePuy expressed it, he wanted to know "what was happening over the next hill, right now!"



The Major Recommendation



Develop a Tactical Infosphere for the Objective Force to provide robust SA, C2, and rapid targeting on the move. The enablers are:

- **Organic sensors with automatic data processing, reporting, and fusion**
- **Communications exploiting commercial capability based on Internet Protocol (IP), compatible with the GIG, and new Radios**
- **The tools to manage combat information**
- **Family of dedicated UAVs to support communications relay, RSTA, range extension and reducing sensor-shooter latency**
- **Positioning, Navigation, and Time by upgrading GPS capabilities and adding inertial and network-assisted positioning**
- **Capability to degrade Red's communication, RSTA and GPS**

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 24

There are three critical elements to the Objective Brigade as it is envisioned today, the Future Combat System, the Future Tactical Rotorcraft and the TI. Without the InfoSphere, the goals of high survivability and control of an extended battle space will not happen.

Six months of study and analysis by this study group highlighted the need for the Army to develop a TI to support the Objective Force. The TI will afford robust SA that will enable precision maneuver, it will support Command and Control over a dispersed force and it can provide targeting beyond line of sight - all critical functions.

As pointed out earlier, the mechanism to provide a realtime assessment of the battlefield consists of a chain of elements - all of which are necessary if the system is to meet the Army's expectations.

- A mix of organic sensors under the direct control of the Brigade and Battalion commanders which have the capability to sense, process and report on enemy activities start the process.
- Internet Protocol based communications, employing modern wideband radios and supported by airborne radio relay provide the backbone for information distribution.
- A family of tools to manage the routing of data and the sorting of these products at each combat platform, to ensure that the information is distributed as needed.
- A family of dedicated UAVs must support the airborne sensors and the radio relay functions. By employing long duration platforms they can be staged from outside the zone of combat with no overhead to the supported commander. There is the potential that the Army or the DOD might "hire" these platforms on a contract basis with a civilian contractor providing all support.
- Redundant Pos / Nav / Time capabilities are essential to generating a common picture of the Battlespace. GPS is the keystone of this capability, but it needs to be augmented with Psuedolites to both improve our capability and to disrupt the enemy capabilities. A back up capability, in the form of dead reckoning and / or Time of Arrival algorithm in organic radios is needed for combat in forests and in built up areas.

- The capability to execute offensive Information Operations must include systems that are capable of attacking the threat info systems. A corollary to the attack function is the ability to measure the effectiveness of our capabilities, that allows our forces to fine-tune their operations.

The TI must be included in the planning for the Objective force. It represents the third leg of the milk stool!



Recommendation

Acquire the Tactical InfoSphere

- **Form an IPT to coordinate all efforts under the VCSA**
- **TRADOC/DA provide the Operational Architecture**
- **Systems Engineer (AAE)**
 - Promulgate standards,
 - Define and enforce the Systems Architecture
 - Focus Tech Base R&D investment
- **AAE acquire Tactical InfoSphere, leveraging commercial technology**
- **Assess in simulations and field trials**

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 25

Acquisition of the TI will demand a team effort.

Acquiring and fielding the TI will involve coordinated efforts spanning the entire Army. To capture the importance, magnitude and breadth of this undertaking, the Army Science Board recommends that the Vice Chief of Staff, Army form an IPT to guide the Army's overall efforts in developing the TI.

TRADOC must develop new concepts and requirements that capture the internetted nature of the TI, and create DTLOMS solutions consistent with the TI concept. Materiel requirements must then be vetted by HQDA to enable Army forces to operate decisively in ways to achieve information dominance. TRADOC must create an Operational Architecture for the Objective Force to guide systems upgrades and developments.

The AAE, through a TI Systems Engineer, must also ensure that technical and systems architecture adopt commercial approaches and standards consistent with the evolution of the commercial information technology field. This will enable the Army Science and Technology community to focus their technology base efforts towards meeting the TI's technology needs. Prototype capabilities should be developed for experimentation and red teaming, and assessed via simulations and models to achieve robust and critical C4ISR capabilities for the Army.



Recommendation



Develop DTLOMS to support the Tactical InfoSphere

- **Establish a simulated Tactical Force to represent the “Objective Force”**
 - Learn to use UAV with mobile tactical forces
 - Learn to reduce latency in sensor-to-shooter process
 - Develop leaders for the InfoSphere environment
- **Evaluate Candidate Technology and TTP**
- **Incorporate lessons learned in field trials**

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 26

An Objective Force equipped with FCS and FTR vehicles and enabled by the TI will possess the revolutionary capability to quickly deploy anywhere in the world and conduct successful combat operations on arrival.

The result of this revolution in warfighting materiel will be a concomitant change in the spectrum of the DTLOMS of that force. Each and every element will be impacted as the forces learn to capitalize on their new capabilities. Key to the transition to this "new force" is a continuous experimental program to evaluate future concepts, develop TTPs, and to outline training processes for future soldiers and their leaders.

Building on the success of the 11th Air Assault Division we would propose a force be established to experiment with the concepts associated with the TI. For example, the Army has very limited experience with the operation of UAVs for RSTA and almost none associated with UAVs as radio relay platforms. Concepts need to be evaluated and TTP developed to baseline these capabilities.

Business processes need to be developed and refined. The concept of "sensor to shooter" is often heard, but the procedures by which a shooter will be "allowed" to fire without intervention by a human operator is not answered. Alternative concepts need to be explored, based on proposed rules of engagement and the required technology to enable a given solution must be evaluated. With the Objective Force goal of controlling terrain to 20 to 40Km, the reduction of sensor to shooter latency to seconds - or zero - deserves critical review.

Given the concepts, the TTPs and the technology, Objective Force leaders must be developed to "think outside the box." Planning functions will change radically, real time management of the battle will likely be more autonomous than the current practice - in essence every function must be revised to reflect the increased pace of the battle. Many of these processes can be evaluated rapidly in a virtual simulation environment at modest cost. Once the procedures and the supporting technology reach a modest level of maturity, field trials can refine the process and demonstrate whether the technology is reliable in the real world.

From the TRADOC perspective, the bottom line must be to capture the lessons learned from this experimental process and to embed the lessons in future doctrine and training. The US Army is without question the best trained force in the world. The revolution attendant to the fielding of the Objective Force will demand a revolution across the DTLOMS.



Recommendation



Create an independent, technical **Red Team to challenge the Tactical InfoSphere through Development and in the Field.**

- **Support assessment of commercial components and their integration into the system**
- **Challenge system design throughout the development process**
- **Provide Engineering Support the NTC OPFOR to attack**

Blue C4ISR - Extend capability across FORSCOM

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 27

Without an independent, dedicated Red Team to challenge the development of the TI, it is unlikely that the C4ISR capabilities demanded of the Objective Force will materialize.

Based on the complexity of the TI and the challenge of integration of the many technologies that will make up the system, we believe a Red Team is essential to a successful fielding. This team must fulfill multiple missions such as:

- Playing a critical role in the evaluation and selection of candidate COTS / GOTS hardware and software elements which form the basis of the TI. As these components are integrated into larger system elements in the laboratory the Team must evaluate the effectiveness and vulnerabilities of the resulting system. When weaknesses are found the team would recommend fixes to the PM / PEO. The process is likely to become a fix, test, fix cycle, which will insure a robust product. This process will require extraordinary cooperation between the developers and the Team.
- Participating in the inevitable design trades which are a part of the development of a major system. It will be important to keep the focus on producing a robust Information Warfare capability, not just a reliable automation system. The TI must be designed to operate in a very hostile IW environment with the Team providing the checks and balances to keep the program on track.
- Providing an aggressive OPFOR with IW capabilities representative of a likely threat. We would envision a cell of the Team supporting the OPFOR at NTC to enable realistic IW in each NTC rotation. This same capability should be provided to the FORSCOM so that the troops at Ft Hood can routinely train in an IW environment.

Fortunately, the Army has the nucleus of the Red Team today in the Survivability, Lethality, and Analysis Directorate (SLAD) of ARL. The elements that make up SLAD have a long history of playing the Red Team role. However, as resourced today they do not have the manpower, or the budget that begets independence, or the charter to assume this critical role. This shortcoming should be fixed!



Near Term Actions

- **DA publish a Vision Statement to Build the Case for the Tactical InfoSphere in the Objective Force**
- **Initiate the System Engineering Team to establish a preliminary System Architecture to drive R&D priorities - Start NOW!**
- **Establish a program to:**
 - Demonstrate and Evaluate Operational Concepts
 - Determine Technological Shortfalls and System needs
- **Establish a Test Unit - a Bn slice of the “Objective Force”**
 - A Company team, Bn command element, peer company elements
- **Establish a simulation test bed - IOC in 6 months**
- **Build on current digitization capability - IOC in 12 months**

Early demonstration of potential combat capabilities

*Technical and Tactical Opportunities for Revolutionary Advances
in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era*

Page 28

The Army should initiate near term actions to demonstrate the potential combat capabilities afforded by the TI. These actions will augment long-term efforts underway by the Army and DARPA.

A Vision Statement for the TI should be published. The vision would provide goals to be achieved by all involved in developing materiel solutions for the TI specifically, and for the Objective Force, in general. The vision would support synergy in planning and execution of S&T and EMD projects by the many organizations involved. The statement should take on the form of a document like the Joint Vision 2020. Preparation should start immediately under the direction of HQDA.

A Systems Engineering Team needs to be established now. This team should initially be directed to design and document preliminary systems architecture for the TI. The C4ISR S&T program should be evaluated against this systems architecture to drive R&D priorities - focus the scarce R&D dollars on those technologies that do not exist and which will not derive from the commercial sector. This team should report to the AAE and be funded to develop and enforce the systems architecture

To hasten the development of the TI, early demonstration of operational concepts and determination of technology pitfalls necessary for system operation is recommended. To that end, a program should be established under the leadership of a combat arms officer (who is tolerant of technology) with strong support from the Systems Engineer. The program should involve virtual and live simulation exercises with real soldiers who would; assess results, document lessons learned and focus S&T efforts. These soldiers could be organized as a slice of an objective force battalion, including a company team, the battalion command element, and peer company elements.

Within Six months, an initial operational capability for a virtual simulation test bed could be developed through the leadership of the Systems Engineering Team. The battalion slice would conduct simulation exercises using this test bed in a manner similar to that being used in the Battle Command Reengineering Simulation Exercises conducted at the Fort Knox Mounted Maneuver Battle Lab.

Within twelve months, an initial operational capability for a live digitization test bed could be developed through the leadership of the Systems Engineering Team. The battalion slice would conduct a small scale live exercise using this test bed in a manner similar to that for the Focused Dispatch Advanced Warfighting Experiment.

APPENDIX A

TERMS OF REFERENCE



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON DC 20310-0103

February 28, 2000

Mr. Michael J. Bayer
Chair, Army Science Board
2511 Jefferson Davis Highway, Suite 11500
Arlington, Virginia 22202

Dear Mr. Bayer:

I request that you conduct an Army Science Board (ASB) Summer Study on "Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era." The ASB members appointed should consider these Terms of Reference (TOR) as guidelines and may include in their discussions related issues deemed important or suggested by the sponsors. Modifications to the TOR must be coordinated with the ASB office.

I envisage that this work by the Army Science Board will also yield practical near term insights and opportunities that will assist the Army Leadership in focusing priorities for our limited research, development and acquisition accounts to create the most combat effective and cost efficient rapidly deployable joint ground forces for the 2015-2025 period.

The study should be composed of four parallel investigations leading to an integrated set of recommendations. This work is to be guided by, but not limited to, the following lines of inquiry:

Team 1 - Operations. To the goal of achieving rapidly deployable forces with dominant maneuver supported by precision fires, look at those opportunities which offer the greatest pay off for quickly deploying forces which feature a highly flexible array of full spectrum force capabilities. Focus on combat operations, accounting for capabilities required to achieve systems overmatch as a critical component of overall force effectiveness both for initial entry into a theater of operations and to enable operational maneuver within the theater once operations begin. The array of systems and force capabilities should assure future commanders retain battlefield freedom of maneuver and are not denied tactical options for offensive or defensive schemes of maneuver. While combat operations are the focus, the relevance of the capabilities to stability and support operations, such as peace operations, should be assessed. Consider, but do not limit your investigation to the following opportunities:

- a. Look at the feasibility of synchronizing the requirements for the Future Combat System, the Joint Transport Rotorcraft (JTR), and Comanche to provide revolutionary tactical and theater mobility and increased strategic mobility. If feasible, what are the assumed tactical benefits of this union?
- b. Assess the capabilities gained by exploiting robotic air and ground systems as reconnaissance/surveillance, attack systems, and other functions. Which force capabilities or platforms appear to benefit most from this relationship?
- c. Propose a suite of smart munitions/sensor combinations in our direct fire and indirect fire forces that offer the most cost effective investment and the most decisive outcome in expected scenarios.
- d. Determine those areas of the force that demand robust 24 hours a day, 7 days a week manning, and portray the benefits of various manning arrangements.
- e. Identify the optimal organizational structures that best exploit future information technology.
- f. Determine the need for or utility of an Advanced Theater Transport (ATT) to replace the C-130 to support the operational capability and systems described above.

Team 2 – Sustainment and Support. To the goal of providing this force a support/sustainment capability with significantly reduced logistic burden, look at the opportunities in providing forces with significantly greater systems reliability (including mechanical, electronic, photonic reliability, etc.) along with graceful degradation and ultrareliability leading to simplified battlefield maintenance, repair and diagnostics/prognostics (including disposable/expendable components/systems), significantly smaller fuel and ammunition tonnage requirements, improved battlefield medical support, transport means (manned and unmanned), and remote services. Consider, but do not limit your investigation to the following opportunities:

- a. Assess the opportunities to leave outside the theater significant logistic, intelligence, and administrative support, thereby reducing the force requiring in-theater support.
- b. Assess the opportunities for advanced power plants that reduce the specific fuel consumption at least 25% per HP delivered.
- c. Assess the logistic implications of the alternative families of smart munitions (as generated by Team 1).

- d. Exploit the opportunity for remote surgery (telemedicine) to reduce the number of in-country specialty surgeons.
- e. Assess the capability of the JTR to contribute to rapid medical treatment and evacuation along with other joint force options.
- f. Assess the opportunities to improve the Army's capability to conduct Near Shore/Logistics-Over-the-Shore operations.

Team 3 - Information Dominance. To the goal of providing this force Information Dominance through the provisioning of an advanced "central nervous system" to meet the needs of our forces and to deny the threat force basic information needs consider at least two perspectives. First is the broad, relatively global C4ISR focus that flows vertically from the Joint Task Force down through corps and divisions (as units of employment) all the way to units of action executing their tactical operations and tasks. The second perspective includes the time sensitive information at the local level that is dependent on rapidly changing battle command and control, "around the next hill/corner" situational awareness, and the needs at the tactical maneuver/support units and teams level - platforms and organic sensors centric. This assessment should consider both of these complementary perspectives. The objective of providing maneuver units a fundamental capability to expand their engagement envelopes to include short timeline, beyond line of sight and fleeting targets may provide a catalyst for this information dominance challenge. Look at capabilities which provide digital map location and terrain elevation data to support the needs of ground maneuver commanders and precision fires employment, yield superior situational awareness of friendly and threat forces, instantaneous critical logistic asset status and location, theater missile threat detection, location and ongoing tracking of any threat weapons of mass destruction, and deny the threat forces this basic capability using both lethal and non-lethal means. Provide forces with timely, reliable information updates (unit and platform level updates) to facilitate tactical and support mission planning and rehearsal during deployment and on the move. As technology opportunities are assessed, it is essential that future forces operating in urban and complex terrain environments have robust, high confidence situation awareness, across the full spectrum of military operations. Consider, but do not limit your investigation to the following opportunities.

- a. Assess the suite of National and Theater sensors: overhead, air breathing, manned and robotic necessary to provide the desired data and information.
- b. Assess the technological opportunity to provide necessary bandwidth for data, voice, and video requirements for the force.

c. Ascertain the requirements to deny the threat the necessary voice and data information he requires to effectively employ his forces.

d. Assess the ability to link all systems through an inter-netted system of non-line-of-sight communications.

Team 4 - Training. To the goal of ensuring that these deployed forces have an organic capability to train to peak effectiveness within the theater of operations, look at opportunities for providing embedded training devices for crew, team and small unit training; the ability to deliver training into the theater using "distance learning" opportunities; the ability to provide "mission rehearsal" capabilities as required; and the ability to permit staff and command training with sensitive intelligence products. These investigations should be grounded in a vision of a future training strategy for both collective and individual training which leverages a proper mix of live, virtual and constructive training and which is supported by an information based system of systems architecture. Consider, but do not limit your investigation to the following:

a. Assess the command and control systems' ability to provide necessary alternative mission analyses and threat scenario generation using all source intelligence.

b. Assess the opportunities for embedding necessary training system requirements in the Future Army Land and Aviation Vehicles, to include mission rehearsal capabilities. This assessment should include embedded joint training and real time cooperative training with units and systems both in and out of theater from alert through deployment and employment.

c. Assess the training requirements necessary to train the sensor to shooter precision fires employment.

d. Look at the need for and feasibility of using distance learning techniques to train portions of the force with out-of-Theater resources.

e. Investigate approaches which can link training and operational system capabilities to facilitate the creation of realistic conditions and which can store, fuse, filter and disseminate relevant information to a variety of training system components.

Study Support. Sponsors of this study are GEN John M. Keane, Vice Chief of Staff; GEN John N. Abrams, Commanding General, US Army Training and Doctrine Command; GEN John G. Coburn, Commanding General, Army Materiel Command, and LTG John J. Costello, Commanding General, Space and Missile Defense

Command. LTG Paul J. Kern is the ASA(ALT) cognizant deputy and LTG Randall L. Rigby, Jr., is the TRADOC cognizant deputy.

Schedule. The study panel will initiate the study immediately and conclude its effort at the report writing session to be conducted July 17-27, 2000, at the Beckman Center on the campus of the University of California, Irvine. As a first step, the study co-chairs will submit a study plan to the sponsors and the Executive Secretary outlining the study approach and schedule. A final report will be issued to the sponsors in September 2000.

Sincerely,

A handwritten signature in black ink that reads "Paul J. Hooper". The signature is written in a cursive, flowing style.

Paul J. Hooper
Assistant Secretary of the Army
(Acquisition, Logistics and Technology)

APPENDIX B

PARTICIPANTS LIST

PARTICIPANTS LIST

**ARMY SCIENCE BOARD
2000 SUMMER STUDY**

**TECHNICAL AND TACTICAL OPPORTUNITIES
FOR REVOLUTIONARY ADVANCES
IN RAPIDLY DEPLOYABLE JOINT GROUND FORCES IN THE 2015-2025 ERA**

Study Co-Chairs

Dr. Joseph V. Braddock
The Potomac Foundation

LTG Paul Funk (USA, Ret.)
General Dynamics Land Systems

Dr. Marygail Brauner
RAND

ASB Panel Chairs

The Operations Panel

The Information Dominance Panel

Dr. Robert E. Douglas
Lockheed Martin Electronics and Missiles

Dr. Philip C. Dickinson
Private Consultant

LTG Daniel R. Schroeder (USA, Ret.)
Private Consultant

LTG John W. Woodmansee (USA, Ret.)
Private Consultant

LtGen Paul K. Van Riper (USMC, Ret.)
Center for Naval Analyses

Gen James P. McCarthy (USAF, Ret.)
United States Air Force Academy

The Sustainment and Support Panel

The Training Panel

Mr. Ed Brady
Strategic Perspectives, Inc.

Dr. Harold F. O'Neil, Jr.
University of Southern California

GEN Leon E. Salomon (USA, Ret.)
Private Consultant

MG Charles F. Drenz (USA, Ret.)
C.F. Drenz & Associates, Inc.

VADM William J. Hancock (USN, Ret.)
Hancock Associates

RADM Fred L. Lewis (USN, Ret.)
National Training Systems Association

ASB Panel Members

The Operations Panel

Dr. Frank H. Akers
Lockheed Martin Energy Systems

Dr. Sheldon Baron
Baron Consulting

Dr. John Blair
JBX Technologies

Dr. Gregory H. Canavan
Los Alamos National Laboratory

Dr. Inder Chopra
University of Maryland

Dr. Herb Dobbs
TORVEC

Dr. Gilbert V. Herrera
Sandia National Laboratories

Dr. Anthony K. Hyder
University of Notre Dame

Mr. Ira F. Kuhn, Jr.
Directed Technologies, Inc.

Dr. Joanna T. Lau
Lau Technologies

LTG Charles Otstott (USA, Ret.)
Global InfoTek, Inc.

Mr. Srinivasan 'Raj' Rajagopal
United Defense

Dr. W. James Sarjeant
SUNY at Buffalo

Mr. George T. Singley
Hicks And Associates, Inc.

Dr. Tony Tether
The Sequoia Group

The Information Dominance Panel

Mr. John Cittadino
JCC Technology Associates

Dr. Derek Cheung
Rockwell Science Center

Ms. Christine Davis
Executive Consultant

Dr. James R. Fisher
DESE Research, Inc.

Mr. Jerome S. Gabig
The Time Domain Corporation

Ms. Dixie Garr
CISCO

Mr. Gary Glaser
LDCL, LLC

Dr. Lynn Gref
Jet Propulsion Laboratory

Dr. John Holzrichter
Lawrence Livermore National Laboratory

Ms. Suzanne Jenniches
Northrup Grumman Corporation

Dr. Don Kelly
Advantech Consulting

Mr. Kalle Kontson
IIT Research Institute

Mr. David Martinez
Massachusetts Institute of Technology

Dr. Rey Morales
Los Alamos National Laboratory

Dr. Prasanna Mulgaonkar
SRI International

Dr. Sam Musa
Northwestern University

Dr. James A. Myer
Photon Research Associates, Inc.

Dr. William Neal
The MITRE Corporation

Mr. John Reese
Private Consultant

Dr. Stuart Starr
The MITRE Corporation

Mr. Alan Schwartz
Policy Futures LLC

Dr. Nick Tredennick
Tredennick, Inc.

Dr. Robert Ziernicki
Mirage Systems, Inc.

The Sustainment and Support Panel

Mr. Buddy G. Beck
Thermo Washington

Mr. Anthony J. Braddock
The Loch Harbor Group, Inc.

Dr. David S. C. Chu
RAND Arroyo Center

Mr. William S. Crowder
Logistics Management Institute

Mr. John H. Gully
SAIC

Dr. Larry Gladney
University of Pennsylvania

Dr. Michael Krause
Freightdesk.com

Mr. Ray Leadabrand
Leadabrand and Associates

Mr. Paul Lumpkin
Plexus Scientific

Dr. Gary R. Nelson
SRA International

Mr. Donald R. ('Rob') Quartel
D.R. Quartel, Inc.

Dr. Joseph E. Rowe
Private Consultant

Dr. James S. Whang
AEPCO, Inc.

Dr. Annetta P. Watson
Lockheed Martin Energy Resources / ORNL

The Training Panel

MG Charles F. Drenz
C.F. Drenz and Associates

LTG John Miller (USA, Ret.)
Oracle

Dr. Charles Engle
ECC International

Dr. L. Warren Morrison
Carnegie Mellon University

Mr. Frank Figueroa
Lockheed Martin/Sandia National
Laboratories

Dr. Irene Peden
University of Washington

Dr. Peter Lee
Carnegie Mellon University

BG James Ralph (USA, Ret.)
Ralph Consulting LLC

Ms. Susan Lowenstam
Attorney

Mr. Philip W. Spence
The McVey Company International

Staff Assistants

Operations Panel

Mr. Mike Hendricks
Logistics Integration Agency

Information Dominance Panel

Dr. Bert Smith
ODCSINT

Sustainment and Support Panel

CPT Dennis Gibson
Pennsylvania Army National Guard

Training Panel

Ms. Cherie Smith
PEO STAMIS

Sponsors

GEN John M. Keane
U.S. Army Vice Chief of Staff

LTG John J. Costello
Commanding General
Space and Missile Defense Command

GEN John N. Abrams
Commanding General
U.S. Army Training and Doctrine Command

MG Charles C. Cannon, Jr.
Acting DCSLOG

GEN John G. Coburn
Commanding General
Army Materiel Command

Cognizant Deputies

LTG Randall L. Rigby, Jr.
DCG, TRADOC

LTG Paul J. Kern
MILDEP to ASA(ALT)

Operations Panel Gov't Advisors

Brig Gen James Bankers
U.S. Air Force Reserve Command

Mr. Earl Rubright
Headquarters, U.S. Central Command

Mr. Bob Dodd
TRADOC

Mr. Ralph Shaw
U.S. Army Reserve Command

BrigGen Donovan
U.S. Marine Corps Battle Lab

Dr. Mike Sculley
U.S. Army AMCOM

Dr. Jasper Lupo
Office of the Director of Defense Research and
Engineering (Sensors and Electronics)

Mr. H. Jack Taylor
Office of the Deputy Under Secretary of
Defense (Acquisition, Technology and
Logistics)

COL Mike Mehaffey
TRADOC

BG Jimmy Watson
Florida Army National Guard

COL Kip Nygren
U.S. Military Academy

Mr. Bruce Zimmerman
Office of the Assistant Secretary of the
Army(Acquisition, Logistics and Technology)

Maj Gen Paul Pochmara
DC Air National Guard

Information Dominance Panel Gov't Advisors

Mr. Craig Baker
SMDC

Dr. Bert Smith
ODCSINT

Ms. Alita Farr
ODCSINT

Mr. Paul Tilson
NRO

Mr. Kurt Kovach
CECOM

COL Ron Vandiver
TRADOC

LTC Jack Marin
U.S. Military Academy

LTC Keith Wooster
OCAR

Mr. Jeff Ozimek
CECOM

Sustainment and Support Panel Gov't Advisors

LTC Gary Engel
USARC

COL Dan Roh
AMC

BrigGen Feigley
USMC

Mr. George Scherer
TRADOC

MG Michael Gaw
USAR

MG Walt Stewart
Pennsylvania Army National Guard

LTC Matt Gorevin
TRANSCOM

LTC(P) Dan Sulka
USA DLA

Mr. Patrick Holder
TRADOC

Mr. Tom Sweeney
Army War College

Mr. Zbigniew Majchrzak
Deployment Process Modernization Office

Mr. Mike Williams
MTMCTEA

COL Buck Mandville
TRADOC

Training Panel Gov't Advisors

CWO Doug Champion
CECOM

Mr. Thomas Moore
Logistics Integration Agency

Dr. Mike Farmer
PM Distance Learning support contractor

COL David Raes
Iowa Army National Guard

Dr. Dexter Fletcher
Institute for Defense Analyses

COL Bob Reddy
TRADOC

MAJ Mike Freeman
Office of the Chief, Army Reserve

Dr. Sandy Wentzel-Smith
U.S. Navy

Dr. Stephen Goldberg
ARI

Mr. Bob Whartenby
CECOM

BrigGen Michael J. Haugen
North Dakota Air National Guard

Mr. Gary Winkler
PM Distance Learning

Dr. Michael Macedonia
STRICOM

Dr. Wally Wulfeck
SPAWAR

APPENDIX C

ORGANIZATIONS VISITED



Who We Visited



- Department of Defense
- DSB (Dr. Mike Frankel)
- OSD (Mr. John Osterholtz)
 - DARPA
 - GLOMO/MUBUL (Dr. Bob Ruth)
 - Smart Radar Tags (Dr. Dave Fields)
 - Advanced Concepts (Dr. Amy Alving)
 - DODCIO
 - CENTCOM (Mr. Earl Rubright)
- Department of the Army
 - ARL/SLAD
 - TRADOC
 - CECOM
 - RDEC
 - PEO C3S
 - PEO IEW&S
 - C4ISR
 - FCS C2
- Department of the Army (cont)
 - SMDC
 - ASPO
- Department of the Navy
 - Office, Chief of Naval Operations
- Commercial
 - Overlook Technologies
 - BBN
 - GRC, International Inc.
 - Global Infotek
 - ORACLE
 - LLNL
 - Overlook Technologies
 - TPED
 - BIOS

APPENDIX D

INFORMATION MANAGEMENT

APPENDIX D

Tactical InfoSphere Information Management

InfoSphere Management

Challenge - Establish an InfoSphere that will more efficiently direct relevant information throughout its life cycle to the right person at the right time in a useable form to facilitate decision-making.

- **Transition from legacy systems to an InfoSphere.**
- **Manage the InfoSphere.**
- **Provide useful capabilities to assist with command and control.**

Key Recommendations

- **Develop policies and procedures that can apply rapid changes in commercial technology.**
- **Scrub the current information requirements.**
- **Define a GIG-compatible data architecture.**
- **Attract and retain personnel necessary to manage the InfoSphere.**
- **Invest in appropriate C2 technologies.**
- **Design the system for Information Assurance and Security.**

The challenge of information management in the InfoSphere is to establish a tactical information system that will efficiently direct relevant information to the right user when needed and in a useful form. Achieving this objective will facilitate the Commander's decision making.

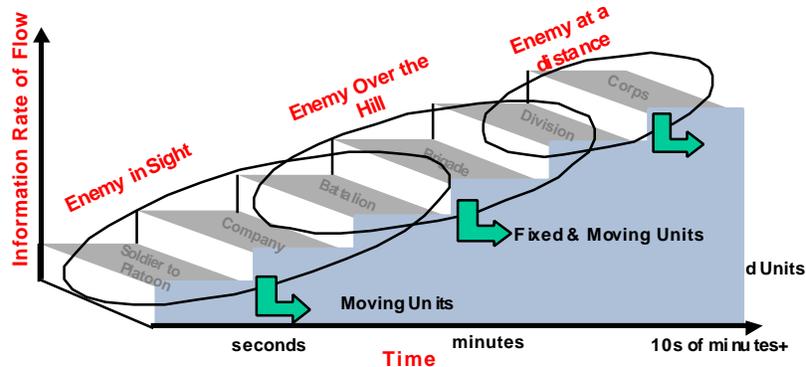
Why do we need to do things differently? First, we have in place legacy systems that are stove-piped and do not talk to each other. They are human-intensive in their operation, which slows down the passage of information. They are usually point-to-point, leading to a slower flow of information that is difficult to share.

In contrast the Tactical InfoSphere is an internet based system which makes use of automated servers and routers to transfer information quickly without human intervention. It is networked, meaning that many more nodes may participate in the sharing and use of the data. This also means that Situational Awareness can be made a cornerstone of its design. Further, connecting the Tactical InfoSphere directly to the Global Information Grid (GIG) will provide higher echelons real-time awareness of what is happening in the tactical domain and will provide the tactical echelons the "big picture." The TI will provide the decisive edge.

Transitioning our legacy systems to operate more effectively in the presence of the Tactical InfoSphere and the GIG will not be easy. It will require appliques to legacy systems to permit new hardware to function in the presence of older hardware; it will support a major reorientation in our approach to communication, fire direction, fusion of information, control of maneuver, and logistics. It will support streamlined, real-time processes.

In the future, because of the presence of the Tactical InfoSphere, the "Chain of Information" will not always follow the Chain of Command. While The Tactical InfoSphere will support the traditional echelon approach to command and control, it will not necessarily provide information by echelon. This is necessary if the TI is to distribute combat information in real time.

Time Scale and Information Flow Needed at Each Echelon



Lower echelons have to operate on very short time scales and require minimal information flow, but there are many soldiers!
Higher echelons operate on longer time scales and require lots of information at fewer nodes.

In planning the management and use of the InfoSphere, one must think of the information content flowing from echelon to echelon and of the time scale of that flow. At lower echelons, the soldier is more apt to be engaged in close combat where instantaneous voice communication will warn him of near term, life-threatening situations. In these cases only short warnings are needed. The information content is low, but is extremely important and must be transmitted on the time scale of seconds. At the intermediate echelons where engagement is often imminent, planning and support become more important. The types of information are different, with more emphasis on the coordination of troop movements and unit identification. The volume of this type of information is higher and the flow of information content may be slower than in a firefight, possibly of the order of minutes. At the higher echelons where staff size is larger, the planning cycle is longer, more complex communication equipment is available, and the information volume of the command is higher. Here the time scale for planning information is longer – of the order of tens of minutes at Brigade and perhaps an hour at Corps HQ.

The classic timelines for information management are changing with the fielding of long range weapons like ATACMS, which is managed at Division or Corps. Because this weapon can attack mobile targets it is critical that at least the targeting information have near zero latency. Providing real time information at higher echelons has been impossible in the past. The bandwidths for communicating relevant information at the higher echelons will be larger for at least two reasons – broad band fiber optics and landlines will be present, and the higher echelons will be able to make good use of them. The bandwidths available for moving units will be considerably smaller, necessitating prioritization of the use of the narrower bandwidths. The challenge of “the last mile” is a serious and important one. Although the individual foot soldier may not need much information per unit time to be effective, there are a very large number of them who all must share a scarce resource – bandwidth. This makes the need for Information management within the Tactical InfoSphere particularly acute.

InfoSphere Management: Making the Tactical InfoSphere Work

- **Collect and process the information users need:**
 - Integrating sensors
 - Synchronizing data storage
 - Constructing the operational picture
- **Move the information as quickly as technically possible:**
 - Tailor methods of data dissemination
 - Develop intelligent routing techniques
 - Ensure flexible, responsive, and secure communications
- **Policies and procedures governing InfoSphere Management**
 - Requirements-based analysis of doctrine to determine automation equipment.
 - Hardware & software must be frequently updated



The presence of a Tactical InfoSphere and its tie to the (GIG) is a sufficiently new concept that will require extraordinary management and monitoring. The processes embedded in the collection, processing, and transmittal of information differ from the traditional ways of doing business. The details of the process, how the information is shared, the handling of databases, and the real time development of Situational Awareness, are all new.

During the collection and processing of information, sensor coverage must be managed, the data collected by the sensor must be automatically processed to provide a machine-readable report, and an operational picture generated.

When information is moved from node to node, new methods of data dissemination must be tailored to each individual user using intelligent routing techniques that get the information where it is needed with the least possible delay. Since the battlefield is constantly changing and constantly undergoing reconfiguration, the movement of information must be done with security and with as much flexibility and responsiveness as the system will permit.

For these reasons, policies and procedures must be established for the InfoSphere. Clearly the focus must be on real time processes if the TI is to meet the needs of the tactical warfighter. Because of the reliance on COTS standards and products the vulnerabilities of the Internet will be inherent. The excellent work by the DSB in the March 2000 report "Tactical Information Management" addresses the processes and procedures necessary to protect these battlefield systems.

InfoSphere Management Challenges

The design, manipulating, and controlling of information throughout its life cycle in order get the right information to the right person at the right time to facilitate better decision-making.

Nature of the Problem

- **Overzealous definition of commanders' needs produces technically infeasible solutions because of bandwidth and processing limitations.**
- **This InfoSphere must be configurable to support any mission, but have minimal impact on operators' activities.**
- **The quality of decisions made is directly effected by the InfoSphere's rapidly evolving hardware & software capabilities.**
- **Security penetrations by the enemy could have unimaginable, far-reaching effects.**
- **The Army is competing with the civilian sector for technically competent officers, enlisted, and civilians.**

The major challenge of the InfoSphere Management process will be to design, structure, and oversee its interface to the GIG. The InfoSphere must ensure that directly relevant information is quickly routed to the right place in a form that is actionable by the decision-maker.

A major problem is battlefield automation required for legacy systems. There has been an overzealous definition of the commanders' needs. These requirements, if slavishly followed can lead to a level of system complexity or over taxing the available bandwidth, both resulting in information which is time-late, hence useless.

The challenge to the structure of the InfoSphere is that it must be configurable and flexible enough to support any mission. In addition to flexibility, commander's ability to make rapid and timely decisions must not be impacted by the reconfiguration of the InfoSphere.

The presence of the InfoSphere and its tie to the Global Information Grid must be as transparent to the Commander as possible. To accomplish this in the presence of rapidly changing hardware and software capabilities will require continuous oversight of the process.

Two other challenges to InfoSphere management will be:

- The need for good security, since enemy penetrations of databases and communications links will have far reaching effects.
- The need to identify, recruit, and retain technically competent officers, enlisted and civilian personnel in the face of strong competition from the civilian sector.

Ingredients for a Successful Transition

Legacy Systems → Infosphere

- **Conduct a ruthless scrub of the stated requirements by Battlefield Functional Area (BFA).**
- **Limit FBCB2 implementation to only the bare essentials.**
- **Define the architecture for a common data sharing environment (e.g., ownership, unit requirements, storage).**
- **Much of the functionality of current software can be modularized and directly applied to the InfoSphere.**
- **The Army needs a major human factors program to determine effective computer / display interfaces with a Battle Captain operating on the move - See ASB C2 On The Move 1992.**

Current management system cannot take advantage of rapid advances in commercial technology.

To make a successful transition from our legacy systems to the Tactical InfoSphere, the following actions will be required.

- Conduct a thorough, detailed review of the requirements within each battlefield functional area and limit the Objective Brigade implementation to *only the bare essentials*.
- Investigate the sharing of information with elements on the battlefield and determine, what requirements each unit has, and determine where, how, and if the data should be stored and shared.
- Investigate the extent to which the software can be modularized to support a truly distributed processing environment.
- Initiate a robust human factors program, to determine the most effective computer/display interfaces to the Warfighter, to support rapid decision making.

The Tactical InfoSphere will require a major shift in the Army's traditional approach to implementing the entire C4ISR process. The current DOD acquisition cycle exceeds a decade in an environment in which commercial technology doubles capability every two years. A very innovative acquisition approach must be used if we are to capitalize of the COTS revolution. In information Warfare environment, one may face a threat who has equipped his small but elite force with the latest in commercial equipment - which might be five to ten years newer than ours.

C2 Support

Provide necessary capabilities, such as Situational Awareness, Course of Action (COA) Analysis, and Mission Planning and Rehearsal to the warfighter.

- **The essence of command will remain unchanged!**
- **The InfoSphere will greatly accelerate the flow of information, but, the amount and magnitude of information will challenge commanders.**
 - **Commanders will require a common operational picture of the battlefield. Data fusion, synchronization, transmittal (bandwidth), and timeliness will be major obstacles.**
 - **The InfoSphere must allow planning processes that are parallel and collaborative, to include the concept of a Virtual staff.**
 - **Software must be developed to assist with COA formulation, visualization, assessment, and rehearsal. Pursuing technologies that require expert knowledge of the commander's thought process will be unproductive.**
 - **Intelligent agents will be required to search available data sources for needed information.**

Preventing information overload is a persistent concern in the Army. The solution lies in Information Management which provides the Warfighter the ability to descope the information provided to his platform by geographic area, by type of information (tanks, but not trucks) and by correlating multiple reports on the same entity to show one tank, not 100 tanks. The Army must continue to invest in necessary capabilities to provide the warfighter with better situational awareness, course of action analysis, and mission planning and rehearsal.

We are in agreement with the precepts concerning the Operational Concept, Enabling Concepts stated in Chapter 3, part 3 of the draft of *The Army Vision* dated 12 June 00. These points are emphasized below:

- The essence of command will remain unchanged! We strongly believe that technology will never replace the human decision process. Technology should assist the human in command and control decision making.
- The InfoSphere will greatly accelerate the flow of information, but the amount and magnitude of information will challenge commanders as well as InfoSphere managers. Our message here is simple – beware of information overload.
- Commanders will require a common operational picture of the battlefield. The types of information that must be fused to provide a common picture will come from single or multi-spectral imagery, SIGINT, HUMINT, spot reports, and perhaps real time video. Fusing this information for a variety of users, poses a significant problem. By implementing a process in which: data sources detect and automatically report "targets" digitally, reports can be broadcast to users in the area and fused on the combat platforms in real time. This approach could be implemented by 2010. Synchronization of the data refers to the process of ensuring all proponents are looking at the same common operating picture.

Current and anticipated commercial technologies, such as client-server and multicast, should enable users to develop very similar "common operational pictures."

The InfoSphere will allow planning processes that are parallel and collaborative, to include the concept of a Virtual staff. Technologies, such as white-boarding and collaborative decision support systems are currently available and will continue to evolve during the timeframe of this study.

- Software must be developed to assist with COA formulation, visualization, assessment, and rehearsal. Pursuing technologies that require expert knowledge of the commander's thought process will be unproductive. Since military decision-making is remarkably personal, it is doubtful all military experts would agree on an identical course of action given a complex situation. The commander will generally take the first, practical solution that appears workable. Thus, knowledge acquisition would be a difficult process. Machine learning systems, such as neural networks, genetic algorithms, or Bayesian Decision Trees require an abundance of training data that is not generally available. Additionally, the ability of these systems to adapt to unforeseen circumstances is suspect.

Intelligent agents will be required to search available data sources for needed information. We fully expect the commercial industry to develop these applications.

InfoSphere Management Challenges and Innovations (I)

- **Issue: Infosphere managers must design and test information support plans for tactical commanders.**
- **Innovations:**
 - **Software that recommends system configurations based on tactical mission requirements.**
 - **Information flow simulations to test the information plan and identify possible vulnerabilities.**
- **Challenge: “Buy-in” at all levels on how the Infosphere will fundamentally change the Army’s approach to voice and data communications**
- **Issue: Infosphere managers must create the information support package for tactical commanders.**
- **Innovation: Plug and play, intelligently configurable systems, smart routers, and thin clients.**
- **Challenges:**
 - **Prioritization of info content because of limited available bandwidths, particularly at lower, more mobile, echelons**
 - **How to transmit, receive and protect classified data**

Managers of the InfoSphere must design and test the information support plans that will serve the needs of the tactical commanders. This process will require innovative software that will recommend system configuration changes that will occur rapidly as the battle situation evolves. It will require simulations of the information flow to test the information plan and to identify weak points in the changing configuration. The challenge will be to “buy-in” at all levels of management to be sure that all those levels understand how Army’s new approach to communications will change the use and effectiveness of voice and data communications.

Managers of the InfoSphere must create information support packages for the tactical commanders. This process will require innovative (1) plug and play techniques; (2) intelligently configurable systems that are machine-intensive and do not require significant human intervention; (3) smart routers that can determine who the recipients should be based on the originator and/or the information content; and (4), thin clients. The challenge will be to prioritize the information content, particularly within moving echelons with limited bandwidth. In addition, the challenge of how to transmit, receive, store and protect classified data is ever present. Perhaps the perishability of the data may be a clue to solving this problem – timely data that requires a short response time may not need to be classified at all, since, with the passage of time, it will not be useful to the enemy either.

InfoSphere Management Challenges and Innovations (II)

- **Issue: Infosphere managers must oversee a system that gets the right information to the right echelons in the right format at the right level of detail at the right time.**
- **Innovations:**
 - **The GIG enables information to flow to any echelon and is joint.**
 - **Chain of information flow may not be the same as the chain of command.**
- **Challenges**
 - **Role of Army managers in the Army and in the Joint arena**
 - **Each sensor must report its collection – to whom and how?**
 - **Data sources must share information – with whom and how?**

Managers of the InfoSphere must oversee the information flow process so that the right information gets to the right echelons, in the right format, at the right level of detail, at the right time. Innovations will enable information to flow freely and quickly to and from the GIG as well as into and out of all Army echelons and communications nodes.

This innovative way to communicate will entail communication links that will not necessarily follow the normal chains of command. It will be a challenge for the modern commander to take advantage of this new capability and to exercise normal command functions while units are obtaining and giving out information to other units.

Implementing these new innovations will involve Army communications managers in broader communications interfaces than they have previously experienced. Much more emphasis will be on lateral communications, the routing of sensor information, connectivity in the joint and allied systems, and the use of shared databases across all echelons.

Technology Needs

... not expected to be available from commercial-off-the-shelf

- **Information management software and algorithms necessary to assist warfighters in decision-making**
- **Improved sensor and data fusion**
- **Improved target recognition**
- **DOD Specific security needs:**
 - **Information Assurance (esp. counter computer network attack)**
 - **Multi-level security classification**
- **Improved ruggedization over COTS systems (e.g. shock, vibration, low probability of detection)**
- **Simulation and training needs**

TECHNOLOGY NEEDS -- Do not compete with or replicate commercial development that Army can use.

A large part of the hardware and software that will permit the Army to be a major player in the Tactical InfoSphere is under development as COTS. It will also be available to our adversaries as well as our allies. Army information managers must stay abreast of these developments, buy these new capabilities intelligently, and tailor their application to Army use. Investment will be required for technologies that will:

- Aid the commander in making decisions
- Improve the processing of sensor data and fusion;
- Improve the timelines and validity of target recognition;
- Increase levels of security and handle different levels of security classification efficiently, within the Tactical InfoSphere and its connection to the GI
- Ruggedize COTS components to operate under extremes of weather, shock and other battle conditions that are not normal in civil applications;
- Provide realistic simulations and training aids.

Key Recommendations

- **Develop policies and procedures that can react to the rapid changes in commercial technology, identify Army-specific needs, and apply DOD Research and Development to those needs.**
- **Scrub the current information requirements for each element in the InfoSphere.**
- **Define a GIG-compatible data architecture to ensure that each element in the InfoSphere will get the information it needs.**
- **Identify and provide the incentives necessary to retain officers and enlisted soldiers who are necessary to manage and operate the InfoSphere.**
- **Invest in technologies that will accelerate, but not replace, the command decision process.**
- **Ensure that information assurance and security are not an afterthought; otherwise, the entire system is subject to failure.**

The following recommendations are offered to assure successful implementation of the TI.

- Develop policies and procedures that will enable our acquisition system to react to the rapid changes in commercial technology so that they will be up-to-date and useful to the Army. The rapid insertion of new hardware and software will be required to meet Army-specific needs, which also must be identified. The R&D for supporting the future of the InfoSphere should be identified through the development of a Systems Architecture that will expose necessary (non-COTS) capabilities that must be developed.

- Scrub current information requirements for each node (element) in the InfoSphere that sends or receives information. This process must consider nodes that are on the boundaries of the force, or that are accessing the GIG. Emphasis must be on information exchange with other Services and allies.

- Define Architecture to ensure that each element in the InfoSphere will get the information it needs, and is able to contribute the information it has that other elements will need. This structure must be GIG compliant, and ensure that information assurance and security are not an afterthought; otherwise, the entire system is subject to failure.

- Manage expectations. The bandwidth available to carry information to and from moving echelons is limited by physics. This fact requires prioritization of the information that MUST be sent and received.

- Identify the officers, enlisted men and civilians who are necessary to design, implement, manage, and operate the InfoSphere. Provide the incentives necessary to retain them.

APPENDIX E
COMMUNICATIONS

APPENDIX E

Communications

Communications

- **The Army lacks a communications network to support the Objective Force**
- **Tactical InfoSphere communications (based on commercial and technical) must be a multi-layered (space, airborne, and terrestrial), self-healing, mobile network that fuses platforms and soldiers**
- **The most pressing challenge is establishing a viable, “plug and play” architecture for the Tactical InfoSphere**
- **Leverage, adapt, and build on commercial, mobile networking and wireless technologies**
- **Establish MOSAIC as the priority program to build an enabling Tactical InfoSphere**
- **Integrate commercial Army and DARPA technology through MOSAIC**
- **Current technology assessment: Green to Yellow**
- **Support Tactical InfoSphere within the GIG**

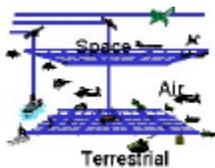
Robust, timely, and secure communications are essential to the implementation of the Tactical InfoSphere for the Objective Force. This communications system will be largely based on commercial communications technologies, with augmentation from DARPA and the Army in those areas that are military specific. The following slides discuss these ideas and comments relating to the communications system needs for the Tactical InfoSphere:

Operational Challenge - Communications

Nature of the Problem

- Comms network is line of sight, point-to-point
- Contemporary Radio provides very limited bandwidth
- Tactical forces have limited assured non line-of-sight communications
- Legacy, stove-piped, systems costly to maintain
- Situation awareness limited by LOS sensors, and comms
- Missing/late messages

GIG



Tactical InfoSphere

Objective

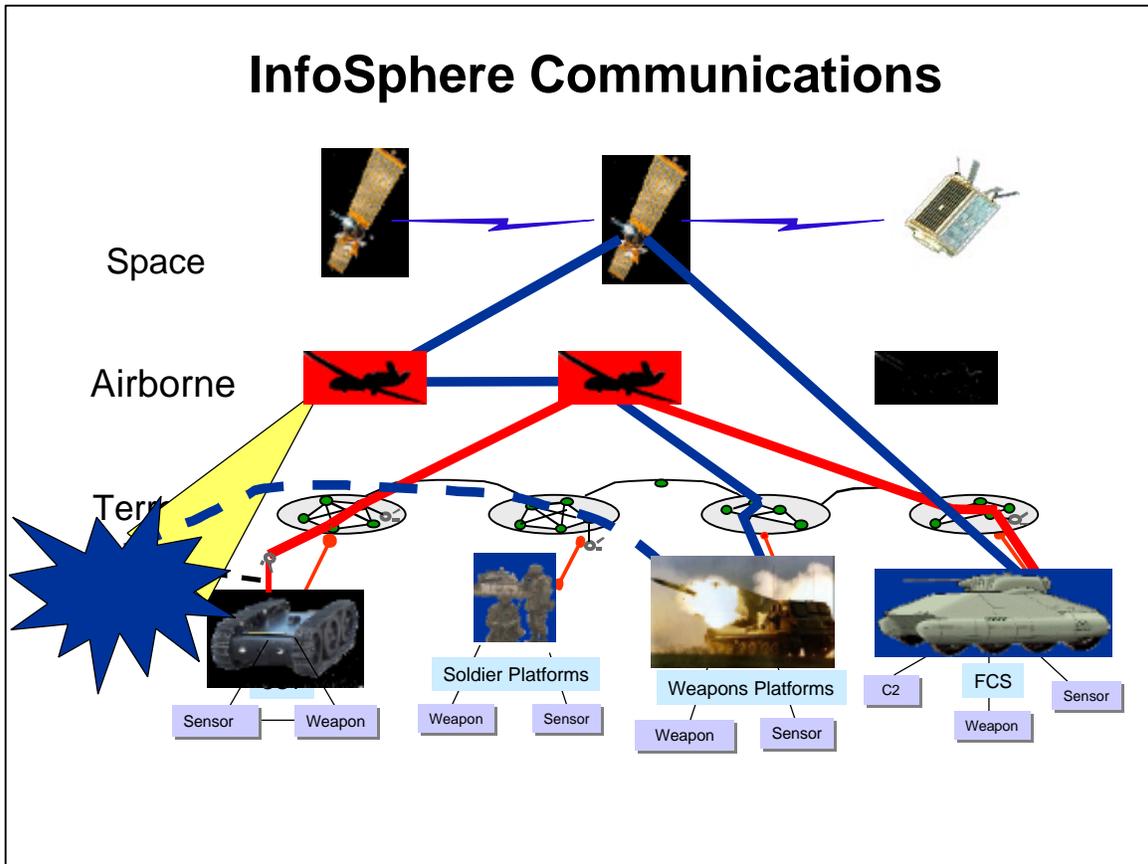
- Fully networked, multi-layered (space, airborne, and terrestrial)
- Compatible with the GIG for Joint and Coalition interoperability, and reachback
- Wide bandwidth, LPI, Smart radios with routers, processors, and technologies to maximize spectral bandwidth efficiency
- Based on commercial technology augmented by Army/DoD developed technology
- Robust, self directing, self healing networked comms

There are enormous challenges, and opportunities, in creating the information system needed for the Objective Force. On 31 March 2000, the Deputy Secretary of Defense issued a Guidance and Policy Memo on the Global Information Grid (GIG). The memo described the GIG as “a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.” The next generation of communications and information systems will be designed to provide military, networked capability largely based on the commercial Internet. The Army challenge is to develop a mobile network, compatible with the GIG, which includes the characteristics discussed below.

Existing and programmed Army communications, although adequate at the higher echelons, are woefully antiquated and inadequate to support the Objective Force. Current Army terrestrial communications systems are limited to line-of-sight (LOS), narrow-band, point-to-point communication links. (SATCOM terminals have been issued to the Brigade, but operational experience shows that transponder access is rarely allocated at this level.) Furthermore, existing data radios are severely limited in bandwidth (data throughput), are stove-piped (vertically integrated), are costly to maintain, and often have prolonged latencies resulting in missed or late messages. These systems not only constrain accurate situational awareness and command and control today, but they are hardly adequate for the additional demands of the Objective Force, such as near-real-time-sensor to shooter communications.

The communication system needed for the Objective Force will be very different. It needs to be fully networked and multi-layered. The networks for this communications system will be self-directing (ad hoc) and self-healing. It must provide sufficient, flexible, scaleable bandwidth (data

throughput) to support the information flow within the tactical AOR. It must also have the reachback capability for the support of functions such as sustainment, training and intelligence. By being compatible with the GIG, issues of Joint and Coalition interoperability, if not completely solved, become workable. Future JTRS radios for this system should be designed as follows: (1) built in network management, (2) IP network compatible, (3) wider in bandwidth (data throughput), (4) low probability of intercept and detect (LPI/LPD) waveforms, and (5) capability to maximize and adapt spectral efficiency for any geographical region. Commercial telecommunications technologies will provide the core technologies, but must be integrated with Army/DARPA technologies and engineered to service the Tactical InfoSphere.



The Army has stove-piped communications systems which parallel the echelonment of the force. The Army must move to an integrated network concept to achieve the Tactical InfoSphere, by adopting, adapting, and developing technologies needed to accomplish this vision. Communication systems must be integrated with the information management, assurance (security), and distribution systems. To enhance warfighting capabilities, reduce operational footprint, and improve deployability, the Army needs to simultaneously eliminate as many wires and cables as possible, while increasing throughput and decreasing vulnerability. Much of the backbone infrastructure for Objective Force will be provided by the space and airborne systems. The movement towards the space and airborne support will significantly reduce the footprint and improve deployability. This reduced signal footprint will allow deploying Objective Force units to have full communications capability throughout their deployment.

The Tactical InfoSphere is based on the “living Internet” that provides mobile NLOS communications. The concept is predicated upon the emerging DoD’s Global Information Grid (GIG) infrastructure. The GIG will provide ubiquitous data/information transport and distribution to the warfighters, independent of location degree of mobility, or platform dynamics. It will utilize a heterogeneous mixture of available media, including civilian fiberoptic cable plants, landlines, terrestrial and satellite based wireless services, and unmanned aerial vehicle (UAVs). This infrastructure will be a mix of both commercial and military systems. It will integrate these components into a seamless, dynamic, and extensible information transport system that is scaleable and has security appropriate to the military mission and the information warfare threat.

The Army must move from a physical network and bandwidth management orientation to a virtual network comprised of broadcast (multi-cast) and a “service-on-demand”. The communications architecture, as shown on this slide, contains the same components previously

described in the GIG. This Joint and global infrastructure is comprised of both commercial and military systems and is richly interconnected with cross-links.

The Joint TI concept moves Army communications from a two dimensional grid to a three-dimensional sphere. Traditionally, Army communications has been predominantly line of sight with relays and nodes creating an extended range of connectivity. At the higher echelons, satellites are used to provide connectivity between major nodes well beyond the range of line of sight. The Joint Tactical InfoSphere will expand the capability to three dimensions with increased routing and relays over the battle space. This is particularly beneficial at the lower echelons where speed of movement and operational lethality is important. It allows for continuity of communications while conducting maneuver and reduces the communications support infrastructure that is deployed with the forces. At higher echelons, where movement is not so rapid, a more traditional terrestrial-based backbone is an alternative.

The overhead connectivity is layered and consists of terrestrial, airborne, and space layers. The architecture provides secure, wireless, high-speed, 100% digital packet or cell based, service to soldiers independent of echelon. The terrestrial communications layer contains a myriad of points-of-presence such as soldiers, weapons, vehicles, attended and unattended sensors. All points-of-presence are capable of performing a relay function. The overhead airborne communications layer contains a robust, multi-level secure, backbone infrastructure that supports the terrestrial layer. Low Earth orbit (LEO), medium Earth orbit (MEO) and geostationary Earth orbit (GEO) satellite constellations may provide a backbone infrastructure along with fiber optic systems. This diversity of backbone elements provides robustness. For low to moderate threat deployments, a mix of DoD and commercial satellite constellations should adequately support the Joint tactical forces. However, a multi-level airborne communications relay capability must be deployed to support communications timelines and ensure robust and sufficient data through-put.

These nets will allow distributed data analysis and mission planning. All information being moved through the network will be in packets or cells, whether it is voice, data, pictures, maps or video. At the very front of the forces, where small size and rapid movement is most important, radio systems will be able to organize autonomously into line of sight nets where the terrain permits. When that is not possible, nets will organize using overhead assets of airborne relay platforms or satellites. The small line of sight nets will also be connected beyond line of sight by airborne and space systems. Some of those airborne systems will be small but with concise coverage to provide support in both otherwise potentially inaccessible areas such as natural and urban canyons.

Perhaps the most fundamental transition into the Tactical InfoSphere is to move from a concept of physical networks and assigned bandwidth to the concept of "service-on-demand." It starts with implementing Quality of Service (QOS) capabilities for existing networks and progresses to virtual networks that transparently utilize the available RF spectrum.

Virtual networks will support all users/functions. The architecture supports global split-base operations, enabling virtual network participants anywhere around the globe and in space. The virtual network concept is a powerful enabler for dynamic bandwidth utilization. It allows the totality of the available physical capacity to be pooled and dynamically allocated to the virtual networks. Service can be automatically assigned based on priority of the transmission function; an example is information to assign a target and fire on it being given preference over a wide bandwidth video teleconference (VTC). The network management system negotiates with applications such as the VTC to obtain bandwidth by reducing picture quality in preference to interrupting service.

Based on the Internet concept of sending packets of information, the ground segments become a mobile Internet. The optimum design, assuming no bandwidth limitations, would provide voice, data and video. No longer would there be one earth terminal for inter-switch trunking, and wholly different terminals for reception of stove-piped systems such as weather data. Since all information is packetized, any terminal could perform a multitude of functions as well as reduce logistics costs. A modular design would also allow the terminal physical size to be optimized for the mission.

At higher echelons, where movement is not so rapid, a more traditional terrestrial based backbone would be established. It would seek to maximize application of existing infrastructure. Where existing infrastructure is not sufficient, a civilian contractor could be called upon to install the infrastructure. This contractor would be one of several on a “retainer” contract, much like the Civil Reserve Air Fleet.

Connectivity Concept

All communications are done in packets or cells. The user’s communications units arrange themselves in networks based on the ability to physically connect together, not by operational hierarchy. The packets are routed through this physical network toward the users that are in the “operational net”. Thus, the physical and operational networks are not necessarily the same. Within the richly interconnected network, information is moved among users and sources. Some small, localized relays may be utilized to insure communications network paths can be continued in urban areas and extremely difficult terrain. Airborne relays provide connectivity over longer distances and complement the space layers to provide increased throughput and access in active theaters. The space layer is the global infrastructure, tied to the terrestrial infrastructure at many points. All layers are interconnected, or capable of being interconnected, with each other. Thus a SOF element with a portable TACSAT terminal can connect to the grid directly via satellite if needed, or with peers via a short range line of sight link if available. It is envisioned that sensors with smart “onboard processing” would be directly connected to this grid, so users can gain quicker access to information, particularly that of local interest.

Radios accessing the network will intelligently select the best available RF frequency. To avoid overloading airborne and space relays, radios will look first for a terrestrial connection. Each unit will be capable of being a node in the system; therefore, there will be no concentrated points of vulnerability. The military network will tie into and use the worldwide terrestrial commercial fiber infrastructure. Common, modularized components will be carried based on platform needs. Commercial systems and technology will be used as much as feasible.

For initial deployments into a hostile area, the forces will use the space systems for enroute communications and initial operational support. As the theater activity and forces build, an airborne layer will enhance connectivity. As the buildup increases, gateways into the commercial terrestrial fiber infrastructure will be connected.

During the buildup, high-altitude UAVs will be vital. By the time the Army is fully transitioned into the Objective Force, new generations of satellites and aerial vehicles will permit the establishment of an intelligent information infrastructure backbone in both the airborne and space layers. At this distant date, the networks for unattended sensors, munitions, and robots will have been integrated into the terrestrial layer and, as a minimum, the Objective Force will have migrated to virtual networking and service-on-demand.

Challenges and Innovations - Communications

Challenges	Innovations
Adopt an approach to leverage major advances in wireless commercial technology	Program for the engineering and integration of commercial standards and technologies
Establish Tactical Infosphere within the Global Information Grid (GIG) to achieve Joint and Coalition interoperability	Design all systems to plug-and-play within the GIG
Develop future (JTRS) radios designed for IP	Redirect JTRS program to assure IP capability and harmonization with commercial wireless access technologies
Establish a multi-layer communications architecture to support non-line-of-site communications	Acquire dedicated UAVs under the control of Army Brigade
Adopt a spiral process to design and build under a "system-of-systems" scalable architecture	Establish a single PEO for C4ISR with strong system engineering capability and authority over Comms, ISR, EW

To realize the Tactical InfoSphere by the 2010, the legacy circuit-switched communications must be phased out and replaced by integrated packet switching for all combat and support functions. Each wireless device function, whether sensor, communications, or EW, should be inserted into the InfoSphere network on a plug-and-play basis. The hierarchical communications structure of today will be flattened; i.e., peer-to-peer connectivity between sensors, shooters and EW players should make maximum use of available bandwidth, and information sharing will be enabled.

Platforms such as the FCS will be capable of maintaining a common picture and opportunistically "seeing, hearing, smelling, tasting and feeling" the battlefield through both their own and various sensors. Beyond 2015, these functions will be merged into common RF devices, driven by high-capacity microprocessors, powerful digital signal processors, wideband analog-to-digital and digital-to-analog converters, and multi-function/multi-band RF hardware, including antennas. When the Tactical InfoSphere transitions into a mature system, each platform will simultaneously serve as both a source and subscriber. In order for the Tactical InfoSphere to become a mature system, five categories of challenges and innovations must be pursued today.

The first challenge is the implementation of an Internet Protocol (IP)-based architecture by leveraging commercial technology developments in the wireless Internet arena. The most immediate goal should be an architecture that is based on an "IP router" on every platform; thus, every platform serves both a specific function (e.g., weapons platform, radar, SIGINT, ELINT, fuel truck, or MLRS launcher) and also as a network communications node. Currently, CECOM has initiated a program called the Multifunctional, On-The-Move, Secure, Adaptive Integrated Communications (MOSAIC) that is a credible start towards this new architecture.

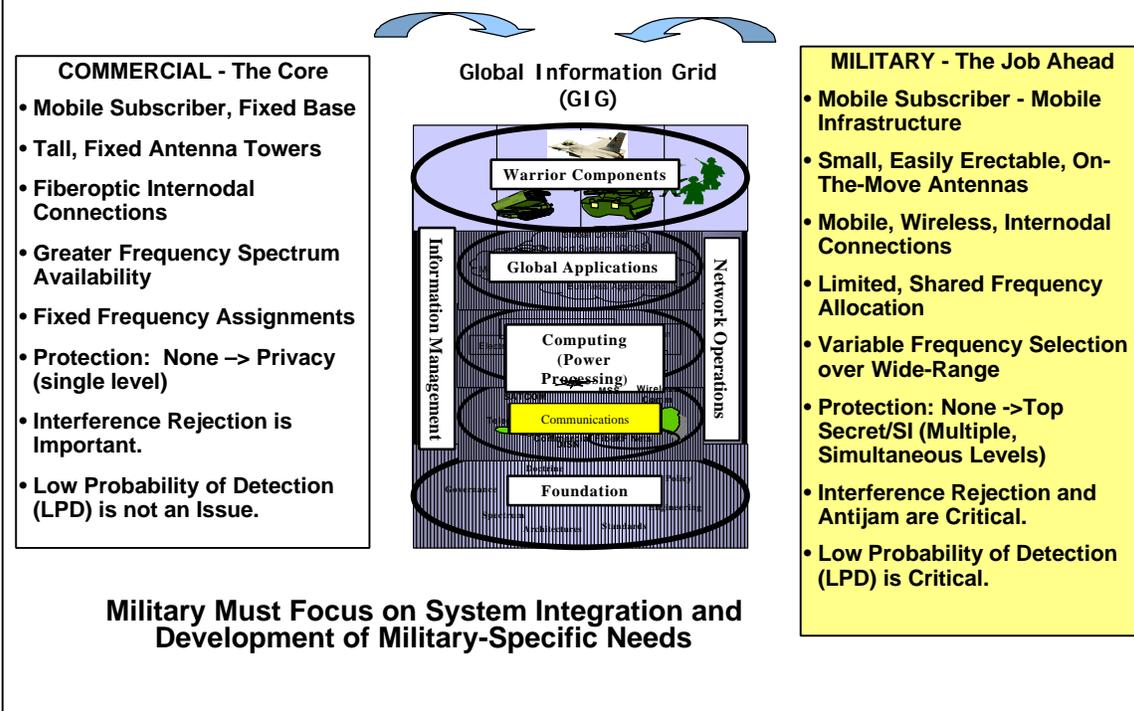
The second challenge is to establish the Tactical InfoSphere within the Global Information Grid (GIG). This achievement would largely resolve any worries about interoperability with Joint and Coalition forces. The innovation needed to develop this capability is to ensure that all systems and users can plug-and-play within the GIG. This is analogous to the current commercial trend toward global roaming, ad hoc capability, where any cell phone can become an integral element of the worldwide telecommunications infrastructure the minute it is turned on regardless of its location.

The third challenge is to develop IP-based, wideband capable radios for the Tactical InfoSphere. To accomplish this challenge, the JTRS program must accommodate integral IP-routing, spectrum efficiency, variable bandwidth, reduced power consumption, reduced weight, and LPI/LPD.

The fourth challenge is to establish a multi-layer communications architecture to support non-line-of-site communications. An indispensable component of this architecture will be long duration UAVs that are OPCON to the Brigade and are capable of relaying multiple channels of JTRS traffic.

The final challenge is the adoption of a spiral development process to systematically transition into the Joint InfoSphere new commercial technologies as they become available. This will require astute program management. The fact that the new technologies will have applications for soldiers, weapons, platforms, sensors, etc., the recommended management structure to meet the challenge is to have a single PEO responsible for the Joint InfoSphere. Second, systematic transitioning of new technologies will require an innovative acquisition strategy. Fortunately, the Federal Acquisition Regulations are sufficiently flexible to accommodate an innovative acquisition strategy.

Communications Technology



Implementation of the Tactical InfoSphere will require radically different communications technologies than those currently used by the Army. Circuit-switched communication technology will be replaced by packet-switched networks. Sensors, manned and unmanned vehicles, national information sources, intelligence assets, communications nodes, and individual communications will, be analogous to Web sites and subscribers in the commercial sector, by all being treated as information sites and points-of-presence within the network. Each such entity will be multifunctional - simultaneously a wireless communications node, a router, a sensor, a processor and a database – all accessible by authorized members of the Tactical InfoSphere by an Internet Protocol (IP)-based system. This structure can support the integration of command, control, communications, data and imagery capability into a single warfighter device. This solution is a major departure from legacy Army systems, and it will support radically different operational. It will require significant investments in the new technologies.

Fortunately, much of the technology to implement this structure is being aggressively pursued in the commercial sector. This chart indicates the match between the elements of the Tactical InfoSphere, and the corresponding trends and investments in commercial technology. At the highest level, the “seamless integration” sought by the Army is directly related to “convergence” in the telecommunications industry. Convergence is the trend toward the delivery of multi-media – voice, data, video – through a seamless, ubiquitous IP based infrastructure, to any user, using a single, multifunction access device. Third and fourth generation PCS is an example of this trend, and also an example of the rapid progress toward that full capability. These services should be available in one year, and within five years, respectively.

The opportunity to build on commercial telecommunications investments in technology becomes evident when comparing the technical capabilities and operational functions in the two domains: the Army Tactical InfoSphere and the commercial wireless industry. The requirement for the Tactical InfoSphere user is to use a single, automated interface to interact with the InfoSphere. The functions include ordinary communication; that is, transmitting and receiving voice, data, or video to/from any recipient in the InfoSphere. The technology to accomplish this function with IP-based common protocols is clearly achievable in the emerging commercial technology.

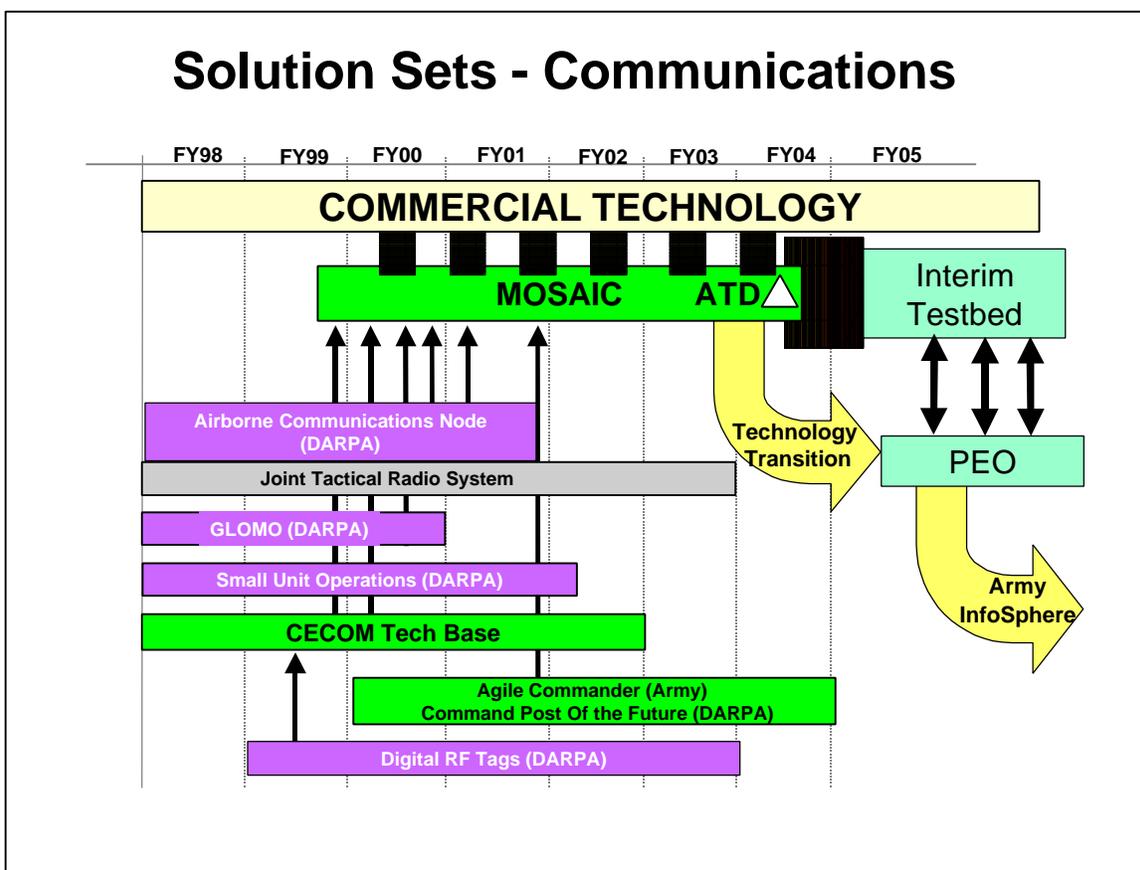
Another required function is to access information resident on other platforms, broadcasts, and databases residing elsewhere in the Battlespace or in the CONUS. In addition, the warfighter will need to “post” information he or she has produced, for distribution, either by “broadcasting” or allowing access to a particular site. This functionality is an essential attribute of the convergence in telecommunications services being engineered into the next generations of wireless devices and infrastructure. The need to command and control remote devices, whether manned or unmanned, must also be supported. It is encouraging that the commercial sector supports such remote control of devices through the Internet.

In addition, the Army needs to address military unique requirements for: (1) security, (2) mobility in routers and relays, (3) devices that have a simplified, intuitive user interface, (4) plug-and-play capability into the Tactical InfoSphere. Commercial wireless industry is addressing all but one of these technical solutions. The one significant difference is in the router and “base-station” infrastructure. The Army needs mobile routers and relays mounted on every airborne and ground-based platform. The commercial sector is currently designed around the use of fixed cell towers. This difference will require substantial investment to adapt commercial router technology and its associated configuration software as a solution.

The Army’s required functionality described above can be supported by the Internet and World Wide Web constructs being merged into the commercial wireless service providers. “Convergence” in the industry is causing billions of development dollars to be invested in perfecting these capabilities for the consumer. However, to adapt and leverage the commercial technology, the Army must reengineer C4ISR to require that every platform, wireless device, database, sensor and soldier be configured to behave as a “Web-site”, router and communications port within the Tactical InfoSphere. In essence, every member of the network must be configured as a full-functioned point-of-presence within the IP-based network. It must be capable of being accessed as an information source, communicate and relay information packets within the InfoSphere.

To implement a solution based on this approach requires commitment to change the process in which the Army designs and develops systems. DARPA and the Army have already begun working toward some of these capabilities.

Solution Sets - Communications



The Army Communications and Electronics Command (CECOM) has an approved Advanced Technology Demonstration (ATD) Program called Multi-functional On-the-move Secure Adaptive Integrated Communications (MOSAIC). The focus of MOSAIC is to demonstrate the integration of highly adaptive, networked communications to support a seamless flow of multimedia services across a layered (terrestrial, airborne and satellite) communications architecture. MOSAIC will be IP-based and utilize open systems solutions. It will conform to the Joint Tactical Architecture (JTA) and will be compatible with the Global Information Grid (GIG). The network will be designed to accommodate the mobility of tactical forces. The wireless network will support: Quality of Service (QOS) for streamed services; ad-hoc networking; bandwidth management; traffic scaling and multimedia applications. MOSAIC will build on a core of commercial technology and standards that will be integrated with technology from Army and DARPA programs.

CECOM has recently released a Broad Agency Announcement (BAA) for MOSAIC. Over seventy white papers have been received on how to accomplish the various technical goals. As the chart shows, the ATD will be conducted in FY04. Transition to the PEO, Tactical InfoSphere can be accomplished during FY05. An EMD decision could be made by FY06 in line with the FCS program.

Assuming MOSAIC successfully meets its objectives, it can provide the nucleus of a first generation of the Tactical InfoSphere.

This chart depicts the roadmap for developing the communications network of the Tactical InfoSphere. It identifies key DARPA programs that can contribute needed technology. The

Airborne Communication Node (ACN) is a collection of high technology communications translation/relay capabilities conceived as a payload for Global Hawk. DARPA has recently decided to eliminate the flight demonstration and will terminate the program following a laboratory demonstration of the technology. Additional funding would allow the Army to fulfill the original DARPA plan by flying the ACN payload in the MOSAIC ATD.

DARPA's Small Unit Operations (SUO) is developing advanced, military "smart-radio" technology that will be integrated into the MOSAIC ATD. Noteworthy technologies expected from SUO are: Ad hoc networking algorithms and software; LPI/LPD waveforms; mobility protocols; user terminals for Dismounted Warriors and co-site interference mitigation. Phase III will be completed in FY02 and could provide radio prototypes.

DARPA's GLOBAL MOBILE (GLOMO) Communications Program will provide key technologies in: network management; routing protocols; Quality of Service (QoS); security-information assurance; survivability (self-healing algorithms and anti-jam); and dynamic channel access and power levels.

Both CECOM's Agile Commander and DARPA's Command Post of the Future are developing new concepts in the exercise of command and control that envision eliminating the "tyranny of the TOC" to permit dispersed staff functions. Concepts and products developed in these programs will be integrated with the communications elements of MOSAIC to demonstrate new, network centric concepts of C2 and Battlespace management.

The MOSAIC program requires new, wideband digital radios to demonstrate sufficient throughput to meet network demands. The Joint Tactical Radio System (JTRS) is an OSD mandated program governing the acquisition of all future DOD radios. The JTRS program has recently awarded a contract to produce JTRS stage 2C radios. Some JTRS radios will be provided to MOSAIC for the ATD. These radios will provide throughput equivalent to NTDR and will also include some built-in networking features. However, it should be noted that it is not a contractual requirement that the JTRS 2C radios be either IP or GIG compliant - a major shortcoming!

The following steps should follow a successful MOSAIC ATD:

- Establish a spiral development plan with update timelines that are in sync with commercial wireless developments;
- Target the introduction of the MOSAIC "beta version of the 1st Generation" Tactical InfoSphere into an operational unit Test Bed prior to the ATD demonstration. This Test Bed will be the basis for the development of tactics, technologies, and procedures (TTPs) for this new capability. The test bed will also provide an experimentation center for the CECOM RDEC and PEO in much the same manner as the 4th ID contributed to the accelerated development of "digitization".

Transition the MOSAIC product and technology to the PEO, Tactical InfoSphere in 2005 as a basis for the EMD program. This program should result in a fully integrated Tactical InfoSphere in which is fully integrated so that every platform "looks" the same to the network.

Communications Technology Scorecard

- **Radio Technologies**

- **Software to provide smart, IP-based networking radios**
- Variable bandwidth (bandwidth based on need)
- **Adaptive use of spectrum**
- Positioning using time-of-arrival or other sensors to augment GPS
- Phased array antenna
- Application Specific Integrated Circuits (ASIC) miniaturization
- Digital signal processing

- **Network Technologies**

- Network management algorithms/smart routing
- **Network security and counter C2**
- **Human machine interfaces (HMI)**
- **Robust, ad hoc, plug-and-play and mobile networks**

Green - Will support 2006 EMD

Yellow - Could support 2010-2015 Integration

Implementation of the Tactical InfoSphere requires the maturation or development of several key technologies. Radios for the Tactical InfoSphere will need to be more “intelligent;” able to join and leave the InfoSphere at will and able to assist in the routing of information. We assessed seven radio technology areas necessary for the InfoSphere.

- 1) Software to provide smart, Internet Protocol (IP)-based networking on the move
- 2) Capability for varying bandwidth
- 3) Adaptive use of spectrum
- 4) Positioning using time-of-arrival or other sensors as alternatives to GPS
- 5) Phased array antennas
- 6) Application Specific Integrated Circuits (ASICs) miniaturization
- 7) Digital signal processing

We assessed two items as yellow (“could support 2010-2015 integration”) and the remainder as green (“will support 2006 EMD”). The two yellow areas were items 1 and 3. We felt that there was sizeable risk associated with the development of smart radio software and in being able to maximize the effective use of spectrum.

We also identified four network technologies necessary for the InfoSphere.

- 1) Network management algorithms and smart routing
- 2) Network security and counter command and control (Counter C2)
- 3) Human machine interface (HMI)

- 4) Robust, ad hoc, plug-and-play, mobile network capability

We assessed item 1 as green and the remainders as yellow. The yellow areas were rated as such due to the additional needs of DOD in these areas. Commercial technology development is likely to provide a lower level of capability than what DOD requires.

Recommendations

- **Integrate Commercial and DARPA/ARMY Technology to Demonstrate the Tactical InfoSphere by 2004**
 - Establish CECOM MOSAIC as the priority pilot program
 - Use a spiral evolutionary process in sync with commercial standards and technology
- **Transition the Tactical InfoSphere to a Test Bed**
- **Army Technology & Program Initiatives**
 - Support and steer the GIG to ensure that Army-developed capabilities are Plug & Play compatible
 - Re-engineer on-going Army C4 programs to meet Objective Force requirements and compatible with the Tactical InfoSphere/GIG
 - Establish a program for man machine interfaces for FCS/FTR
 - Establish an Army-funded program to transition technology from DARPA to Army, e.g., CAN, SUO-SAS and GloMo

Establish CECOM MOSAIC as the priority, pilot program

The Army is fortunate to have established a program focused on engineering and integrating commercial technology leading to a first generation mobile internet. We endorse this effort and urge that the Army take all necessary actions to enhance the probability of success. Accordingly:

Establish the CECOM MOSAIC ATD as a priority program with sufficient resources to mitigate risk areas. Funding profiles should be reviewed to permit multiple contract awards in risk areas and to permit the program to target and achieve all of the exit criteria defined for the program. Assuming successful demonstration of the exit criteria, the Army should plan to transition the technology to the designated PEO.

Use a spiral, evolutionary process in sync with commercial standards and technology

One of the most difficult challenges will be to promptly transition new commercial technology into the Tactical InfoSphere as they become available in the public sector. To avoid such problems, the Tactical InfoSphere should be developed using a spiral, evolutionary process to take maximum advantage of contemporary commercial standards and technologies. In this regard, unreasonably rigid approaches to configuration management as well as unreasonably rigid contractual provisions for deliverables contribute to the “freezing” of antiquated technologies into major systems. The spiral, evolutionary process helps restrain such rigid practices.

Transition The Tactical InfoSphere To Test Bed

The Army learned from the “Digitization experience” that there is no substitute for having a soldier test bed for feeding back for both TRADOC concepts, doctrine and TTP and for the PEO improving design and implementation. This critical program can be accelerated if the Army will identify an operational unit to serve as a test bed for MOSAIC.

Army Technology & Program Initiatives - Review and re-orient JTRS program

OSD has mandated that all future DOD radios be part of the Joint Tactical Radio System (JTRS) family. The study team has reviewed the JTRS program and finds that it is overly conservative in its pace toward meeting its overall program objectives.

The fundamental principals of the JTRS program must be reviewed. Clearly the next generation radios must facilitate full interoperability among US forces and with our allies. Given the rapid change of technology, the Cell Phone for example, it is not at all clear that the JTRS program should dictate ANY of the internals of the next generation radios. The study team has reviewed the Defense Science Board Task Force on Tactical Battlefield Communications Report dated December 1999. We agree, in general, with its findings that “If the networking, bridging, routing, and automated system-management objectives called out in the JTRS Operational Requirements Document (ORD)” are to be realized the program must be reoriented. The development of an IP-based, smart, networking radio is crucial to the employment of the InfoSphere.

Therefore, the Army, as Lead Service for the JTRS program, should immediately initiate a review to insure that the program goals are to provide radios that are compatible with the Tactical InfoSphere and the GIG.

Support and steer the GIG

Under the guidance of the ASD C3I, the DoD has embarked on the development of the Global Information Grid (GIG). The GIG will be a major undertaking requiring the support and cooperation of virtually the entire department. The Services must be key players. OSD and the OJCS have already started on the development of the Joint Operational Architecture. Various Steering and Working Groups have been formed to establish policy, procedures and architecture. The promise of the GIG is so important, that it must not be allowed to fail. Since it is in its embryonic stage, the Army has opportunity to steer the GIG to meet tactical needs. The Army needs to play a lead role with OSD, the OJCS, and the other Services to move toward an early implementation of the GIG supporting the tactical warfighter.

Re-engineer on-going Army C4 acquisitions

Several Army communications programs, notably WIN-T, are in various stages of acquisition. These programs should be reviewed and where necessary re-engineered and / or revised to put them in harmony with the model of the Tactical.

Establish a program focused on man machine interfaces for the FCS/FTR

Bringing the InfoSphere down to the operator level will require a whole new generation of man-machine interface devices. User/operators must be free to “fight the battle” with virtually no time to search for meaningful information and with minimal distraction by the presentation of the

"Situational Display." Development of highly intuitive, simplified man-machine interfaces is an imperative. The ASB recommends that a program be established to develop such devices for the FCS and FTR.

Establish an Army-funded program to transition technology from DARPA

During the course of this study we found several DARPA programs, including SUO-SAS, ACN and GLOMO, which have developed advanced technologies and products that are key to the development of the Tactical InfoSphere. DARPA and the Army have worked closely on each of these programs and there is a desire on both sides to transition them to the service. The limitation is the lack of programmed funds for transition. We recommend that the Army provide the funding to transition these programs and consider establishing a program line for continual technology transition, to include promising commercial technology.

APPENDIX F

RSTA

APPENDIX F

RSTA

Reconnaissance, Surveillance, Targeting & Acquisition (RSTA)

Challenge - "Timely, Sufficient Knowledge" rather than "Perfect, Late Information"

- Blend available sensor data for automated targeting and warning
- Must move to a highly automated precision information solution
- Layered Organic & Joint assets are necessary for Brigade in 2015
- Commercial Remote Sensing provides significant, relevant RSTA circa 2015
- Innovations are required to realize Brigade and below RSTA Needs
- Program Actions are required to meet the RSTA Challenge
- Right Architecture through Simulation & Experiments

Key Recommendations

- Set the Vision: Timely Sufficient Knowledge; Not Perfect Late Information
- Demand a quickly fielded and evolvable architecture
- That architecture shall use a suite of hardware and software to fuse into automated target recognition and cueing
- Develop and Validate through incremental build and test

The challenge of RSTA (Reconnaissance, Surveillance and Target Acquisition) is to provide the knowledge to the Warfighter that will enhance effectiveness and assure survivability. This is captured in slogans such as "shoot before being shot", "avoid surprise" and "overcome the home court advantage". The major elements of the RSTA section are articulated in this chart. These findings lead to a set of recommendations that are outlined here and developed more fully at the end of the RSTA section. These recommendations focus on the vision, architecture, implementation and validation.

Reconnaissance, Surveillance and Target Acquisition (RSTA) has the mission of sensing the world and blending the "collected visions" to form a single view that is reasonably correct, reliable and timely. The knowledge RSTA provides must give the Army a decisive advantage over all potential adversaries by providing superior threat warning, attack assessment, battlefield ordinance awareness, battle damage assessment and targeting. Today many sensors view the theater. Some belong to the Army - others to other services, other nations or commercial enterprises. The views are from space, high flying aircraft, ships, UAVs and the ground. Each sensor, standing alone, has by definition, limitations in perspective. Fusing or blending views that are spatially diverse and perhaps spectrally diverse will - when well done - markedly improve the quality of the knowledge and hence improve decision making. The challenge of RSTA is to blend available information to improve decision quality. But recognize that "perfect knowledge" that is late is of little value and may be no more valuable than having no information. Thus the vision of RSTA must be to create knowledge with a quality sufficient for the mission but with a timeline and reliability that assures decisive victory with minimal casualties.

Today the sensors viewing the theater are stove-piped with mission-specific requirements. Sharing their views with other sensors has not been a priority requirement. This narrow vision of sensor use must

change. With the improvements in communications, signal processing, data compression, etc., all sensor data can be made available to those warfighters who can use it. However, netting and fusing sensor data alone, while necessary for improved decision making, is insufficient for the task of assuring timely, correct decisions for the brigade and below.

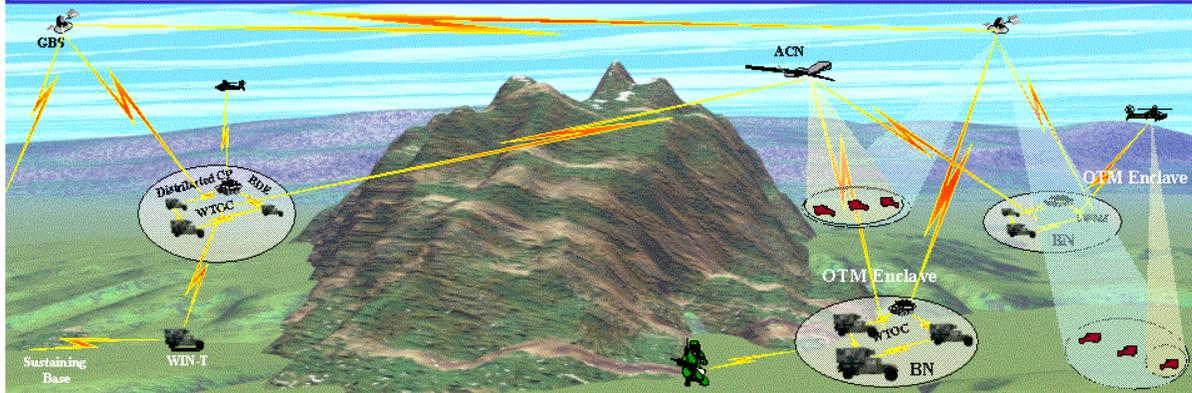
An architecture must be developed to assure that each Warfighter can select and process that information which is necessary to his success and survival. Too much information can be as bad as no information if the selection, fusion and display process has timelines beyond seconds for the tactical troop. Given the stress of battle, the fog of war, the realities of recruitment, and the press of technology toward unmanned systems, knowledge must be augmented with decision aids to allow “best alternative” recommendations and automated targeting and cueing. This future RSTA system should be fielded through an evolutionary process and subjected to active field tests that validate its value and ease of use.

Blend Available Sensor Data for Automated Targeting and Warning

Must Provide Real Time Situational Awareness via Integrated Joint and Organic Solutions

Future Combat System & Brigade Information Needs

- Targeting (Seconds)
 - Survival (Seconds)
 - Battlefield Ordnance Awareness (Seconds)
 - Intel Prep of Battlefield (Hours)
 - Operations beyond LOS
 - Information Interoperability for Knowledge Fusion
- ➔
- Automated Threat Warning & Assessment
 - Automated Targeting
 - Dynamic Tactical InfoSphere
 - Knowledge on Demand



The focus in developing and fielding an integrated and joint RSTA system is to provide automatic sensor processing to enable:

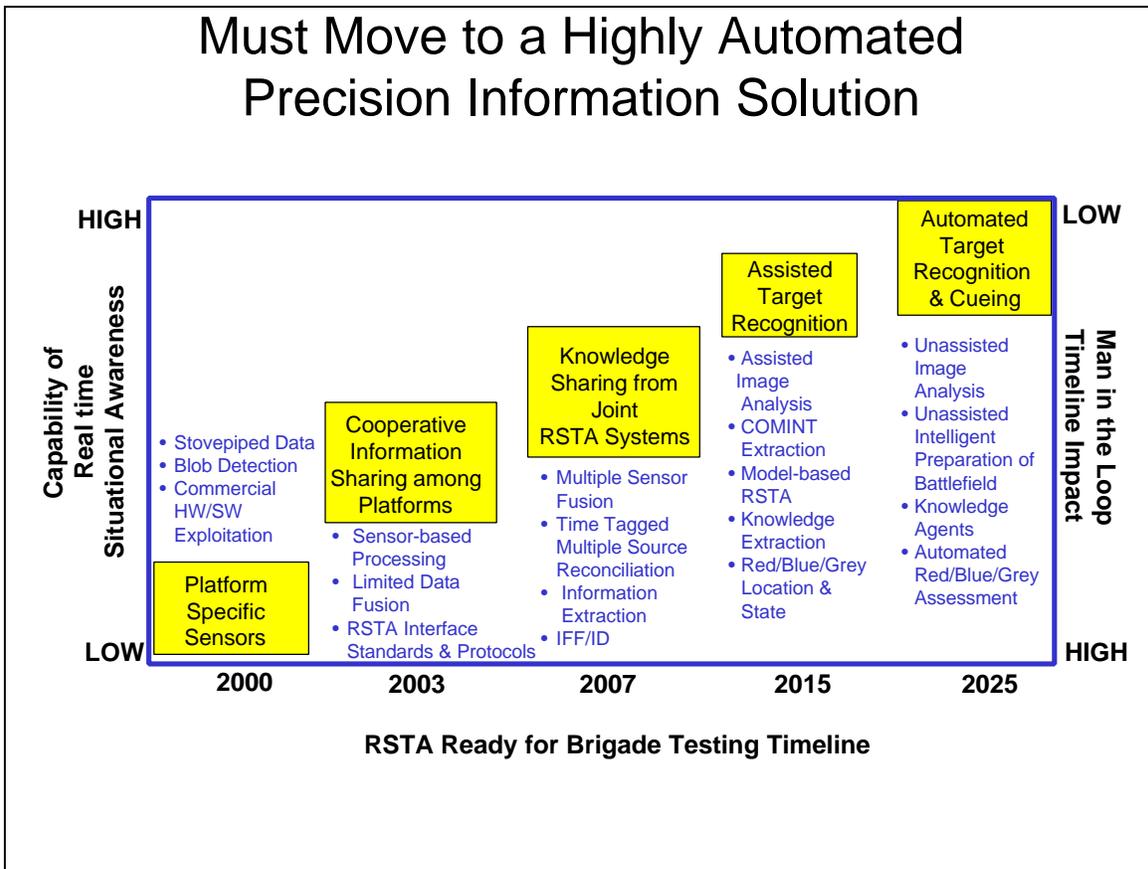
- Automated targeting
- A dynamic tactical InfoSphere
- Knowledge on demand.

The key parameter for the Future Combat System and for the Brigade and below, is actionable information (knowledge) in a timely fashion, with minimum latency.

The most driving areas are targeting and force survival, which demand information in seconds. The intelligence preparation of the battlefield can be accomplished over days with necessary update in minutes, at Brigade and below.

As shown in the architectural picture, data can result from a variety of sensor sources ranging from satellite based to UAV based. Timely situation awareness will derive from all applicable data sources being exploited **automatically**, resulting in actionable knowledge inside the decision timeline. The system structure is horizontally focused, not stove piped, providing the basis for multi-sensor data fusion and exploitation. A key ingredient to successful implementation of an integrated architecture is the rapid development and field testing of emerging innovative communications solutions.

Netted sensor fusion provides the basis for the future automation of battlefield Situational Awareness. It is essential to automatic targeting and real-time intelligence preparation of the battlefield.



The RSTA problem is depicted in this chart. Today's capabilities can be characterized as having little real-time impact, requiring lots of human activity and employing single sensor solutions. The future combat system will require a high level of real-time situational awareness that is obtained essentially automatically from an integrated suite of sensors and software. This necessitates a systematic approach to standards and protocols to enable automatic fusion of the various data inputs. Today's environment for operational software is essentially platform or sensor centric, where the operational software for RSTA 2015 must have time-tagged, relational data which can be deconflicted and fused into a common operating picture for real-time situational analysis. To exploit the emerging commercial imaging products and associated tasking, processing, analysis and exploitation tools, it is essential that DOD standards and protocols be consistent with COTS products.

The objective of the RSTA in the future Objective Force is to provide real-time situation awareness to all force elements. The road map of development leads from current platform specific sensors and the associated stovepipe data to real-time target recognition by 2025. This evolution will provide increased capability towards this objective with a major milestone in 2015 as the program achieves near real-time knowledge extraction through assisted target recognition. The available software will provide the means of minimal man-in-the-loop image analysis and information extraction from the variety of sensor systems available.

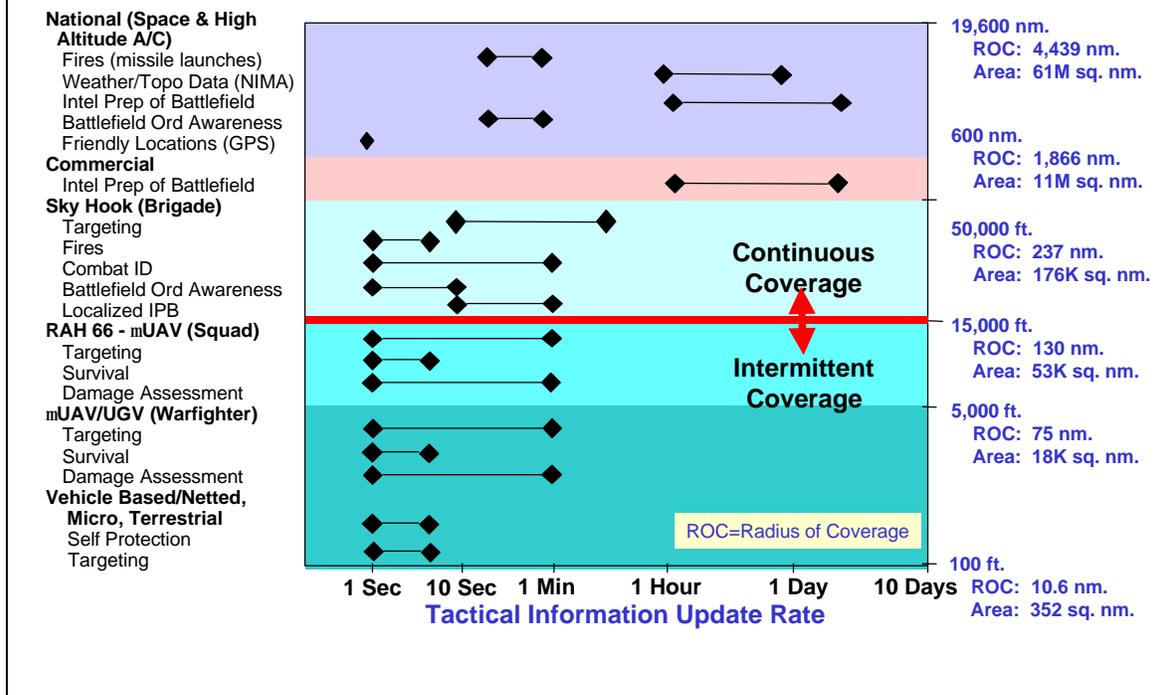
Continued advancement in software development and tools will result in knowledge agents and analytic image evaluation tools that will provide for automated target recognition and cueing by 2025.

This result provides the objective force with assured situation awareness based upon collection from all available automated sensors.

This evolution will result from incorporation of then current COTS software, augmented by focused software and tool development. Sensor technology is more an engineering task, than a development issue. Basic sensor technology is demonstrable with prototype equipment, but the ability to fuse various sensor outputs into an automated real-time situation awareness is in its infancy and will require realistic testbeds to prove out the technologies and procedures.

This approach results in an operational quality RSTA capability by 2015 and evolves in a complete, automated, real-time situation awareness capability for in the field forces by 2025.

Layered Organic & Joint Assets are Necessary for Brigade in 2015



The brigade in 2015 will have available a layered structure of assets to help prepare for and successfully execute the battle. These assets will range from micro- and tactical- UAVs providing as-needed support at the fighting element and squad levels, to Sky Hooks, commercial and National overhead systems providing continuous support at the brigade level and above.

The radius of coverage (ROC) and area of surveillance varies with the altitude of the sensor. For example, a micro-UAV at 100 feet altitude has a ROC of 10.6 nautical miles (nm.) and has a surveillance area of 352 square nautical miles (sq. nm.), a RAH-66 at 1,000 feet has a ROC of 33.5 nm, for a surveillance area of 3,526 sq. nm, and a Sky Hook at 40,000 feet covers a ROC of 211 nm. and an area of 140,663 sq. nm. Satellites offer continuous coverage from an entire theater up to a full global hemisphere and full global coverage with multiple satellites.

Having identified an area of interest from the broader field of view sensors, the Brigade and below Warfighter needs to control and direct specific sensors to receive focused, rapidly updated battlefield information. The use of these “unmanned scouts” provides the fidelity required for tactical “on the move” decision process of the Brigade and below that cannot be extracted from broad coverage assets. This focused coverage provides the field commander with critical organic capability.

Self protection of the vehicle and beyond line of sight engagement will be achieved by a combination of micro-UAV, vehicle borne and netted terrestrial sensors. Again, a single sensor type will not suffice. The platform will need the ability to locate RF emitters, detect others observing them, find hard to locate targets (e.g., hidden in the tree-line), avoid unattended mines/booby-traps, counter fires against them, and detect movements within the area of regard. Achieving this requires coverage of the full spectrum of sensor capabilities.

Commercial Remote Sensing Provides Significant, Relevant RSTA Circa 2015

HARDWARE CAPABILITIES						Software Exploitation & Distribution Capabilities
	Number of Satellites	Resolution	Revisit Time	Tasking/Delivery Cycle Time		
2000	Panchromatic	1	1m	~3 days	14 days	<ul style="list-style-type: none"> • Geospatial Information Systems (GIS) • Simple online exploitation tools • Offline spectral/spatial analysis • Limited internet distribution and tasking capability
	Multispectral	1	4m	~3 days	14 days	
	Hyperspectral	0	N/A	N/A	N/A	
	Radar Images	1	5m	3 days	30 days	
2005	Panchromatic	20	0.5m	<1 Hour	1 day	<ul style="list-style-type: none"> • Geospatial Information Systems (GIS) • Online spatial/spectral analysis tools • Offline complex exploitation tools • Wire connected internet distribution and tasking capability
	Multispectral	14	2m	<1 Hour	1 day	
	Hyperspectral	2	8m	2 days	5 days	
	Radar Images	5	2m	8 hours	5 days	
2010	Panchromatic	30	0.5m	<1 Hour	~1 hour	<ul style="list-style-type: none"> • Geospatial Information Systems (GIS) • Online spatial/spectral analysis tools • Limited Offline complex exploitation tools • Wireless internet-class distribution and tasking capability
	Multispectral	20	1m	<1 Hour	~1 hour	
	Hyperspectral	15	2m	<1 Hour	~1 hour	
	Radar Images	5	<1m	8 hours	~1 day	

Commercial space-based sensing of the earth is now poised to breakout and will ultimately enable it to rival both space-based navigation (GPS) and communications for impact on the economy and the society in general. Also, like navigation and communications, remote sensing has the potential for a significant revolution in military affairs, particularly as regards applications to surface forces, such as the FCS.

At the present time, at least three U.S. corporations and fourteen foreign firms/countries are committed to launching remote-sensing satellites. At the planned rate there will be as many as 30 separate orbiting satellites by the year 2005 (as contrasted to the current 2-5, depending on how you count them). These include high resolution and imaging types - panchromatic, multispectral, hyperspectral, and SAR radar. Each of these classes of sensors has the potential to provide unique and valuable information to the ground force combatant. As the sensors grow in complexity and capability, the need for sophisticated software in the form of processing/exploitation and distribution capabilities will grow even faster.

There is no doubt that the sensors are going to be there, and unless denied by counter measures or other denial actions, their information products will be available to friend or foe alike. The means to automatically process, exploit and distribute time-urgent information to the ground forces are the areas where U.S. technological superiority has the potential to tilt the playing field in our favor (and keep it there). By 2005 the large number of satellites and the wire-based internet tasking and distribution capability with simple on-line spectral and spatial analysis tools will enable daily tasking/delivery (~24 hours) capabilities to monitor the status and actions of opponents in the field. Processed SAR or hyperspectral imagery will require extensive man-in-the-loop and high-powered processing and periods

of the order of days for turn around. For very high value, partially fixed targets, dissemination of this information is probably “time-critical” category with data and detailed knowledge of over-the-horizon force maneuvers that can be provided with simple band-rationing processing and distribution networks.

From 2005 to 2010, the number and capabilities of the satellite sensors will probably not change that dramatically (although the reliability probably will). But the maturation of sophisticated on-line processing tools and global wireless Internet tasking and distribution have the potential to enable a dramatic revolution in the use of space-based sensors. FCS operators will be able to task satellite sensors for information anywhere/anytime with maximum tasking/delivery cycle times no longer than one hour. In the 2010-2015 timeframe, space-based commercial remote sensing should be mature to the point where it can be a critical component of the FCS RSTA architecture and capabilities. S&T investments must be made in the very near future to enable U.S. forces to maintain an unfair advantage in its exploitation and dissemination and that the U.S. has the capability to deny any adversary’s access to this class of data. Commercial interests have already begun to move out in this field and the Army S&T community must stay abreast of these developments and leverage its capabilities for the FCS, as well as other ground forces.

Innovations are required to realize Brigade and below RSTA Needs

Challenge	K	Limitations	Innovations
• Sensor-based Processing		• A Few Dedicated Sensors	• Develop & Test for Bde Sensors
• Data Fusion		• Limited to Easier Specialized Applications	• Develop "Data Fusion Machine"
• Information Extraction		• MTI locations & velocity • Ballistic projectile info • Commercial little used	• Develop, Identify & Validate Algorithms
• Multi-Source Sensor Fusion (SIGINT, MASINT, Acoustic, etc)		• Non-real time/Fragmented research	• Extend "Data Fusion Machine" to all sources
• COMINT Extraction		• "Word" search • Limited Natural Language Processing	• Adapt Technology to Army Specific Needs
• Knowledge Extraction		• Academic Research	• Initiate Aggressive Program at ARL/DARPA/National Labs
• Unassisted Image Analysis		• Limited "Assist" Tools	• Identify & Test Algorithms
• Knowledge Agents		• Academic Research	• Initiate Aggressive Program at ARL /DARPA/National Labs
• Unassisted IPB		• Limited "Assist" Tools	• Identify & Test Algorithms

Key: Technology will Support Timely Sufficient Knowledge Current Advances will support Realizeable with Accelerated Army Funding

To accomplish the goal of real-time Situational Assessment for the Brigade and below, innovative actions must be taken to correct for current limitations. As the architectural concept evolves, performance limitations in the capabilities listed in the first column must be overcome. Dependent upon the current limitations, program actions ranging from development and testing to aggressive research and novel design must be initiated. In every case, significant engineering must be accomplished to achieve a robust, real-time solution.

The key innovations required to meet the RSTA challenge are presented in this Table. These challenges have been evaluated on a color scale which assesses whether current advances in commercial and funded government technology will support the Army 2015 RSTA vision (Green) or if the Army must spend at levels above current planning (Yellow) to achieve the objective. The prime limitations that inhibit the 2015 vision are stated with suggested solutions.

The context of this table is based on RSTA solutions for the brigade and below. To satisfy their needs, the challenge will be to get knowledge to and from:

- Individual soldiers,
- Crew served weapons,
- Munitions,
- Manned and unmanned vehicles,
- Platforms,
- UAVs,
- Aircraft
- Space-born sensors.

Walking through the table with a few examples will aid interpretation. Key sensor outputs must be blended or fused to increase knowledge quality. This sorting, blending, culling, analysis, interpretation and recommendation must be done within a time window that will assure success and survival of the tactical forces.

Today, below-the-brigade sensors are carried by individual soldiers, weapon crews, and platforms. These are dedicated to a specific purpose (e.g. give vision to the Bradley or assist aiming of a weapon) and they are not configured to share information with other sensors. While the Tactical InfoSphere is addressing the problem of getting sensor data from one sensor to another, RSTA must solve the following issues:

- What is the minimum set of information that must be transferred to assure the correctness of the transmission and allow fusion;
- Does one monitor and grade the quality of each sensor's output;
- How do you blend or fuse views with different aspects, quality, geographic and temporal diversity, etc., to obtain a single "best view of reality"; and
- How do you do this in a timeframe to allow the decision-maker or Warfighter to win decisively with minimal casualties?

These are an extremely difficult problems that cannot be solved solely in engineering laboratories or centers of thought. Inventory and developmental sensors must be tested netted in a variety of field conditions and accurate sensor data collected. Then theoretical and heuristic signal processing and fusion techniques can be developed to produce solutions that are highly useful.

Non-real time data fusion takes place today, but not at echelons brigade and below. Data from USAF and National Space assets are being blended or fused, but these situations are somewhat easier to solve than the tactical problem. They are simpler because of established static infrastructure. The Army can take advantage of fusion work in the other services and the commercial world, but it must recognize that Army-specific targets and timelines will require Army-specific initiatives.

Program Actions Required to Meet the RSTA Challenge

Programs	Recommend	Recommended Actions
1) ASAS		1) Refocused to Support future Army
2) Vehicle Based Sensors		2) Refocus to support FCS
3) Micro, Expendable, Terrestrial		3) Exploit technology development in system solution
4) DARPA ATR		4) Join with DARPA a la FCS
5) Intel COMINT Auto Processing		5) Track & Exploit
6) NIMA Common Operating Picture		6) Track & Exploit
7) ASPO TENCAP		7) Develop products for future force and integrate
8) Discoverer II		8) Survivable, robust GMTI by 2015
9) Eagle Vision II		9) Exploit Commercial for Tactical InfoSphere Needs
10) AF RSTA A/C		10) Task ASPO to integrate into TENCAP solutions
11) Army RSTA A/C		11) Task PEO C4ISR to integrate into TENCAP solutions
12) Brigade & below Sensors		12) Initiate new program for miniaturized sensor for TUAUVs
13) Automated IPB		13) Initiate new program
14) Automatic Fusion		14) Initiate new program in collaboration with NIMA, NSA & CMO
15) Knowledge Extraction		15) Initiate new program
16) Model-based RSTA		16) Initiate new program

Key: Accelerate & Add'l Funding (blue), Army Influence (purple), New Program (green), Redirect Program (yellow), Terminate Reallocate Funds (red)

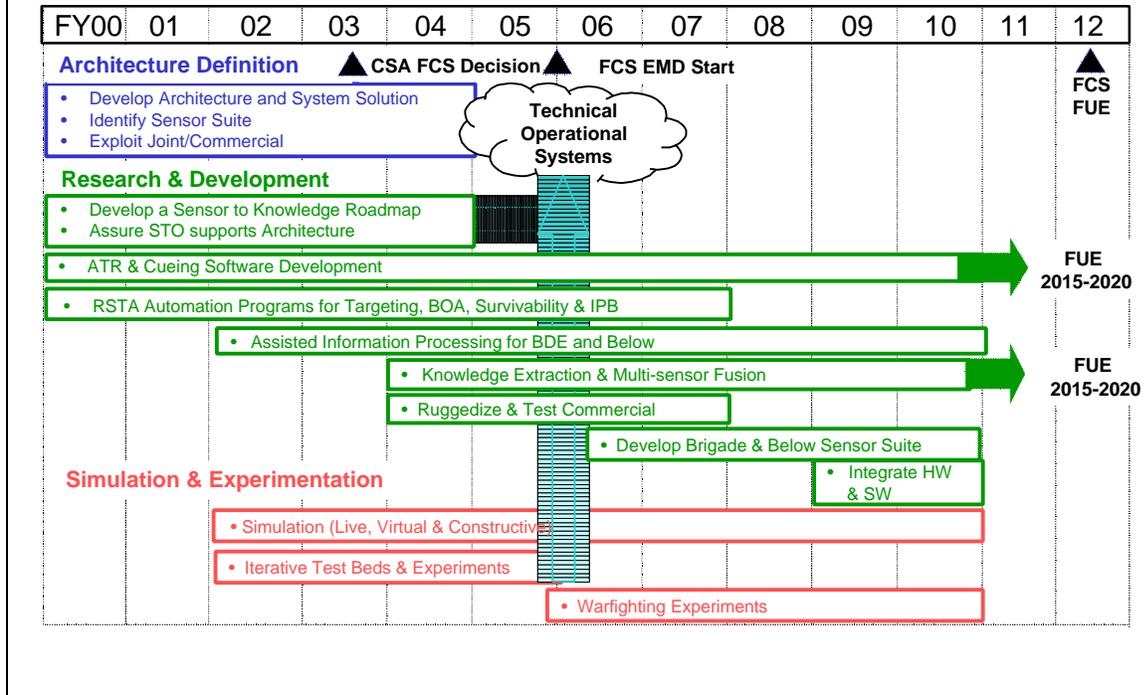
As discussed in the previous paragraphs, a number of innovations/programs are required to meet the RSTA 2015 challenges. This chart indicates some of the changes to existing programs and suggestions for new initiatives that will be required to achieve the RSTA goal. Although the study also involved reviewing current programs that could be terminated to free up funding for reallocation, no redundant or obsolete programs have been identified. Whereas these suggestions are appropriate in general, the detailed research and development program will have to be configured based on the RSTA architecture and overall system concept. Over the course of the development of the Tactical InfoSphere, all existing and proposed programs should be challenged to demonstrate their contribution to the tactical warfighter.

Some programs currently exist that will facilitate attainment of the RSTA 2015 challenge. These programs have been examined, evaluated, and recommendations made in the following categories:

- Accelerate and apply additional funding;
- Apply Army influence; these programs are in process and the Army needs to “catch the wave” and suggest requirements, interface definitions, message management, etc., that will assure the timeliness and usefulness to the brigade and below RSTA challenge;
- Redirect the program; the program objectives were formulated in a older world and are not consistent or optimal for the envisioned tactical InfoSphere; and
- Terminate and reallocate the funds.

In addition to evaluating current programs, recommendations are also made for new initiatives or programs needed to get timely, adequate RSTA information to the brigade and below. These initiatives are linked to the previously identified list of required innovations.

Right Architecture through Simulation & Experiments



A technology roadmap is suggested to frame the future. Three distinct parallel activities are envisioned:

- System Definition and evolution
- Research and Development
- Testing

This framework is consistent with the vision: “Timely Sufficient Knowledge - not “Perfect Late Information” and the precept that a rapid, iterative build/test program plan based on an evolvable architecture is the sound go-forward strategy.

A RSTA Systems Engineer should reside in the Systems Engineering Office charged with defining the Tactical InfoSphere Architecture, its sub-elements and the integrated engineering, development, test and implementation plans. The RSTA solution should draw heavily on ongoing USAF, USN, NRO, Army, Joint and Commercial sensor activities. Blending these sensors and new initiatives to assure timely - mission sufficient knowledge will be the challenge.

Given the complexity of the Army mission, the sensor suite must perform in all weather, day/night, and in all terrain, against complex targets masked with camouflage and protected with active and passive countermeasures. Consequently, Army unique, in theater (organic) sensors will be needed and must join the architecture. This would be particularly true for extremely challenging tasks like mine detection, foliage penetration and automated targeting of masked, camouflaged, and counter-measured protected targets.

RSTA research and development efforts should begin immediately to support the ultimate objective of automated targeting, warning and threat assessment. The key word is **“automated.”** In this domain, the knowledge from the sensors is sorted, prioritized, weighted and blended to provide a “best view of reality.” Given this estimate of the situation, decision aids (e.g., neural networks, expert systems, heuristic rules, game theory, genetic algorithms, fuzzy logic, Bayesian decision-making) are applied to posit solutions that may direct automated machines or support human decision making.

Since most of the sensors necessary to support the tactical already exist, at least in prototype form, hardware and software are needed to process the sensor to achieve the RSTA imperatives. Hardware and software that provide automated targeting, automated threat assessment, automated threat warning, battlefield ordinance awareness, battle damage assessment, passive and active defense must be developed to take full advantage of organic, joint and commercial sensors. Routing and fusing the sensor inputs, assuring the timeliness and appropriateness of knowledge at each level of the Brigade and doing it in configurations useful to the soldier will require extensive development.

To assure suitability for the soldier, emerging solutions should be fielded quickly and evaluated by the people that will use them. The soldier will quickly deduce what is of value and what needs to be improved or discarded. This "test-improve-test" work can yield an operational RSTA framework within affordability constraints.

Key Recommendations

- Set the Vision - “Timely, Sufficient Knowledge” - not “Perfect, Late Information”.
- Demand architecture that can be fielded quickly and facilitates timely, cost effective updates.
 - Commercial GIS, image and special processing with standards and protocols
 - “Plug and Play” use of National, commercial and Joint hardware and software
- Establish a process that provides a systems solution to RSTA that drives from platform-specific sensors to a confederation of hardware and software supporting automated target recognition and cueing.
- Validate RSTA progress through a program of “build a little and field test it.”

Basic Truths of RSTA

RSTA needs to cut across stovepipes (horizontal rather than vertical integration).

User specific knowledge is customized from common information set.

Sensor technology can support acquisition of essentially anything measurable.

Perfect information for the Warfighter is not essential, but timely information is.

We have seen there is a path for success, but the path is sufficiently new and so steep that we need to start now. The Army must set the vision, establish an initial architecture and implement the program. In the process of this study we have identified some basic principles which if applied to the decision process will help assure a proper outcome.

The bottom line -

Timely Information is Essential and Achievable!

APPENDIX G

UAVS

APPENDIX G

Unmanned Aerial Vehicles

UAV Platforms

Objective: Provide the platforms to support continuous sensor coverage and multiple radio relays over the Tactical AO

- Organic UAVs operating at low, medium, and high altitudes under the direct control of tactical commanders
- COTS will provide the high altitude platforms and components for high and medium altitude
- Army should focus S&T for UAVs on cost reduction, self-protection, autonomous operation, and MEMS sensors and actuators
- Without strong proponency, these technologies will not be ready for the FCS

ORGANIC UAVS ARE CRITICAL FOR THE TACTICAL INFOSPHERE

The dynamics and high mobility of the FCS battlefield led to a requirement for rapid, responsive, and organic sensing and communications capability. Such a capability can only be provided by airborne platforms under the direct control of the commander. A multi-tiered family of unmanned airborne vehicles (UAVs) is therefore a critical enabling technology that must be considered for the objective force. This family, and the suites of individual UAV types within each of categories, is required to be organic to the commander at the Brigade level (Bde) and below.

The concept of tactical InfoSphere implies that information flows unconstrained by echelon-hierarchy or asset ownership. This means that information flows laterally, up, down, etc. based on needs. The dynamics of the Objective Force battle space imply that no fixed information lines will work in all conditions, and as a consequence, reconfigurable communication systems will rely on a multi-tiered family of UAVs.

A great deal of information will be produced and consumed by organic sensors and assets that are closest to and controlled by the warfighters and local commanders. This information may be merged with information from other assets in the GIG, including national and theater assets. Further, this localization implies that the InfoSphere "surrounds" and moves with the forces as they move, again requiring special UAV systems configured as communication nodes.

Distributed fusion and information processing - conversion of sensor data into usable information - with several levels of detail - takes place as close to the sources as possible. UAVs configured for sensing and processing will be a major source of such information. This minimizes the latencies of the information flow and results in rapid decision making well within the

Opponent's Observe, Orient, Decide Act (OODA) decision loop. This results in a see-first, decide-first, shoot-first paradigm.

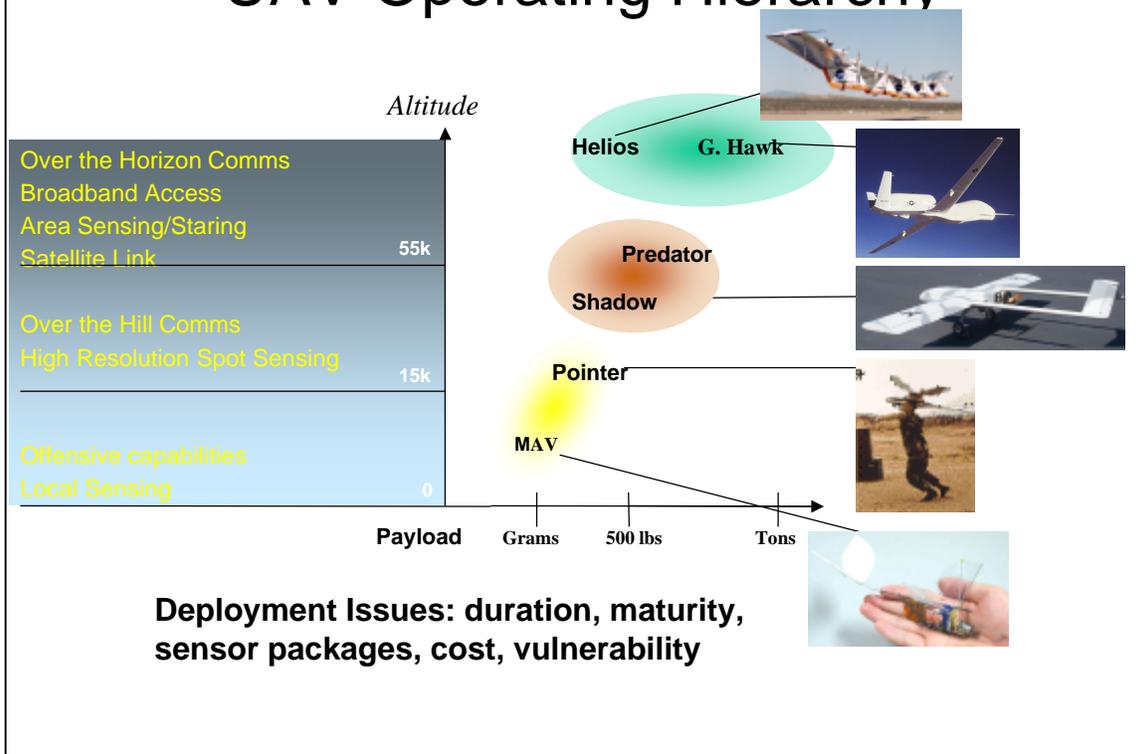
Every node on the battlefield is becoming a sensor, router, generator, and consumer of information in a seamless, globally interconnected fashion, in which UAVs will play an increasingly important role. With all nodes participating actively and passively, and organic UAVs serving as both sensor systems and communications nodes, integration of protocols across all platforms and functions will be critical to success.

The ISR community's vision for information acquisition, processing, and dissemination relies on a seamless flow of information that is consistent with the requirements of other communities, as stated above.

There are other factors that the Army needs to address to make multi-tier UAVs operational. The need for miniaturized ISR payloads is paramount to allow fielding significant capability on these small platforms. The survivability of these UAVs is also a critical issue to maintain reliable C4ISR for real-time continuous operation for the Brigade commander. Other technology challenges are the ability to provide long endurance, at long range, under low power, and at affordable costs. Many of the technologies will be leveraged from commercial developments. The Army needs to accelerate its procurement cycles to be able to exploit the commercial production cycle.

The panel observes that the main impediment to the adoption of UAVs in the Army has been the lack of a focused community advocating the design and adoption of such platforms. Currently, advocacy for UAVs, especially tactical UAVs comes from the intelligence community. As the Army transitions to the objective force, the multifunctional capability of UAVs must be recognized (including the communications and the offensive operations aspects) to enable an effective family of UAVs to be fielded. The Army does not presently have a program executive office responsible for integrating across functions to field a multi-tier set of UAVs effectively. Each type of UAV must be integrated into the appropriate unit's tactics and be compatible with an associated weapons system (e.g., as an Apache scout). It is crucial that the Army establish an overarching office to see the development, integration, testing, and fielding of a multi-tier suite of UAVs in support of the tactical InfoSphere.

UAV Operating Hierarchy



For organizational simplicity, UAVs are categorized within three zones; high flyers capable of operating autonomously at 55,000 ft or beyond; medium altitude, typically considered tactical UAVs, operating in the 5,000 -20,000 ft altitudes; and low flyers in the 0 to 5,000 ft region, with emphasis on a few hundred feet or less.

Examples of high flyers are the USAF Global Hawk and the HELIOS electric powered platform. The high flyers will have the capability to support multiple functions within the context of C4ISR. Examples of this organic battlefield support are over- the-horizon communication for larger combat units, broadband access, area sensing and staring, and satellite link. The high flyer UAVs will provide information to multiple units in the battlefield, and probably will evolve as “joint tactical” assets. Additional platforms may be deployed to support the JTF infrastructure.

The next tier of UAVs operate at medium altitudes. The USAF Predator is an example of this tier UAV. Another example under development by DARPA is the long endurance Hummingbird A-160. The Hummingbird has as its goal to achieve a range of 4,800 Km, with on station endurance in excess of 40 hrs. Medium altitude flyers will provide over the horizon sensing, but will also be able to focus the field of regard much more precisely on valuable targets than a high flyer UAV. These will also play a major role as a communications nodes for brigade to platoon communications.

Finally, the 3rd tier of UAVs are the “low flyers” (e.g., Micro Air Vehicles (MAVs)). These include platforms operating below 5,000 ft, and they would be maintained and launched at the company and scout platoon levels. The troops can afford to lose several of them in battle due to their low cost, expendable design. Most of this category’s development effort is under the auspices

of DARPA. They will be available for both defensive and offensive tactics. In a defensive mode, the low flyers will focus reconnaissance and surveillance over a much smaller region than either the medium or high flyers, with a much lower latency. In an offensive mode, the low flyers can carry small munitions, serve to “jam” enemy electronics, or serve as a sacrificial beacon for smart munitions.

UAV Families: Advantages

High

- Long time on station
- Low Bde/Bn burden. Most support can be from stations out of theater
- Large footprint of support vehicles (ground stations) in theater
- High altitude provides capability for over the clouds relay
- Multi-function utility (EO/IR, SAR/GMTI, Sigint, Elint)
- Staring sensors

Medium

- Flexible tactical control
- Medium Bde/Bn burden
- Medium footprint/medium quality images
- Reduction in Bde/Bn communications overhead
- Beyond line of sight communications and sensing

Low

- Inexpensive
 - Low vulnerability
 - Cheap enough to allow cost-effective swarming
- Small unit control (company down to individual platform)
- Offensive and flexible operation

Each class of UAVs has special advantages that will continue to evolve over the next decade. The high flyer is specially designed for high altitude loitering with a wide field of view (> 60,000 ft. and 10,000 km² areas), long loiter times (24 hours to a week or more), reasonable payloads (up to 2000 lbs. and 10kW), and is difficult to destroy. Furthermore, they can be launched and serviced outside of theater, reducing the logistics burdens on in-theater forces. These systems provide satellite-like communications links as well as platforms for sophisticated staring sensors. Operating mostly in friendly airspace, they are difficult to destroy because of their altitude, their low visual and standard radar cross-sections, and their ability to deploy counter-measures against missiles.

The mid-altitude class of UAVs (up to 15,000 ft) comes in a variety of configurations. Three examples are Predator, Hunter, and Shadow. Capabilities include payloads of 50 to 500 lbs., auxiliary power up to 1 kW, and loiter times of 12 to 24 hours, and performance of a wide variety of passive (e.g., communications relays, reconnaissance, ELINT) to active military missions (e.g., target designation, decoys, special munitions delivery, etc.). They can be controlled from battalion, division or brigade organizations, as well as out-of-theater locations, to reduce in-theater logistics burden. As the situation requires, their communications links, and control, can be transferred to in-theater users. These systems are particularly important, and are a significant part of the solution to the beyond line-of-sight communications problems of the tactical InfoSphere. These systems will profit from expected technical advances in commercial wireless technology (e.g., low cost & low power routers, transmitter/receivers, software), in semiconductor processor and memory improvements (>1000x in 15 years) for increasingly autonomous control, simplified

ground control systems, and increasingly compact, low power payloads (e.g., SARs, ELINT systems).

The low-flyers are a new class of miniature air platforms, ranging in size from 6 inches to wingspans of a few-feet, and weighing from a few ounces to a few pounds. Six inch wingspan flyers with semi-autonomous control, endurance times of 20 minutes and CCD imaging sensors have been demonstrated by several groups under the names of black-widow, MAVs, etc. They are usually electrically powered, use ultra-lightweight control systems, and carry lightweight, real-time, visible, and near IR EO viewing sensors (e.g., < 10 g). Their main advantages are that several of them can be carried in one backpack, and they provide instant information to the company-level user. They will take advantage of expected improvements in battery replacement technology (e.g., > 100x power/weight improvements) and miniaturized sensors, processors, and communication links. It is expected that their costs will drop to below \$1000 each. When procured in large quantities, these are expected to play an increasing role in company tactics as their roles in reconnaissance, target designation, decoy generation, and in self-organizing "swarming" missions become understood.

UAV Families: Limitations

High	<ul style="list-style-type: none"> • Cost • Sensor resolution • Support/burden • Sanctuary/airstrips • Relay capacity • Ownership & control 	<ul style="list-style-type: none"> • Currently very high • Low resolution due to high altitude • Requires large runways but can be out of AOR • Infrastructure needed for launching • Limited number of channels • Not under brigade commander's control
Medium	<ul style="list-style-type: none"> • Airspace deconfliction • SAM/AAA vulnerability • Cost • Affected by weather 	<ul style="list-style-type: none"> • 5000-15000 ft airspace is congested • Within range of cheap weapons • Not enough volume yet to reduce costs • Platforms and sensors
Low	<ul style="list-style-type: none"> • Limited endurance, coverage • Autonomous control • Payload/power • Platform stability • Severe weather effects 	<ul style="list-style-type: none"> • Smaller field of regard • Necessary to avoid obstacles • Battery technology is the limiting factor • Small size leads to instability • In the turbulent zone

The technical limitations of each family of UAVs varies greatly and are associated with size, complexity, cost, and the primary beneficiary of the information. The high flyer units are large and expensive, have large logistical footprints, require several vans of control electronics, sensor direction and data acquisition electronics, maintenance equipment, and use a substantial amount of fuel. The control of the sensor data stream from these systems is often hindered by stove-piping, security concerns, and by the need to process immense amounts of data. These delays can take hours to days before data updates to the front lines occur. Because of their operating altitudes, the sensors have reduced resolution compared to those on lower flying platforms, and they are beyond the range of wireless communicators planned for use by platoon personal.

The mid altitude systems presently are expensive and have a large base-operations footprint requiring on-ground full time pilots, systems operators, and maintenance personnel (e.g., Predator and Hunter; Shadow can be operated from two HMMWVs and trailer). These devices operate at sufficiently low altitudes that they are in the way of manned aircraft and can be shot down by an adversary. For example, a large number of Predators were lost in Serbia/Kosovo. In addition, the platform stability and control are hindered by bad weather. These systems are presently expensive and impose a high logistics burden at the battalion and brigade level. Present issues on ownership and control of these systems are not consistent with their crucial role in the tactical InfoSphere of the FCS.

The support burden associated with both high and medium altitude platforms could be ameliorated by basing them outside the combat zone. Long duration UAVs could be staged from

sanctuary locations, flown to the tactical area and turned over to the Bn or Bde command for the duration of the mission. This "service" could support both communications relay and sensor missions with very small impact on the tactical warfighters.

Low flying systems suffer from very small payloads (e.g., 10 grams), low auxiliary power (e.g., < 0.5 W), short endurance times (e.g., 20 minutes), and platform stability. They fly low which takes them within range of hand-held guns (e.g., shotguns). They require substantial development over the next decade to become robust and useful.

Commercial Development & Military Needs ~2015

		Platforms	Payloads
High >50K ft.	Process for Rapid Commercial Technology Acquisition Needed	Commercial	< Communication Nodes < Comm < Sensor for Visual and IR < (CONOPS, fires, floods, urban)
		Military	< Stealth < Self protection < Sensor (SAR/MTI Ultra hyperspectral) < Miniaturization for multi-functions sensing (MMS)
Medium >5K-15K ft.		Commercial	< Component technology (engines, actuators, materials) < Sensor for visual & IR < Lange comm infrastructure
		Military	< Self protection < Stealth < Packing for mobility < Platform adaptation of commercial technology < Light SAR/MTI < MMS < Adaptation of Comm commercial technology
Low 0-5K ft. Battery Substitute		Commercial	< MEMS actuators < Batteries (PDA, cellular) < MEMS sensors
		Military	< Engines < Batteries (MIT, ISI, Turginli, Swiss roll) < Navigation control < Fuel cells (amoborine) < Stability control < BloS Tasking < Mid and Far IR < Attack capability < MMS

The technologies needed by 2015 to overcome the limitations identified in the previous chart will need to leverage commercial UAV developments. The commercial communications industry is investing in field high flyer UAVs that will provide relays for the telecommunications industry, especially in urban areas. There is also a lot of interest in utilizing high flying UAVs for terrain mapping, tracking of fires, and flood sensing.

Several U.S. and European companies are fielding UAVs in the medium altitude class to facilitate farming fumigation. We also believe many of the commercial components (e.g., engines, MEMS technology, actuators, and avionics materials) developed for the high flyer UAVs can be adapted to medium altitude UAVs.

However, the military adaptation of these commercial technologies is necessary to provide self-protection techniques to minimize vulnerability to enemy attack and to increase the UAV's survivability. The Army will rely on continuous real-time operation of these platforms. UAV survivability is crucial to assure that the tactical commander is not limited by a single point system failure.

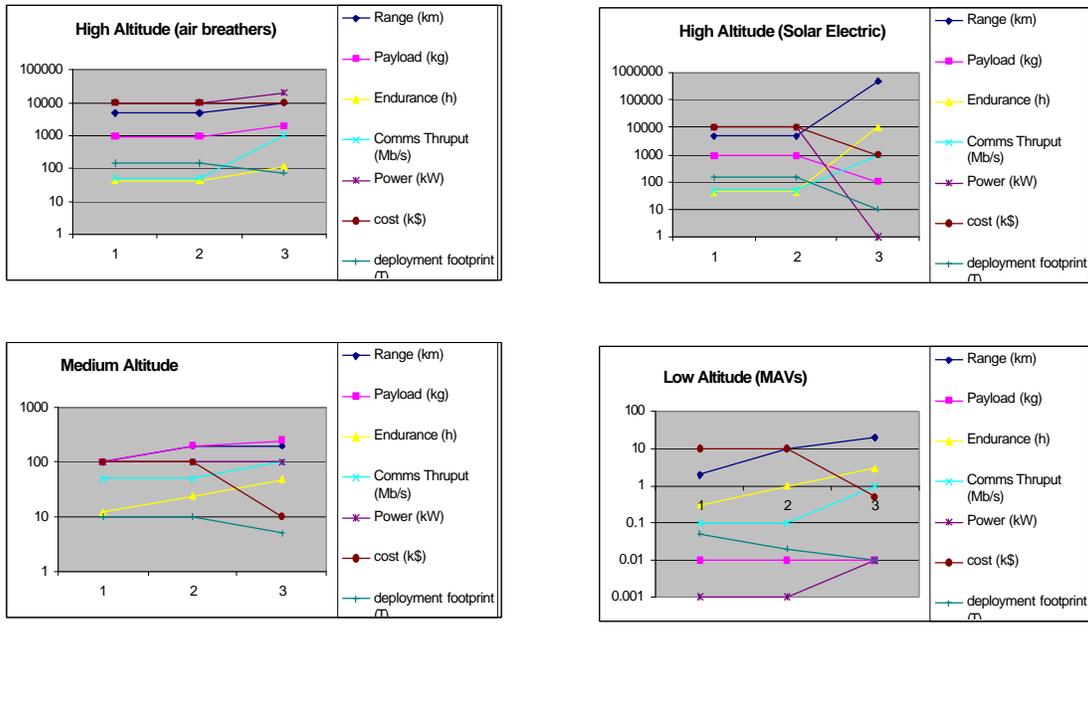
From the perspective of ISR sensors, the commercial industry is also depending on synthetic aperture radar (SAR) capabilities. However, other functions such as moving target indication (MTI), intelligence communications (SIGINT and ELINT), and offensive tactical utility are unique to the military systems. Therefore, the Army must invest in ruggedized packaging of

miniature sensor payloads and in the development of unique sensors to support tactical use of the UAVs. The military UAVs also must maintain secure communication links.

The development of most, if not all, micro-UAVs is presently undertaken by DARPA. These systems still need significant further investment in miniaturized engines, substitutes for batteries, ultra-miniaturized payloads, and autonomous navigation and aerodynamic control.

The Army can leverage commercial technology. However, there is a need to establish the overarching executive office to see the effective inclusion of commercial technology. The proper balance, between adoption of commercial technology and the development of military unique platforms and payloads requirements, is paramount to maintain the development and production of UAVs for an affordable tactical InfoSphere.

Solution Sets and Examples: UAV Evolution



Between now and 2015 UAVs will progress dramatically. These are associated with increases in performance of semiconductor processors and memory, miniaturized and low cost sensors, wireless communications technology, electrical technology (e.g., batteries, battery replacements, power management, motors), higher capacity communications channels, autonomous control algorithms, and ultra-light structural equipment.

Relatively conventional, high flying UAV systems are maturing as they are being supported by both commercial interests (e.g., pseudo-SATs) and military interests (e.g., Global Hawk). They will profit from a 10x increase in communications capacity as higher frequency systems become commercially available. New directions in this arena are ultra-light, high flying electrically powered aircraft, that can eventually be solar powered and have unlimited endurance. They will have, however, a relatively low payload, that must be traded off against FCS needs.

Medium level flyers must be developed to serve as non-line-of-sight communications nodes. As manufacturing, survivability and logistics improvements are implemented, these systems will become more affordable, thus making them battalion compatible. Their communications links to the tactical Internet will reduce the information latency to the front troops. In addition, they can be more expendable as their costs drop and their numbers increase.

Low flyers will improve dramatically as battery replacements increase the endurance by 10x or more, for several hours of flight time. They will increase their payload to a fraction of a pound, thus enabling them to be used in a more active, "offensive mode." These devices will become

mostly autonomous and they will be able to communicate with each other. These low flyers will be capable of automatically returning to the user for reuse. Costs can be reduced to below \$1k each. The development of this class of UAV must be supported vigorously by the Army and DARPA over the next decade.

The panel also observed that current warfighting experimentation does not include UAVs. We believe strongly that not only should our troops experiment with such technologies as they mature; we also believe that OPFORs at the NTC should be provided with UAVs (and indeed, other unmanned platforms) to use against our troops. UAVs driven by commercial trends will proliferate in the hands of our adversaries. Unless we learn how to deal with the threat in realistic environments, the Army will not be ready to face them in the field.

Blue UAV Protect and Survive

Different protect strategies for different classes of UAVs

H • Expensive, large - traditional high alt. survivability techniques
• Signature Mgmt., RWR& Missile Warning, Radar & IR Jammers, Chaff, Flares, Towed decoy, Active Protection, LPI / Anti-jam datalinks, SEAD is critical.

M • Costly, medium size - operates in a difficult survival regime : limited survival payload weight, to expensive to accept significant losses, but in an altitude region hard to defend.
• Signature mgmt., RWR & Missile Warning, Chaff, Flares, LPI / Anti-jam datalinks, tactics, SEAD is critical, (??Radar & IR Jammers, Towed decoy, Active Protection ?? Subject to weight, cost, payload trades)

L • Inexpensive, small - Expendable
• Signature mgmt. (IR, Radar, Acoustic, Visible), LPI- / Anti-jam datalinks, tactics, expect losses and replace

A wide variety of aircraft survival technology and tactics are available to support UAV operations. With the exception of micro UAVs, the foundation is an effective SEAD (suppression of enemy air defense) effort (even though micro UAVs do not benefit from SEAD). Technologies applicable to all classes of UAVs are signature management and secure datalinks. Tactics are important for medium and low classes of UAVs, but must be tailored to the application. APS (active protection systems) may have potential for end game defense of more capable UAVs.

High flying UAVs are complex, expensive aircraft that can benefit from the full range of aircraft survival technique. These include:

- Signature Management, RWR& Missile Warning, Radar & IR Jammers, Chaff, Flares, Towed decoy, Active Protection, LPI / Anti-jam datalinks
- SEAD
- US technology for manned aircraft survival

Low altitude UAVs operating under 5Kft. are assumed to be quite expendable and very difficult to detect, track and target with “conventional” anti-air systems. These systems will benefit from measures to decrease their probability of detection. Key technologies include areas such as Signature management techniques in the IR, Radar, Visible and Acoustic, as well as command and datalink protection. Employment tactics will enhance survivability. Losses and replacements must be planned for in this class of UAVs.

The most difficult member of the UAV family to protect are the medium altitude UAVs. These aircraft operate in the most difficult altitude regime (5Kft - 30Kft), are of significant size, have RF signatures and dwell for long periods over hostile forces. This UAV class must deal with the full range of enemy air defense threats and may be accessible to future threats such as homing lethal UAVs (Kamikaze UAV). The full range of aircraft survivability techniques are applicable to this platform, however the available payload weight will probably limit the techniques to only a subset. This platform must rely upon a high quality SEAD (suppression of enemy air defense) effort as a basis for any operation over enemy forces.

Recommendations

- **Develop and field an interoperable family of UAVs that spans the high, medium, and low operating ranges.**
 - High: adopt commercial solutions
 - Medium: develop and field a Bn/Brigade mission scout UAV
 - Low: develop and field micro air vehicles (MAVs)
- **Initiate programs for UAV survivability, self protection, and cost reduction**
 - Survivability and self-protect strategies vary with cost and altitude
- **Fix the proponency for UAVs in a manner that recognizes the critical need for UAVs and the multiple functions that UAVs provide to the Tactical InfoSphere**
- **Support/continue DARPA's MEMS, MAV, and ACN research**
 - The Army must support MAV development
 - Navigation electronics
 - Miniaturized ISR sensor payloads
 - Flight control electronics and actuators
 - Battery replacement/augmentation

The panel has two primary recommendations in the area of UAVs.

First, the Army should initiate a program to develop, procure, experiment with and test a family of UAVs. The exact nature of this family will change as the technology matures. At a minimum, the Army should consider micro or miniature air vehicles that could directly support individual platforms or small units, and medium (tactical) UAVs that could support commanders below the Brigade. These UAVs and their payloads should seamlessly couple into the Tactical InfoSphere, and should be interoperable (e.g. common control mechanisms, common information sharing mechanisms) within the UAV family as well as with other key assets (e.g., UGVs). The design space should include a seamless integration with high-flying assets that may be maintained at echelons above the Brigade, but could be virtually attached to the Brigade.

Second, to make this family of UAVs a reality, the Army should establish proponency for UAVs in support of operators. The perspective of the Intelligence community, the current proponent, is too narrow. Other interests must be accommodated and a mechanism found to integrate across the various stake holders. At a minimum, the maneuver, communications and the weapons communities should be represented. Integration of these views should be enforced by a single TRADOC systems integrator.

In addition the panel finds:

Particular research elements that the Army should continue to support are those that are unlikely to emerge from commercial efforts (as identified on the previous chart). DARPA research in MEMS, MAVs, and in the Airborne Communication Node (ACN) are important to enable the proposed Tactical InfoSphere. The robotics efforts at DARPA and research offices in the Army complement the ground support infrastructure that strengthens the utility of UAVs. Ground robots and UAVs need to be part of a single Tactical InfoSphere architecture. These programs should focus their technology demonstrations on advances in navigation and positioning, autonomous control, ultra-miniaturization of sensor and comms payloads, engines, and actuators.

The Army should plan a series of integrated tests to validate the utility of a family of UAVs and their payloads. These tests must also incorporate the demonstration of survivability and a measure of enemy vulnerability. The effective use of UAVs for C4ISR in a Tactical InfoSphere must operate real-time during all weather conditions. Weather can limit low and medium altitude UAVs. Therefore, the system tests must incorporate a measure of the UAVs susceptibility to adverse weather.

The Army must establish an organization to implement the use of UAVs for the Tactical InfoSphere. This organization must be cognizant of other services' UAV investments, incorporate commercial technologies effectively, and have broad oversight of the proposed family of UAVs. This Army establishment must also be responsible for integration, testing, and fielding of the requisite UAV technologies working closely with DARPA.

APPENDIX H
POS/NAV/TIME

APPENDIX H

Position, Navigation and Time

Pos / Nav / Time

- **Precision Pos/Nav/Time is important for the Army because**
 - It is the enabler for precise targeting, coordinated maneuver, and secure communications
 - The Army owns 86% of the DoD user equipment requirement for GPS -- the linch-pin for Pos/Nav/Time
- **However, GPS is deficient in:**
 - Robustness (e.g., vulnerability to enemy jamming, exploitation)
 - Performance (e.g., limited coverage in complex terrain)
 - System integrity (e.g., “fragile” constellation with higher powered satellites due to achieve Full Operational Capability (FOC) in 2017)

... and the DoD no longer has management control of GPS
- **Potential actions to ameliorate the deficiencies of GPS include**
 - Upgrading GPS user receivers, antennas
 - Augmenting the GPS constellation with pseudolites
 - Degrading Red's capability to exploit GPS
 - Implementing complementary navigation systems (e.g., MEMS inertials/JTRS TOA)
- **Consequently,**
 - Accelerate and expand the Army's Battlespace Tactical Navigation program
 - Transition DARPA GPS pseudolite technology to the Army
 - Develop MEMS inertials
 - Centralize the existing Army activities in Pos/Nav/Time

Precision positioning/navigation/time (Pos/Nav/Time) is critical to all dimensions of ground combat. This includes coordinating maneuver, precise targeting, precision attack, and enhancing secure communications. From a broader, national security perspective, precision Pos/Nav/Time is becoming the enabler for the critical infrastructures that support society (e.g., aviation, energy, finance, civil communications) as well as the host nations' infrastructure upon whose support the Army depends in the theater.

This Pos/Nav/Time capability is provided by a system-of-systems. The core capability is GPS. It provides global Pos/Nav/Time service that is seamless, consistent, and uniform, as well as a precise global timing/synchronization standard. A brief description of GPS' technical and performance features is provided later in this appendix. The Army has stated requirements for 86% of the DoD user equipment. A breakdown of this requirement across organization and requirement type is provided in this appendix.

However, there are a number of areas in which GPS does not fully satisfy the Army's Pos/Nav/Time requirement. First, GPS has significant limitations in robustness. It is extremely vulnerable to jamming and to adversaries employing the system to satisfy their own Pos/Nav/Time needs. Second, the performance of GPS is limited in many types of complex terrain in which the Army is expected to operate (e.g., in urban canyons, in regions featuring forests or jungles). Third, greater than 60% of the GPS on-orbit satellites have single-string failure mechanisms. Although a number of replenishment satellites are available, future high powered replacements with greater jamming resistance will not begin to be deployed until 2009, with FOC achieved in 2017.

Finally, it must be emphasized that DoD no longer has sole control of GPS. There has long been tension between the military and civilian users of GPS in the area of exclusivity vice availability. On 2 May 2000, the tension was resolved in favor of the civil aviation community when the Selective Availability feature, which systematically degraded the accuracy of the signal available to the civilian community, was turned off.

There are several potential actions that the Army should pursue in the near- and mid-term, in conjunction with the other Services, to ameliorate the major deficiencies in GPS cited. First, to enhance resistance to enemy jamming, several technologies are available to upgrade GPS user receivers and antennas.

Second, to enhance resistance to potential enemy actions, enhance coverage, and compensate for the fragility of the GPS constellation, the system should be augmented with Psuedolites in a variety of basing modes. These Psuedolites would transmit high power GPS signals that are less susceptible to jamming and could be employed to degrade an adversary's capability to exploit GPS.

Finally, to mitigate selected coverage and performance issues, a variety of complementary navigation systems could be developed and deployed (e.g., inertial systems employing micro-electromechanical systems (MEMS); time of arrival (TOA) processing in future communications systems such as the Joint Tactical Radio System (JTRS)). These options are discussed in this appendix.

As a consequence of the analyses performed by the panel, the following major recommendations are offered.

- The Army's Battlespace Tactical Navigation Program should be accelerated and expanded. In particular, this program should be the vehicle to transition DARPA GPS Psuedolites technology to the Army and to develop MEMS inertial systems.
- The Army should create a Pos/Nav/Time Center to centralize its RDT&E activities. The current Pos/Nav/Time activities are too diffused lack a critical mass.

Challenges and Innovation - Pos/Nav/Time Robustness

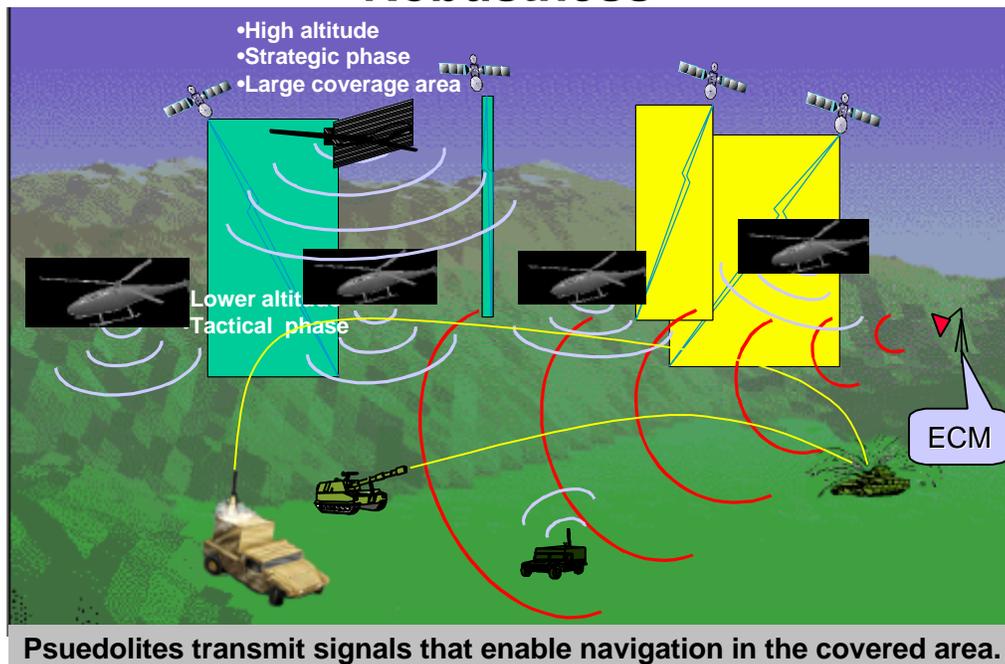
- **Challenge**
 - First enhanced jam resistant satellite not on orbit until 2009
 - Full constellation on orbit by 2017
- **Potential Innovations: Enhance jam resistance through:**
 - Psuedolites; options include
 - High altitude on Global Hawk
 - Low-to-medium altitude on A-160 or Predator
 - Ground based
 - Improvements in
 - Antennas
 - Receivers

The vulnerability of the GPS signals to very low power jamming has been known since the initiation of the GPS satellite development in the mid 1970s. However, serious development of techniques to mitigate the vulnerability of GPS commenced only in the past ten years. One of the proposed means to enhance the jam resistance of the system has been to increase the power of future GPS satellites by up to a factor of a hundred. This higher power GPS satellite will significantly decrease the vulnerability to jamming. However, the present GPS satellite launch schedule, coupled with the planned GPS satellites in the pipeline, will result in a 2009 launch of the first high power GPS satellite. Consistent with this plan, a full high power satellite constellation will not be in orbit until 2017.

Given this long delay in achieving a more robust satellite signal, it has been necessary to explore other ways to enhance the jam resistance of the GPS. One technique is to employ Psuedolites, which are airborne or ground-based transmitters that can emit more powerful GPS signals to counteract the effects of jamming. This technique is the only near-term, force-wide mitigation technology because it recapitalizes legacy equipment. CECOM and DARPA have demonstrated that most current receivers can be used with Psuedolites with only a new load of software for the receivers. The chart that follows illustrates the potential use of Psuedolites in several different deployments, high altitude, low-to-medium altitude, ground-based.

There are several other techniques to enhance the performance of GPS in a jamming environment. These include augmentation of GPS receiver equipment with anti-jamming (A/J) antennas, filters, and other A/J processing electronics. This option is discussed below.

Pseudolites Give Pos/Nav/Time Robustness



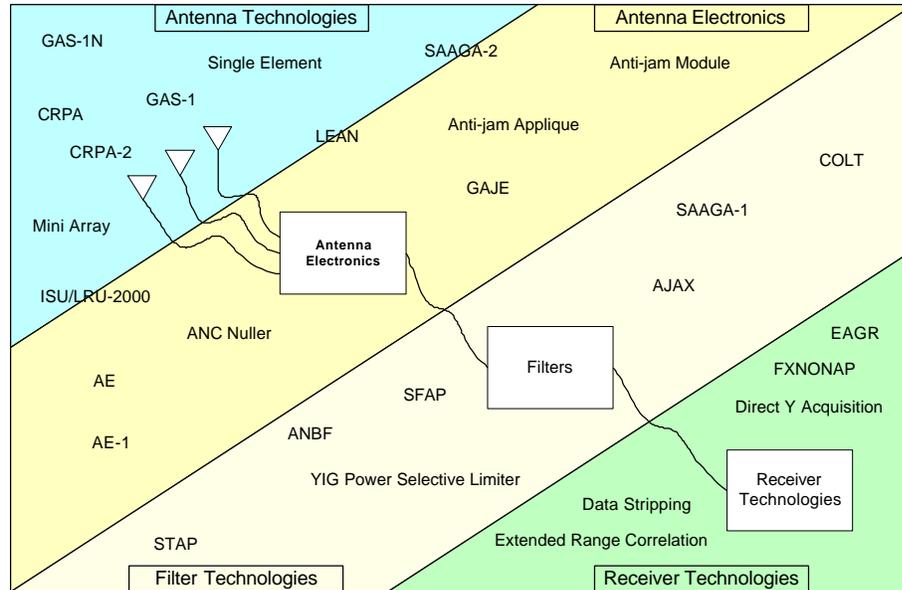
Pseudolites can ensure that a Joint and Combined Objective Force will have the Pos/Nav/Time support necessary for critical coordination. They can be deployed in several ways including high altitude, low-to-medium altitude, and ground-based configurations. As a caveat, note that airborne Pseudolites will generally have reduced accuracy as compared to the space-based service, due to aircraft tracking limitations in the GPS message, sub-optimal ranging geometries in tactical operations, and limited ionosphere measurements.

High Altitude Pseudolites. In the acquisition mode, one or more pseudolites can transmit precise time and satellite data to aid direct military code signal acquisition. This gives some level of A/J immunity and may allow legacy receivers to comply with the JCS mandate not to use the civilian acquisition code. This mode requires visibility to only one pseudolite; therefore, geometrical considerations are reduced and each pseudolite can have a wide area of coverage. A single high altitude pseudolite could be used during the early strategic phase of an operation while reducing the logistical burden and freeing up UAVs for other missions.

Low-to-Medium Altitude Pseudolites. If four or more pseudolites are visible in a widely spread out configuration, they can be used for navigation. Since the user will no longer be reliant on satellite signal reception, the anti-jam capability will only be limited by the power transmitted by the Pseudolites. This type of operation would be most consistent with the tactical attack phase of operations. The larger number of UAVs would be operating in the area to support other functions including communication relay, targeting and BDA.

Ground-Based Pseudolites. In this implementation, the transmitted signal can only be used to counter jamming in the local area. However, it can be sited in such a way as to enhance its effectiveness against enemy jammers whose location is known. It can also serve the same function as a high altitude Pseudolites for precise timing and precise signal acquisition for proximate ground-based GPS receivers.

Promising GPS User Equipment A/J Technologies



There are many alternative A/J technologies that could be implemented to provide relatively near-term enhancement to the robustness of a GPS user. Some can be used together, in succession, and some must be used alone. The diagram shows, pictorially, the components of a GPS receiver with the antenna in the upper left and the receiver itself on the lower right. The other two regions are for in-line A/J enhancements.

The antenna technologies are Controlled-Radiation-Pattern Antennas (CRPA). These are multi-element arrays that can reduce reception sensitivity in the direction of the jammers. More sophisticated systems can form more sensitive reception beams steered to the satellites.

The filter technologies are in-line devices that can be added to legacy receivers or integrated with other technologies. In the most complex installation, spatially controlled sensitivities can be combined with beam forming and filter technologies for maximum jammer rejection. As an illustration, typical existing aircraft nulling antennas are 14” in diameter and feature limited nulling processing. However, mini-CRPAs that are being developed for USN aircraft, use 4” footprint, Space-Time Adaptive Processing (STAP), and beam forming. These new units would be compatible with Army vehicles and greatly enhance their resistance to jamming.

The last region is the receiver itself. Various signal-processing techniques are being developed for use in next generation and notional receivers. For example, Frequency Domain Interference Suppression circuits have been developed for use in adaptive narrow-band filters for aircraft receivers. These units can defeat multiple first generation jammers. This technology is appropriate for hand-held users with A/J performance traded for battery life under jamming conditions.

Challenges and Innovation - Pos/Nav/Time Performance

- **Issue: Coverage**
 - Challenge: Inadequate coverage in complex terrain; e.g., urban canyons; jungles, forests
 - Potential innovations
 - Near-term: Network assisted GPS (e.g., PLRS; TOA into JTRS)
 - Longer-term: Exploit MEMS for micro-miniaturized inertial navigators
- **Issue: Support to precise targeting, robotic navigation**
 - Challenge: Pos/Nav/Time limitations in matching GIS and EO/Video
 - Potential Innovation:
 - Conduct trade-off analyses (e.g., Matching GIS and EO/Video as a function of DTED level)
 - Based on results of trade-off analyses, acquire appropriate DTED level data

Since GPS signals are at L-band (i.e., 1227.6 and 1575.42 MHz), they do not penetrate building walls and are severely attenuated by foliage. Thus, the existing GPS system can not fully support the Army's Pos/Nav/Time needs in urban conflict or operations in jungles or forests. Several technical innovations can help to mitigate this problem.

In the near-term, coverage shortfalls could be ameliorated by employing network-assisted GPS. This technique makes use of a technology that employs cell phones, Position Location Reporting System (PLRS), or SINCGARS to relay data between a central processing site and the user GPS set. In the longer term, incorporating a time of arrival (TOA) position location capability into the JTRS would provide a similar capability.

Another technique consists of using micro-machined accelerometers and gyroscopes (MEMS) to form a low cost inertial navigator to keep track of vehicular or soldier motion. This approach has significant benefits because it is self-contained and cannot be jammed. The technical challenge is that Pos/Nav accuracy is substantially reduced as the size of the devices gets smaller and the system is characterized by relatively high drift rates.

An additional performance issue arises from the challenge of providing precision terrain mapping support to precise targeting and robotic navigation. Current available digital maps do not correlate very well with GPS or other navigation sensors because of the coarseness of the available Digital Terrain Elevation Data (DTED) on a worldwide basis. As a foundation for future efforts, trade-off analyses are required to assess the ability to match Geographic Information System (GIS) and Electro-Optical/Video information as a function of DTED level. Based on the results of these analyses, it is imperative that substantial resources be applied to acquiring the appropriate DTED level to support precision targeting and robotic navigation.

Challenges and Innovation - Pos / Nav / Time System Integrity

- **Issue: GPS Constellation (National/USAF problem)**
 - Challenge: GPS constellation is currently in a “fragile” state
 - Potential Innovations:
 - Develop, field “gapfiller” pseudolites for theater use
 - Army encourage the USAF/National Authorities to address as a Joint problem
- **Issue: GPS Spectrum**
 - Challenge: Absence of coherent national GPS spectrum leadership, strategy
 - Potential Innovations: Urge DoD’s CIO to develop a proactive stance for GPS spectrum protection that the Services would support strongly

The GPS satellite constellation is in a “fragile” state. At the present time a combination of budget deferrals, coupled with satellite operational lifetimes that have consistently exceeded predicted design lives, have resulted in keeping marginally healthy satellites in operation and delaying the launch of replacements. As an example, 16 of 28 on-orbit satellites have a single-string failure mechanism (i.e., there is no back up capability). In addition, the satellite ground-based control segment control improvements have not been accelerated as needed to match satellite upgrades. Finally, the first launch of the higher power satellites designed to mitigate the signal jamming problem has been delayed until 2009. The current plan is to launch three satellites per year, thereafter, for and IOC in 2015 (with 18 on orbit) and FOC in 2017.

As noted above, the development and use of Pseudolites as gapfillers for theater use is the best way to address this problem and to provide a more reliable Pos/Nav/Time capability for all US and coalition forces in future theater operations. In the longer term, this is not a matter that the Army can solve by itself. The USAF manages and operates the GPS under the auspices of the Interagency GPS Executive Board (IGEB), whose members are drawn from DoD/JCS, DOT, DOS, DOC, DOI, DOA, DOJ, and NASA. It is imperative that the Army take whatever action is necessary to secure a voice in the decision making on GPS management, financing, and operations.

A related issue concerns the ownership of that portion of the electromagnetic spectrum assigned to the GPS. For the past several years there have been attempts by international spectrum oversight bodies to reallocate portions of the spectrum now allocated to GPS. This would severely restrict opportunities for improving GPS capabilities in the future. This matter requires much stronger leadership within the DoD to protect GPS spectrum. The Army should urge the DoD Chief Information Officer (CIO) to develop, present, and maintain a proactive stance for GPS spectrum support both within the US and in international fora.

Challenges and Innovation - GPS Institutional Issues

- **Challenges:**
 - DoD no longer has sole control of GPS
 - Given military-civilian equities, major issues persist on GPS management, financing, operations

- **Potential Innovation:**
 - The Army should work with the DoD members of the Interagency GPS Executive Board (IGEB) to support the establishment of an Extra-Departmental GPS National Program Office

The recent termination of Selective Availability has highlighted the fact that the DoD no longer has sole control of GPS. The ramifications of this action are likely to be substantial in both the civil/commercial and the military sectors. From the civil/commercial perspective, the economic and safety benefits are likely to be very high. They will now be able to achieve consistent horizontal accuracy within 5 - 7 meters and to improve timing/synchronization dramatically (e.g., on the order of 8 - 10 nanoseconds). From the military perspective, this action significantly increases the risk of use of GPS by adversaries. By exploiting this capability, a resource-limited adversary can obtain three-dimensional accuracy within 8 - 10 meters. When coupled with data from precision commercial imaging sources, this will enable them to support effective use of precision guided munitions.

This event underscores the fact that the current management, operation, and financing of GPS do not reflect its integral role in operation of national infrastructures or its contributions to national economic and security enterprises. In particular, there is a significant lack of agreement on national Pos/Nav/Time goals and objectives and the strategy that would be needed to achieve those national objectives.

To redress this shortfall, an extra- or intra- Departmental entity is needed to provide national management of Pos/Nav/Time activities and systems. This might subsume a Government Corporation with direct leadership provided by a National Program Office. Such an office should be staffed with individuals detailed from involved agencies (e.g., DoD, DOT, DOS, DOC, DOI, DOA, DOJ, and DOE). Functionally, this National Program Office would develop/coordinate/approve national policy for GPS services and operations; review GPS

resource requirements/budgets; assess GPS' role in economic, security, and technical infrastructures; and work with OMB to ensure funding continuity/stability.

It is recommended that the Army work with the DoD members of the IGEB to support the establishment of this extra/intra-Departmental National Pos/Nav/Time Program Office.

Primary Recommendations

- **Accelerate and expand Army Battlespace Tactical Navigation Program**
 - Pseudolites - transition DARPA GPS pseudolites to Army JPO
 - AJ technologies - develop AJ receiver technologies, electronically steered antennas
- **Identify high value/high risk platforms that require enhanced Pos/Nav/Time capability and fund, deploy as appropriate**
- **Establish an Army Pos/Nav/Time Center**

At the present time, the Army's Battlespace Tactical Navigation Program provides advanced development funding for enhancing the robustness and accuracy of Army Pos/Nav/Time capabilities on the battlefield. This program includes a variety of hardware and technology developments to enable the use of GPS in a jamming environment such as anti-jam antennas and adaptive receiver filtering, as discussed in Chart 5. It also includes the Pseudolites developments for air and ground basing depicted in Chart 6. Additional tasks including map/image/video/navigation registration techniques, and modeling and simulation to emulate current and future Pos/Nav/Time systems and emerging technologies to assist in design and development activities are part of this program. Funding must be increased if these developments are to provide support to the FCS. The Army should expand the Battlespace Tactical Navigation Program from its current funding levels of \$1M - \$2M per year to at least \$10M per year. The USAF and USN are pursuing complementary RDT&E activities, but they are not addressing many of the issues that confront the Army (e.g., battery life, logistics and operational challenges). In addition, action should also take the lead to transition DARPA's Pseudolites development programs to the tactical warfighters.

Second, a process should be initiated by the Army Acquisition Executive (AAE) to identify high value; high risk platforms that require enhanced Pos/Nav/Time capability. Once those

platforms have been identified, the necessary programs must be established to develop, fund, and deploy those capabilities.

Finally, because of the importance of Pos/Nav/Time to all Army operations, the Army should take necessary actions to create a Pos/Nav/Time Center that consolidates all relevant RDT&E activities in this area.

Additional Recommendations

- **Track and Act**
 - Track, take advantage of commercial initiatives in E911
 - Track International Pos/Nav/Time efforts (e.g., Galileo), and take steps to ensure that if a system emerges, it is compatible with GPS, the US Pos/Nav/Time system
- **Accelerate**
 - In FY03, start Precision Navigation for FCS, focusing on MEMS
- **Re-vector**
 - Identify, implement cost-effective DTED Level to support matching GIS and EO/Video
 - Support major institutional initiatives (management, financial, operations; spectrum policy)

There are several ongoing activities that the Army should track and act upon. First, the Army should take advantage of the commercial initiatives that are underway in response to the Federal Communications Commission's (FCC's) 1996 mandate. At that time, they issued a requirement for locating the position of a handset that originated an Emergency 911 call. The FCC specified that wireless carriers should be able to locate 67% of emergency calls to within 50 meters and 95% of emergency calls to 150 meters. Efforts are underway to explore hybrid handset-network solutions to this requirement. In one variant, the GPS front end in the handset transfers partially processed GPS satellite data to the network. It is in the network that the GPS signals are processed and location determination is made. Alternatively, a receiver's performance could be enhanced by downloading satellite ephemeris data and time from the network. This would enable the calculation of position information more quickly and potentially under more adverse conditions. Proof-of-concept activities should be undertaken to assess the utility of these initiatives to the Army.

In the international arena, there have been discussions concerning development and production of a satellite-based Pos/Nav/Time system because of concerns about the availability of GPS services in wartime or crisis situations. In Europe, the discussions have led to a proposal to

develop and deploy a GPS-like system named Galileo. The Army should work with the DoD CIO to track the European activities and ensure that the system, if deployed, is compatible with GPS.

To ensure that the FCS has adequate Pos/Nav/Time support, the Army should initiate a program, the Army Precision Navigation for FCS Science and Technology Objective (STO), to develop and deploy an A/J GPS receiver/antenna system, coupled with a MEMS inertial navigator as a backup. This activity should commence immediately under the aegis of the Army Pos/Nav/Time Center (recommended above).

GPS Characteristics - Signal Evolution

- **Present signal**
 - Frequencies
 - L1 (1575.42 MHz)
 - L2 (1227.6 MHz)
 - Codes
 - Civilian: C/A
 - Military: P(Y)
- **Proposed 2003 signal**
 - Augmentation with a military M code at L1, L2
- **Planned 2005 signal**
 - Augmentation with a new civilian
 - Frequency (L5: 1176.45 MHz)
 - Code (at L5)

Currently, GPS broadcasts civilian and military codes (C/A and P(Y), respectively) at two L-band frequencies: L1 (1575.42 MHz) and L2 (1227.6 MHz). A Proposed IIR Modification (scheduled for launch in 2003) would augment the signals at L1 and L2 with a new military code, M. The planned IIF and follow-on configuration (scheduled for a launch in 2005/2006) would add a new civilian frequency, L5 (1176.45 MHz).

GPS Performance

- **Position**
 - Direct: 7 - 10 meters (3 dimensions)
 - Differential: 1 - 3 meters (3 dimensions)
- **Velocity: <10 centimeters/second (3 dimensions)**
- **Time: 8 - 10 nanoseconds**

The basic GPS system consists of 24 satellites (with 4 on-orbit spares), a master control system, and a large number of receivers that passively employ ranging information from 4 satellites to estimate the state of the receiver user. Since selective availability has been disabled, any direct user of the system will be able to estimate his position to 7 - 10 meters (3 dimensions) and velocity to less than 10 centimeters/second (3 dimensions). For stationary, or very slowly moving users, long term integration can substantially reduce the error in position location. If a calibrated reference source is available, the system can be operated in a differential mode, increasing the position accuracy to 1 - 3 meters (3 dimensions). In addition, users can use the signal to estimate time to an accuracy of 8 - 10 nanoseconds.

Army GPS Receiver Requirements

<u>ORGANIZATION</u>	<u>STAND ALONE REQUIREMENTS</u>	<u>EMBEDDED REQUIREMENTS</u>	<u>TRAINING REQUIREMENTS</u>	<u>TOTAL REQUIREMENTS</u>
APG	0	0	54	54
AIR DEFENSE	5,168	0	182	5,350
AMEDD	2,618	0	10	2,628
ARMOR	13,218	1,518	130	14,866
AVIATION	9,477	5,173	16	14,666
CASCOM	15,812	0	178	15,990
CHEMICAL	1,510	0	34	1,544
ENGINEER	12,482	0	30	12,512
FIELD ARTILLERY	13,682	515,848	145	529,675
INFANTRY	19,906	4,800	473	25,179
INTELLIGENCE	3,410	233	8	3,651
MILITARY POLICE	6,607	0	12	6,619
SIGNAL	5,204	864	91	6,159
SOF	3,137	3,565	65	6,767
OTHER	1,032	0	993	2,025
TOTAL	113,263	532,001	2,421	647,685

*** 86% Of DoD UE Requirement is Attributed to the Army**

The above Chart decomposes the Army's GPS receiver requirements in two dimensions: by organization and by type of requirement (i.e., stand alone, embedded, training). The matrix is dominated by the Field Artillery's need for embedded requirements (i.e., the 515,848 shells that could be transformed into smart munitions by the addition of a GPS receiver). Even if these requirements were deleted from the matrix, the remaining Army requirements would still constitute 55.5% of the DoD's total GPS receiver requirements.

APPENDIX I

PROTECT AND COUNTER

APPENDIX I

Protect and Counter

Protect and Counter

$$\text{Information Dominance} = \frac{\text{Blue Information}}{\text{Red Information}}$$

*Protecting the Blue information infrastructure
is essential*

*Countering the Red information infrastructure
is equally important*

Information Dominance has two elements. First, is Blue's ability to acquire, process and move information on the Battlefield. This needs to be accomplished in spite of Red's attempts (Red offensive I.O.) to degrade and delay the information timeliness and quality. The second is Blue's ability to prevent Red (Blue offensive I.O.) from acquiring, processing and moving critical information on the battlefield.

Red offensive information operations will attempt to attack those vulnerabilities of the U.S. Army's tactical InfoSphere, which have not been hardened and protected. These vulnerabilities, if not corrected, will result in U.S. Army losing timely, critical decision support information on the battlefield. Similarly, if the U.S. Army fields the appropriate systems to counter the adversary's information infrastructure, the impact will severely degrade the adversary's ability to make good battlefield decisions.

Protect and Counter Overview

- **The Operational Challenge - Protect Blue and Countering Red**
 - Impacted by COTS/GOTS availability
 - Need to train in a realistic Information Operation environment.
- **Independent technical protect and counter organization,**
 - Support for stressful testing and exercise
 - Address the countermeasure “avoid” with area surveillance
- **Key is an independent, unbiased organization, a Red Team**
 - Challenge the Blue systems of systems
 - Core exists today in ARL, SLAD
- **Critical technologies must be threat responsive**
 - Require threat knowledge and rapid development cycles
 - Key technologies include sensor CM and hardening, I.O. and Information Assurance, Countermeasure and realistic training, exercise, Modeling and Simulation in a CM / IO environment
- **Recommendations:**
 - Establish a funded, independent red Team ARL / SLAD
 - Fund S&T for mine avoidance
 - Demand stressful modeling, simulation, testing, exercise and training

This VG is a short overview of the Protect and Counter briefing. The details contained on the following viewgraphs are the key thoughts of the Protect and Counter sub-panel. The operational challenge of **protecting Blue** and **countering Red** systems is impacted by availability of COTS/GOTS worldwide. The U.S. Army will need to train in “peacetime” to be prepared to work in the difficult environment of the future. The need to train as we fight in a realistic CM / IO environment is essential and historically not well done because “smart” OPFOR / Red Team countermeasures shut down Army capabilities. The Army must move to a concept more like the U.S. Navy “Top Gun” where training occurs against a highly capable and innovative enemy and provides an order of magnitude of improvement in the actual combat capabilities of U.S. Navy pilots.

Support for the training of U.S. Army forces and hardening of systems is not easy. The best solution requires the decision to allow a strong technical “Red Team” to support the OPFOR units, Trainers, Battlelabs and PEOs activities to provide a truly representative environment. The ASB has described an innovative concept. The innovation of an independent technical protect and counter organization, support for stressful testing and exercise and addressing the countermeasure “avoid” area surveillance problem are key challenges

During the study, the ASB was impressed with the opportunity to grow this type organization from an existing core. An ARL organization already exists with much of the talent, tools, culture and skills to accomplish the task. The key solution is an independent, unbiased organization to challenge (Red Team) the Blue systems of systems core exists today in ARL / SLAD. SLAD also

has the foundation for effective Information Assurance assessment when collaborating with NGIC, CECOM and LIWA.

Critical technologies in the protect and counter area are threat responsive and require threat knowledge and rapid development cycles to protect or countermeasure. The U.S. should have significant advantage from this cycle. Key technologies include sensor CM and hardening, I.O. and Information Assurance, Countermeasure and realistic training / exercise.

In terms of modeling and simulations in a CM / IO environment, the U.S. Army advantage can only be obtained if the development, upgrading and fielding of Protect and Counter systems is executed in a timely manner. At a minimum a spiral development concept is critical in the counter-countermeasure environment.

Recommendations:

- Establish an independent technical vulnerability assessment organization. ARL / SLAD can provide the nucleus of this organization.
- Fund S&T for mine avoidance.
- Demand stressful modeling, simulation, testing, exercise and training.

It is vital that the Army create a process for assuring that all information dependent systems and their operators are subjected to realistic information operations attacks. If we cannot protect our information infrastructure while attacking its counterpart, there is no way to gain information dominance upon which to base the survival of the FCS force.

Operational Challenge - Information Warfare

Info. Dominance = Blue Knowledge / Red Knowledge

Protect our ability to collect/process/disseminate information -
while denying this capability to our adversaries enables Blue to:

Know First / Shoot First / Kill first



- Parity of Technology (COTS / GOTS available to both Red and Blue)
- Red advantage (Home Court) in knowledge of local terrain, local structures, infrastructure, citizens, etc.
- C4ISR signatures “Lights up” Blue Forces presence
- Blue C4ISR is complex, vulnerable and imperfect
- Protecting Blue Information Assurance advantage against Red threats
- Countering Red information assurance and ISR
- Testing, Training and Exercising in realistic Countermeasure / I.O. environments

Information Dominance demands a capable and well protected U.S. Tactical InfoSphere as well as effective degradation and destruction of the enemy information and sensing capabilities.

The Battlefield of the future will continue to reflect a strong aspect of Counter-Countermeasures. This dynamic process of countering opponent systems with powerful, targeted attacks on systems and information vulnerabilities will accelerate as the U.S. Army moves further into the information age. It will become critical to obtain information dominance on the battlefield if one is to be in the position to shoot first. This dominance will be a factor of both the robustness and capability of U.S. Army information systems and our ability to degrade hostile / enemy systems.

In the time frame of the Objective Force, the technologies of information collection, communications, information management, information retrieval and processing, information correlation will be available to the entire world. The ability of the U.S. to exploit this technology and simultaneously deny the advantage to the enemy will be a dynamic process of protect and counter. The hostile forces will continue to have the advantage of defending on their “home court”. This is a significant knowledge advantage. The U.S. will have to offset this advantage with high quality IPB and strong countermeasures to degrade the opposition force advantage.

As an entry force on the “home court” of the opposition, U.S. Forces will be identifiable from the broad range of signatures and activities they will bring into the area of operations. This will allow the opposition forces opportunities to exploit these unique signatures for targeting U.S.

Forces. At the same time, the complex C4ISR systems U.S. forces bring into the area will be targets of opposition force exploitation and attack.

Information Assurance is a critical area of technology for U.S. Forces to win information dominance. We must attack Red information systems successfully and protect our own from stressful Red attacks. Without extensive, realistic training and exercise prior to these information rich activities on hostile ground, the U.S. Forces will be unprepared for the broad range of attacks, (countermeasures and IO) which an enemy force will bring to bear. Hostile forces will have the benefit of years of assessment by many countries on the vulnerabilities and weakness of our COTS / GOTS based systems. We must train and exercise in this challenging environment to be prepared.

Innovations and Challenge

- **Development of an independent technical protect and counter C4ISR activity to develop Hardening and Exploitation solutions:**
 - Overcome Acquisition organizations and operational organizations fear of independent assessment activity
- **Recognition of mines as a critical threat to FCS/FTR requires rapid wide area surveillance to support avoidance tactics**
 - Overcome reluctance to recognize mines as primary killer of US Armor
 - Vulnerability of FCS/FTR to next generation mines is unevaluated
 - Recognition of mines as weapon of choice from asymmetric defense
 - Development of intelligence and analysis in defining next generation mines
- **A process to stress M&S, testing, exercise and training with realistic countermeasures to prepare to fight asymmetric threats**
 - Stressful CM / I.O. shuts down exercises and training

Information Dominance will provide an opportunity for U.S. Forces to gain a significant battlefield advantage in the future. Where U.S. Forces have substantially higher quality knowledge than opposition forces, red forces will challenge this opportunity. Red forces have the operational advantage, knowing both the physical environment and population, and have months to years to prepare. Our forces will enter these areas with only limited knowledge, even with a powerful IPB capability that can exist in the objective force timeframe.

Thus, it is essential that we consider how we will be able to achieve Information Dominance in these environments. This is a two-part activity. First, build a force which will have the sensors, tools and communications to rapidly develop in-depth knowledge of the situation and at the same time, significantly degrade Red knowledge of U.S. force operations and activities.

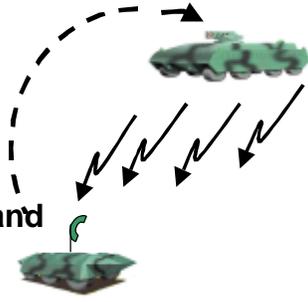
A key limitation we will have to overcome is the ability to adequately prepare U.S. Forces for operation in these counter-countermeasures environments. This will require the development of an independent technical protect and counter C4ISR activity. This action would develop hardening and exploitation solutions to ensure the U.S. forces have the systems, expertise and training to win. Due to the complexity and “systems-of-systems” organization of objective force capabilities, it is essential that an independent, unbiased technical organization be available to develop the range of countermeasures essential to degrade Red information systems and sensors and to protect U.S. Forces information and sensor systems. This organization will provide the stress and challenge during objective force development, testing, training and exercise to ensure the force is well prepared to face the range of attacks on the battlefield where information dominance will determine the winner.

A particular threat to the FCS-based Objective Force requiring increased attention comes from landmines, both current and next generation. These will be the weapon of choice for many hostile forces. History shows a constantly increasing trend of combat vehicle losses due to landmines. This trend is expected to continue, especially with the introduction of next generation advanced detection, fuzing and lethality techniques. A more detailed discussion of these features will be provided with a subsequent slide. These next generation mines will be widely available through international trade channels and there is beginning evidence of this in defense-oriented trade journals already. This says that landmines will be a weapon of choice for our adversaries, since they provide “cheap kills”, an easily deployable defense and exploit their “home court” advantage. An Army organization, such as NGIC, should be designated as Lead Agency to gather intelligence data on and analyze emerging next generation landmines and assess their impact on FCS operations

Pre-combat assurance that the FCS-based Objective Force can achieve the asymmetrical Information and Survivability advantage over our adversaries can be obtained by implementing rigorous Modeling and Simulation (M&S), testing, warfighting exercises and training. Training, in particular, with realistic countermeasures is a key requirement. This is a difficult and challenging task since history has shown that a full-scale operational exercises, such as those conducted at NTC, can be effectively shut down when powerful EW techniques are introduced. This, of course, is just the point. How can you fight through the disruption caused by EW/ECM or I.O.? Because the Objective Force will be information intensive and therefore vulnerable to asymmetric threats, it is imperative that the evolving Objective Force be exposed to these possible threats prior to actual exposure in combat.

Next Generation Enemy Mines - Significant Threat to FCS

- **Sensor fuzed:** Fires mine on positive Recognition of FCS (Acoustic, R.F., Image, Thermal, Seismic, ??)
- **Stand off:** 100 meters +, Counter APS modes
- **Dispersed:** Large areas, thinly populated fields
- **Deployed:** Rapidly, via Air, Artillery, Rocket, hand
- **Probability of Kill:** High, single shot kill
- **Signature:** Mine is Difficult to detect, low / deceptive signature
- **Employment:** Flexible to allow Urban applications



History shows us that the primary killer of U.S. armor is mines. The trend is ominous and the future of U.S. Forces needs to account for this trend. The obvious weapons of choice for forces that do not want to face U.S. lethality head-on are mines and booby-traps. The technology of “smart mines” will provide an awesome threat. Mines will be smart enough to autonomously recognize an FCS, determine the range and direction to the FCS, and then arm and fire munitions at the FCS. Hostile forces will have the opportunity to deploy and activate (or deactivate) these mines before U.S. forces arrive in an area, or deploy them rapidly after U.S. forces are present. The mine munitions will be lethal to FCS class systems and will have a high probability of single shot kill. Mines of similar nature will be encountered in urban environments.

The training and exercise of U.S. Forces must include this class of weapon in both OPFOR class training at the NTC and in home base training and exercises. The potential for rapid, wide area surveillance systems to detect minefields is an essential problem area for Army S&T to emphasize.

Next generation enemy mines will constitute a significant threat to FCS. Current generation conventional Anti-tank (AT) landmines constitute a significant threat now because of their proliferation, ease of deployment, difficulty of detection and lethality. However, there is growing evidence of an evolving family of next generation landmines that will be available to and used by the adversaries to be faced by the FCS-based Objective Force. These next generation mines will be classified as “smart” in that they will employ embedded processors and sensors (acoustic, RF, Imaging, thermal, seismic, magnetic, etc.). They can also be classified as “agile”, in that they may utilize robotic mobility techniques and may be rapidly delivered by a variety of techniques, such

as submunitions from aircraft, artillery and rockets, as well as by conventional hand-delivered emplacement. The agility characteristic may also allow a wider radius of action (exceeding 100 meters), allowing delivery trajectories that permit top and side attack, as well as the more conventional bottom attack. The smart characteristics will give these mines the ability to identify specific targets, such as the FCS vehicles, differentiating them from less lucrative targets.

Mines with these characteristics are already beginning to appear in military-oriented commercial journals, offered by a number of commercial vendors, throughout the world. As MEMS and microelectronics continue to evolve, the intelligence and agility of next-generation mines will only continue to improve, constituting a significant threat to the Objective Force in its operational timeframe. Immediate and urgent action by the Army is indicated to understand the capabilities, availability and employment methods of these next-generation mines, due to their potential as significant threats to the FCS-based Objective Force, and to develop effective countermeasures against them.

A second example is the vulnerability of a FTR to hostile countermeasures and attack. The FTR will be a valuable, visible and attractive target for our adversaries. A preferred method of protecting a high value aircraft is to avoid the threat. With FTR this will be very difficult to do without unduly limiting the FTR's ability to accomplish its mission. For the FTR to be survivable the Air Force must provide total air superiority. The FTR could be designed to fly high enough to avoid the MANPADS (Man Portable Air Defense System) and small arms threats. However, given the elevation of some areas where it must operate and the range of modern MANPADS this requirement will drive the cost up. Unfortunately it is technically feasible to develop a MANPADS with 1.5 to 2 times the range of existing weapons if the requirement to engage high speed aircraft were waived.

In the case of anti-air systems that the FTR cannot negate by flying at high altitude, the FTR must either avoid them, countermeasure them or they must be neutralized. Avoiding or neutralizing them will be difficult since they will be hard to locate unless/until they radiate. Countering these threats is possible - if enough is known about their operation. Of course, a first step should be reducing the signature(s) of the FTR as much as possible. Reducing it to an undetectable level even at significant ranges is very unlikely in most bands; however, the smaller the signature the less difficult it will be to protect the FTR with countermeasures.

Even in the best case, defending the FTR will be a much more challenging endeavor than attacking it. First, the attacker has a broad range of options that have to be defended against. Second, the attack options tend to be less expensive and simpler than the defensive responses. What is needed is some type of generic defense system that will counter the anti-air threat. There are some high risk technical solutions using directed energy that might be available, but it is too early for a reliable estimate of how effective this approach might be.

Clearly more attention must be given to the survivability of the FTR in likely scenarios and against the threats that it will encounter. The problem is not unlike protecting an aircraft carrier - except the potential threats can be concealed nearby.

Enemy Tactical UAVs - A Significant Threat To FCS/FTR

- **UAV Systems' Survivability:**
 - Low cost (expendable?), Very Low signature, "low USAF priority"
- **UAV Systems' Capabilities:**
 - Exposes FCS/FTR to adversaries' enhanced targeting and surveillance
 - EO/IR/Radar (SAR, MTI, FOPEN) and designators - Low cost sensors
 - Communication relay and data dissemination
- **UAV employment modes:**
 - Useful in a variety of environments (Urban, open, weather?)
 - Low technology / cheap sensors are threats (e.g. CCD cameras, I²)
 - No technology challenge for enemy low end systems
- **U.S. Army Response Options:**
 - Shotguns, SAMS, HPM/DE, Sensor and Communications Countermeasures, Cover&Deception , Commanche?

Issue: "How to detect and respond, not the technology to respond"

"Red" UAVs represent a significant potential threat to both FCS and FTR. Although high altitude and medium altitude UAVs will be targets for the U.S.AF and Army air defense, low cost, low signature UAVs will be hard to detect, track and counter. Properly used, a UAV could provide an adversary a way to obtain timely information about the location and identity of U.S. forces and systems across a broad area of coverage with timely reporting capability not available from other sources. The UAV will itself be vulnerable to a wide variety of potential counters-small ballistic projectiles; EW jamming of sensor, communications, data-links; HPM/DE weapons, low altitude SAMS. The issue is how to locate, track and acquire the UAV and efficiently engage with weapon systems



Solution Sets - Examples

• Independent, unbiased organization to challenge (Red Team) the Blue systems of systems

- Identify Vulnerabilities of Red&Blue systems
- Aid development of tactics to minimize Blue vulnerabilities
- Support acquisition decisions
- Enable realistic training / testing
- Collaborate on the Development of I.O. tools

Core Exists today in ARL / SLAD



In the Future need a commitment to

1. Independent organization
2. Development of tools, staff, M&S
3. Support OPFOR, Battelabs, Training, PEO

•Countermine

- Next Generation mines will be developed to counter FCS and FTR
- Must avoid mines with a rapid, non-real-time wide area multi-sensor, fused surveillance systems complimented with on-going IPB, coupled with a real-time forward looking mine detection system (GSTAMIDS)

• Information Assurance Solution

US I.A. Technology



Test
Train
Exercise
Defend

The Army is developing complex, systems-of-systems, using COTS commercial infrastructure, rapidly evolving information technology and sensor technology. The U.S. has the opportunity to leverage COTS technology into a substantial battlefield capability or to build a complex, vulnerable target for the enemy. The final result will be very much a condition of how well we build a robust, protected, tested and stressed system prior to conflict and how well we recognize the strengths and opportunities of our adversaries to attack our systems. It is impossible for the developers and commanders to stress and test their systems adequately without a strong independent, unbiased organization to challenge (Red Team) the Blue C4ISR systems of systems

- Identify Vulnerabilities of Red & Blue systems
- Aid development of tactics to minimize Blue vulnerabilities
- Support acquisition decisions
- Enable realistic training / testing
- Collaborate on the Development of I.O. tools

Much of the core of such an organization exists today in the ARL/SLAD organization. This core needs to be expanded to allow SLAD the breadth and depth to provide the foundation of for ensuring the realistic, stressful assessment of U.S. Forces occurs in the development, test, training and exercise phase before engagement with Red forces and for ensuring that the appropriate fixes are accomplished. In the future, the Army needs a commitment to a SLAD activity which realizes, funds and permits:

1. An Independent organization
2. Development of tools, staff, M&S
3. Support for OPFOR, Battelabs, Training, and PEO development activities

Countermine - The FCS-based Objective Force will face a significant threat from next-Generation Landmines. These advanced mines can be deployed rapidly, have a standoff radius of action, will have a degree of intelligence and will employ a variety of embedded sensors that can selectively target FCS vehicles. These characteristics make the next-generation mine an important factor to be considered on the Objective Force battlefield. Since there is no “silver bullet” that can detect and negate this new threat, effort must be devoted to developing wide-area multi-sensor fused mine surveillance systems, which can be integrated into the Intelligence Preparation of the battlefield (IPB) activities. IPB surveys may need to be conducted more often than previously due to the adversary’s ability to change the configuration of mines on the battlefield, through use of remote delivery methods, such as aircraft, robotic vehicles or munitions. Therefore, the Army must develop an integrated multi-sensor suite that is suitable for UAV carriage, optimized for next-generation landmine detection and capable of reporting on a near-real-time basis. This will provide safe channels for FCS passage and allow the information to be distributed via the tactical InfoSphere to appropriate parties. Continued support is indicated for CECOM’s development efforts in Forward Look Mine Detection for Ground Vehicles, as represented by the Ground Standoff Mine Detection System (GSTAMIDS) program.

Information Assurance - Complex information systems are endemic to all aspects of U.S. military forces. A strong U.S. information assurance technology base is being driven by a strong U.S. government information assurance program. The military has designated a CINC to focus these efforts and the Army has the opportunity to benefit from this significant U.S. effort. However, it still is the job of the Army to ensure adequate hardness is built into the Army Tactical InfoSphere, and this is not easy. NGIC, CECOM and LIWA have key roles, but the essential assessment role of an independent test and assessment activity (such as SLAD) needs to be emphasized. IO techniques need to be utilized to stress Tactical InfoSphere elements and the overall system from the development stage through the test, training and exercise phases. The hardening and information assurance of Tactical InfoSphere systems must be guaranteed.

Technology Score Card

Critical needs

<ul style="list-style-type: none"> • Signature management • E.W systems Sensor denial • E.W. systems C3CM • U.S, Sensor hardening • Defensive Information Assurance • Optical Augmentation application • SAR, MTI Deception • Counter space surveillance EO/IR • Countermine-area surveillance • Institutional Technical Red Team 	<ul style="list-style-type: none"> L.O. and Deception RF, E.O. IR, Acoustic R.F, Optical RF, EO, IR, Acoustic, other Overall I,O, protect For all FCS/FTR elements Against air and space Battlefield protection Rapid detect to allow avoid Critical to Develop, Test, Train & Exercise activities NTC and Home training Hostile C4ISR/Tgt.Acq. Actions to respond to attack Detect, Track, Engage Data to support CM development FCS and FTR integrated suites RF and DE weapons 	<ul style="list-style-type: none"> Yellow Yellow Yellow Red Red Yellow Yellow Yellow Red Yellow Red Yellow Red Yellow Red Yellow Red Yellow Red Yellow
---	--	--

As is reflected in this viewgraph, we have significant room for improvement in every area. If the Army is serious that Information Dominance is key, we must outpace our adversaries. In the critical technology areas we have the opportunity to make our systems very robust and attack the fragile systems that adversaries will field with COTS / GOTS applications. We need to develop the DTLOMS to exploit an adversary's weakness and our information strengths against hostile IO attacks. It is essential to place significant emphasis on this ability to obtain battlefield dominance.



KEY TECHNOLOGIES FOR COUNTER C4ISR



CAPABILITIES	SUPPORTING TECHNOLOGIES	REQUIRED	USEFUL	DEAD END
RED DENY USE OF COMMERCIAL SPACE	I.W. / ACTIVE CM GND ATTACK SYS. DECEPTION SYSTEMS SIGNATURE MGMT.	INTEGRATED SPACE CONTROL, DISRUPT – DECEIVE THEATER COLLECTION & DISSEMIN.	TRAINING VULN. OF US SYSTEMS AND USES	CONTINUED LACK OF BATTLEFIELD SPACE CONTROL RED
PINK HARDEN US Army COTS SYSTEMS	SENSOR AND C3 EVALUATION & POINT FIXES	EXHAUSTIVE EVALUATION OF COTS, RED TEAM, TRAINING	VULN. OF COTS DESIGN OF COUNTER COTS. DIRECT SUPPORT TO OP4 AND EXERCISES	LACK OF UNBIASED, INDEPENDENT VULNERABILITY ASSESSMENT ACTIVITY PINK
GREEN DENY HOSTILE E.O. CAPABILITY	OPTICAL AUGMENT.. C3 GEOLOCATION NETWORK EXPLOIT. ESM GEOLOCATION	LOCATE ALL F.O. IN NRT TO ALLOW TGTING. OR DENIAL/DECEPTION	SUPPORT TGTING. OF ALL OPTICS, C3 AND RF SYSTEMS ON BATTLEFIELD	FAILURE TO DETECT PASSIVE OPTICAL SENSORS ON BATTLEFIELD GREEN
RED INSTITUTIONALIZE SURVIVABILITY & LETHALITY TECH. ANALYSIS ACTIVITY INFORMATION ASSURANCE EFFECTIVE RANGE OF SIGNATURE MGMT.	INTELLIGENCE ASSESSMENTS, TECHNICAL VULN. ASSESS. TECHNIQUES AND MODELS MAJORITY DEVELOPED BY COMMERCIAL. SUPPORTED BY NSC/DOD SIGN. REDUCTION SIGN. MODIFICATION DECEPTION SYSTEMS	INDEPENDENT ASSESS. OF ALL DEVELOPMENT AND OPERATIONAL SYSTEMS INDEPTASSESSMENT OF ALL BATTLEFIELD IT SYSTEMS AND NETWORKS, ON GOING REDUCE BY 50% PD FOR FCS ELEMENTS REDUCE BY 50% PROB of ID ADD FALSE TARGETS	SUPPORT TO PROGRAM MGRS, OP4, OPS AND TRAINING ELEMENTS DEVELOP MET OF ENEMY VULN, OPPORTUNITY FOR BATTLEFIELD DECEPTION REDUCE TGT. ACQ BIAS CENTROID FOR HOMING SENSORS	LACK OF INTEGRATED CRADLE TO GRAVE VULN. ASSESSMENTS AND FIXES IT SYSTEMS WHERE THE BATTLEFIELD COMMANDER DOES NOT HAVE DETAILED VULN. KNOWLEDGE FAILURE TO DEVELOP "OPTIMIZED" SIGNATURE MGMT. PLAN RED

Army needs to develop technology - **RED**
 Army needs to apply COTS/GOTS - **PINK**
 Technology exists- need to apply - **GREEN**

Information Dominance Panel

The Counter - countermeasure process is a rapidly paced activity where both the U.S. and our adversaries constantly examine each other's equipment, tactics, doctrine and operation to uncover weaknesses and vulnerabilities. Tactics or systems to exploit these vulnerabilities are then developed. It is critical that U.S. Army S&T and Intelligence communities be fully engaged in this critical activity to reduce the time cycle of counter-countermeasure. As the Army will rely on Information Dominance the potential leverage that a hostile force will gain by disrupting, denying, deceiving, degrading or destroying elements of the Tactical InfoSphere will be immense.

Therefore, we can expect a substantial attack against our information systems and sensors. Similarly it will be important for the Army effectively disrupt, deny, deceive, degrade or destroy hostile sensors, C4ISR and target acquisition systems. This will require a robust Army technology base to support rapid response to a broad spectrum of threats and countermeasure opportunities.

The tables above and on the following page describe the key S&T activities associated with this Protect & Counter cycle. Items in red require a totally dedicated Army effort. Those in pink are the efforts that can be accomplished with tailoring and application of COTS solutions. The items in green do not require additional technology development, but need application of the technologies to be developed into fielded systems.



Counter Technologies

(CONTINUED)



CAPABILITIES	SUPPORTING TECHNOLOGY	REQUIRED	USEFUL	DEAD END
RED ACTIVE CM / D.E. AGAINST SENSORS & C4	EO/IR JAMMERS RF JAMMERS, D.E. IO & OA	D4 / Hardening AGAINST ALL HOSTILE SENSOR USED FOR DETECTION, ID, TGT. ACQ.	SELECTIVE DEGRADATION OF NEUTRAL SENSING & ID SYSTEMS	NON-INTEGRATED SURVIVABILITY SUITES
COUNTERMINE	UAV BASED DETECTION, SMART MINE DECEPTION	SEARCH AT MANUEVER RATES WITH HIGH Pd, SMART MINES CRITICAL	NEUTRALIZE MINES, CLEAR MINES, BREACHMINES	CRITICAL ISSUE, NEEDS TO BE RESOLVED- MINES ARE KILLER OF ARMY VEHICLES
OFFENSIVE I.O.	NETWORK ATTACKS SENSOR DECEPTION C3CM SYSTEMS INFRASTRUCUTRE MAPS	D4 OF ALL HOSTILE IT AND SENSOR SYSTEMS TO INCLUDE INFRASTRUCTURE	SELECTIVE IO AGAINST NEUTRAL SYSTEMS TO SUPPORT DECEPTION OPS,	Allow Red unchallenged Use of their information systems
INTELLIGENCE KNOWLEDGE	NEXT GEN. FME COTS / GOTS DATABASE SIMULATORS / MODELS	TECHNICAL DATABASE TO SUPPORT VULN. ASSESSMENTS	TECHNICAL CHARAC. OF WESTERN COTS / GOTS SYSTEMS EXPORTED	CURRENT INTELL S&T DOES NOT SUPPORT RED
IO ATTACK ASSESSMENT AND RESPONSE	ATTACK RECOGNITION ATTACK RESPONSE	RESPONSE TO IO ATTACKS WITHIN BATTLEFIELD TIMELINES	SUPPORTS PEACETIME ATTACKS	CURRENT RESPONSE PS HANDLED AS LE DENYS DEVELOP OF WAR RESPONSE MODE

Army needs to develop technology - RED
 Army needs to apply COTS/GOTS - n/a on this chart
 Technology exists- need to apply- n/a on this chart

Information Dominance Panel

The capabilities described in these charts are supported by a multitude of technologies. For example, the capabilities of Counter Space include many of the counter surveillance technologies as well as potential lethal attack options. Details of the specific technologies are beyond the scope of this report, but need to be assessed and a road map developed as part of the overall FCS solution.

APPENDIX J

SYSTEMS ENGINEERING

AND

INTEGRATION

APPENDIX J

Research, Development and Acquisition

Fielding the Tactical InfoSphere to the Objective Force demands major initiatives for research, development and acquisition (RDA). This Appendix addresses the engineering, interoperability and management challenges that must be overcome to develop the Tactical Infosphere.

Tactical InfoSphere RDA

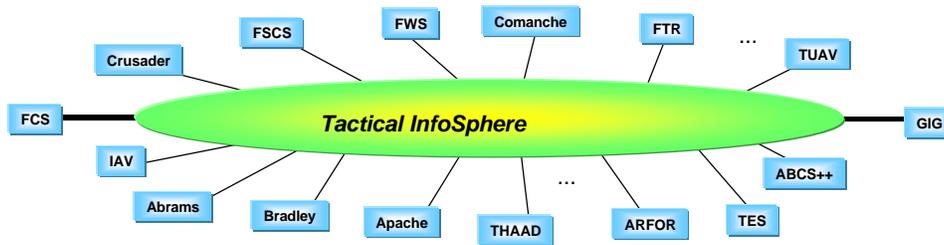
The Unprecedented Levels of Integration Necessary for Objective Force Platform and C4ISR System-of-systems Demand Expanded and New Enterprise-wide Organization and Processes for RDA and Requirements

- **Operational Architecture and Requirements** - Prescribe warfighter needs, and establish acquisition priorities
- **Systems Engineering** - Conduct the architecture design, systems engineering and systems integration throughout S&T and development
- **Commercial-Based Acquisition Strategy** - Plan an acquisition approach focused on leveraging commercial technologies and processes
- **Models, Simulations, and Test Beds** - Provide environments for exploring and developing the Tactical InfoSphere
- **Vulnerability Assessment** - Employ an independent Red Team to challenge the Blue Tactical InfoSphere throughout its lifecycle

The Tactical InfoSphere must be implemented using a wide-variety of technologies and systems. The systems will support functions carried out in today's Tactical Operations Centers and on-board weapon platforms. The magnitude and scale of the systems that must be integrated into the system-of-systems for the Tactical InfoSphere demands a level of integration never before achieved in a tactical ground system. The integration challenge will be unprecedented, even when compared to those undertaken for Army XXI digitization. All relevant organizations throughout the Army must be marshaled into new enterprises and processes must be put in place for collaborative efforts. Additionally, the requirements process must be applied in a holistic and consistent manner to enable the materiel developer to meet user needs.

Introductory slides depict broad challenges and recommendations for managing the Tactical InfoSphere's system-of-systems development. Recommendations are presented for systems engineering, operational architecture and requirements, commercial-based acquisition strategy, models, simulations, and test beds, and vulnerability assessment. Responsibilities for accomplishing the priority efforts are also recommended.

Tactical InfoSphere System-of-Systems Challenge



Nature of the Problem

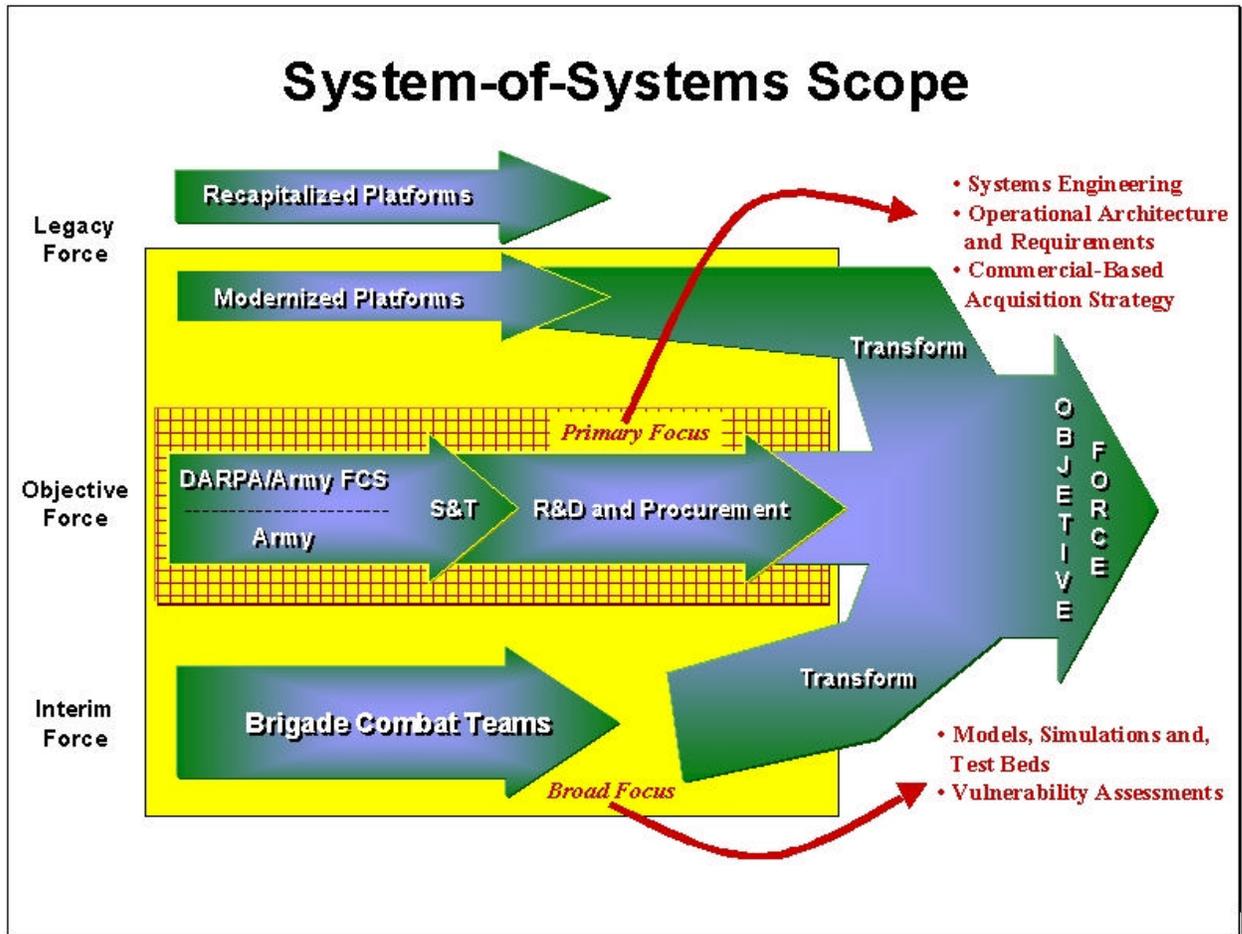
Tactical InfoSphere will include:

- C4ISR for each weapon platform (e.g., FCS, Crusader, FSCS, ...)
- Each C4ISR system (e.g., ABCS++, TUAV, TES, ...)
- Composite of Objective Force weapon and C4ISR systems
- Integration with the GIG
- Interfaces to legacy platforms

A holistic management approach with enabling processes and strategies is needed to cohesively unite all elements of the Tactical InfoSphere

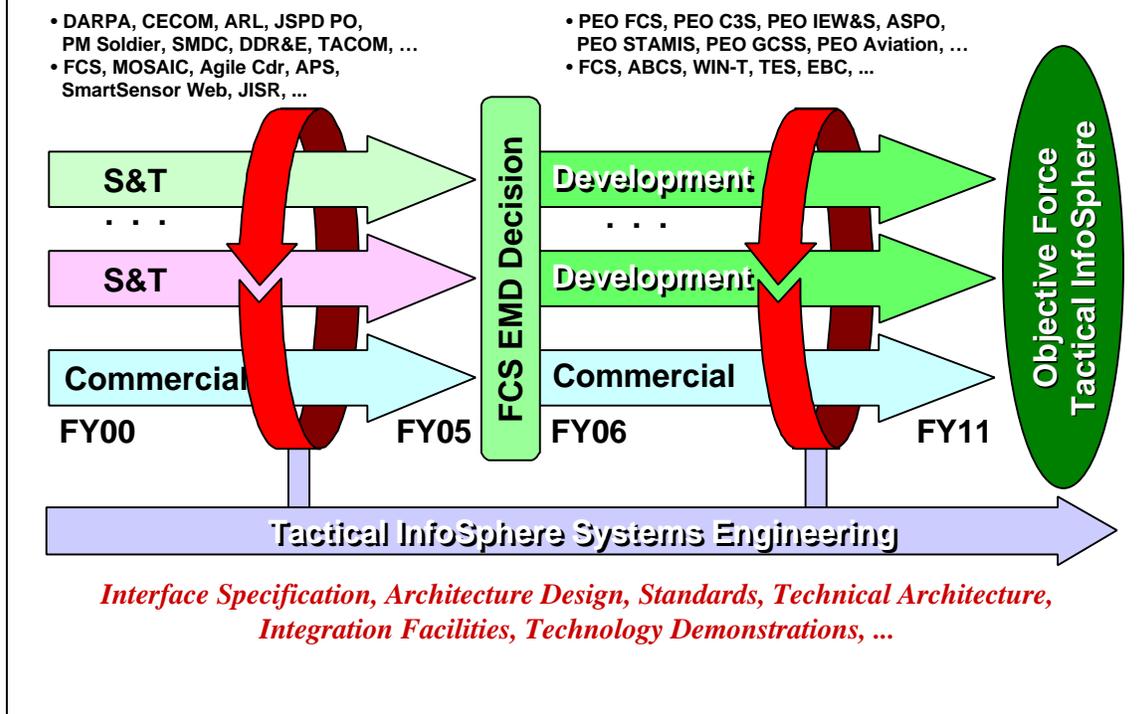
The Tactical InfoSphere must integrate every C4ISR system available to the Objective Force. Embedded C4ISR capabilities on-board each weapon platform will be nodes of the Tactical InfoSphere. The computers, communications, networking and sensors on-board FCS vehicles, Crusader, Future Scout and Cavalry System (FSCS) and other platforms will be included in the Tactical InfoSphere. Program managers for these weapon platforms must cooperate in enabling the Tactical InfoSphere. C4ISR systems and platforms will include the next generation Army Battle Command System (ABCS), Tactical Exploitation System (TES) and Unmanned Aerial Vehicles. PEO C3S, PEO IEW&S, and Army Space Program Office will be major players in the Tactical InfoSphere cooperative. Digitization lessons learned have highlighted the need to deliberately plan for the C4ISR system-of-systems comprised of all weapon platform and C4ISR systems. Objective Force access to and interoperability with Joint and coalition forces will be accomplished through the GIG. Seamless integration of the Tactical InfoSphere and the GIG is crucial. Units provided with the communications, information management, RSTA, UAV, counter C4 and PNT capabilities previously recommended must be able to interoperate with legacy systems. Developments for the Tactical InfoSphere must accommodate a minimum level of interoperability without demanding upgrades to legacy systems.

The current Army RDA organization involves many independent PMs and other organizations which develop the individual systems that will comprise the Tactical InfoSphere. The potential for ten or more organizations providing major systems for the Tactical InfoSphere presents a formidable management challenge unmatched in scale or magnitude. A holistic management approach with enabling processes and strategies is needed to cohesively unite all elements of the Tactical InfoSphere.



The scope of RDA efforts to establish the Tactical InfoSphere must be focused on the Objective Force, but must also accommodate interoperability with the legacy and Interim Forces. The above figure morphs the Transformation process chart promulgated by the CSA to accommodate the development of the Tactical InfoSphere.

Systems Engineering Efforts Must Orchestrate S&T and Developments



System engineering orchestration is crucial for science and technology (S&T) for FCS planned in FY00 through FY05 and for FCS engineering, manufacturing and development (EMD) planned in FY06 through FY11. Systems engineering will support the identification of interfaces, design of systems architecture, selection of standards, definition of a technical architecture, development of integration facilities, and conduct of technology demonstrations. There should be a consistent team effort to conduct systems engineering throughout these phases. The TI will require the same level of effort.

Systems engineering is needed immediately to orchestrate on-going Army and DARPA efforts that can support science and technology (S&T) for the Tactical InfoSphere. S&T efforts that reduce risks in technologies for the Tactical InfoSphere are being sponsored and conducted by: DARPA offices, CECOM RDEC directorates, ARL, Joint Precision Strike Demonstration Project Office, PM Soldier, Space and Missile Defense Command, Director of Defense Research and Engineering, Tank and Automotive Command, and others. Relevant programs and projects include FCS, MOSAIC, Agile Commander, active protection system, SmartSensor Web, and Joint ISR.

After the FCS EMD decision at the end of FY05, Army Program Executive Officers (PEOs) and PMs will commence FCS EMD that should yield the Tactical InfoSphere. EMD will result in a first unit equipped (FUE) in FY12. PEOs for FCS, C3S, IEW&S, ASPO, STAMIS, GCSS, Aviation and others may contribute to the fielded Tactical InfoSphere. These organizations will produce systems for FCS, such as: FCS, and the next generations of ABCS, WIN-T, TES and EBC.

Systems Engineering Will Focus Enterprise Efforts

- **Conduct architecture design, systems engineering and systems integration**
 - For Tactical InfoSphere, alternatively for all Objective Force systems
- **Orchestrate collaborative RDA efforts**
 - DARPA, RDEC, PEOs/PMs, HQDA staffs, TRADOC, DARPA, and others
 - Budget influence/control (potential)
- **AAE authority supported by a dedicated organization**
 - Options for host organizations: CECOM RDEC, consolidated PEO, HQDA
 - General office-level director with staffs for technology and resources
 - Tactical InfoSphere GOSC
 - Supplement by outsourcing to gain cutting edge expertise in commercial technology and processes
- **Alternative: Combine relevant PEO responsibilities (from C3S, IEW&S, GCSS and Aviation) into PEO Tactical InfoSphere**

The System Engineering organization will be responsible for designing working system architecture and orchestrating collaborative RDA efforts across several key Army organizations. To be effective, the Systems Engineering organization must have AAE authority and be supported by a dedicated organization. The scope of this organization needs to encompass the Tactical InfoSphere supporting the FCS as a minimum, but the scope should be expanded to include all of the Objective Force systems.

The current Army structure would lead to independent parallel developments accomplished by multiple PMs. Today's process is stove-piped with a fragmented system and organization responsible for requirements, acquisition, and science and technology causing interoperability issues in the system of systems. There is a complex set of requirements and is further complicated due to the potential interface needs to legacy systems. The Tactical InfoSphere is dependent upon rapidly developing commercial technology advances and, unless changes are made, it will be using the traditional DoD milestone driven acquisition process. In addition, the Army currently has little simulation capability for C4ISR and is required to support the Joint Forces interoperability requirements. Finally, there is currently little expertise and experience across the Army for building such a complex system of systems.

There are innovations that can be used to address these issues, but the key to success is to establish a Tactical InfoSphere Systems Engineering organization that can leverage successful approaches and innovations to ensure a robust working system is developed for the Objective Force. This Systems Engineering organization must have the following capabilities: technical expertise, integration facilities, Joint systems and operations, commercial technology insertion, and it should be broad and deep in full spectrum of C4ISR area expertise. They will need to take advantage of key innovations, such as, the Single Integrated Air Picture (SAIP), open systems architectures, the Global Interface Grid (GIG), Internet Protocol (IP) with voice data and video, spiral development models, a central technical and support facility, integration labs and modeling and simulations

The Systems Engineering organization will conduct the architectural design, perform the system engineering tasks and the systems integration for the Tactical InfoSphere, at a minimum. The scope could be expanded to address the total Objective Force systems. The system engineering tasks will include planning, defining interoperability requirements, perform configuration management, establish technical standards, define and conduct trade studies and perform vulnerability assessments.

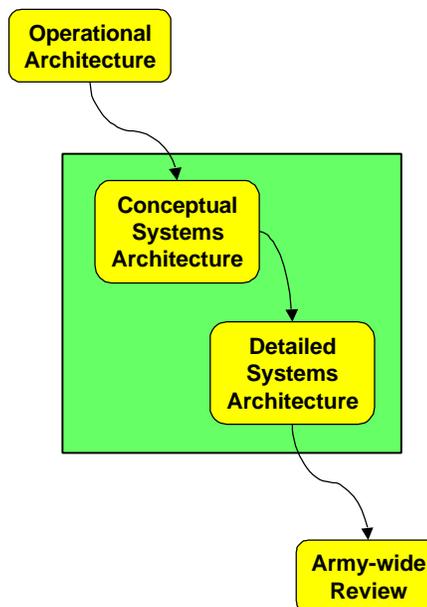
A key responsibility of the Systems Engineering group will be to orchestrate collaborative RDA effort among the cognizant PEOs and their PMs, the HQDA staffs, TRADOC, DARPA and others. The Army should seriously consider giving the Systems Engineering organization significant budgeting influence or control to ensure that they have the proper level of leverage needed to be successful.

The Systems Engineering organization requires AAE authority with support of a dedicated organization. There are several options for the host organization, such as, HQDA or CECOM RDEC. It should have a general office-level director with staffs for technology and resources. And, due to the significant commercial content of the system and the dependency on commercial technology, the organization must be supplemented by outsourcing in order to acquire key resources to gain cutting edge expertise in commercial technology and processes.

An alternative to establishing a separate Systems Engineering Office would be to combine the relevant PEO responsibilities from C3S, IEW&S, GCSS and Aviation into a super PEO, e. g., PEO Tactical InfoSphere. The issue is that this organization could be so large that it would require increased levels of management that tends to create more bureaucracy and slows down the processes. In addition, the Systems Engineering organization needs to be established immediately during the S&T phase of the Tactical InfoSphere definition where the PEOs do not need to engage until later in the development schedule. It is imperative that the Systems Engineering group is empowered to move quickly and that it has adequate resources.

Operational Architecture and Requirements

- **Prescribe warfighter needs for the Tactical InfoSphere in accordance with the C4ISR Architecture Framework**
 - Initiate developments now to support follow-on systems architecture development
 - Focus on critical mission threads
 - Provide Army enterprise drafts for comments
 - Include: DARPA, FORSCOM, contractors and others
 - TRADOC responsibility
- **Establish and prioritize requirements**
 - Provide clear guidance to minimize technology gaps for EMD
 - Commence acquisition planning and scheduling
 - TRADOC and HQDA DCSOPS



An operational architecture for the Tactical InfoSphere is needed which will support development of systems architecture. The operational architecture must evolve throughout S&T activities to accommodate evolving organizational and operational concepts. New concepts from the DARPA/Army FCS program and from TRADOC should be reflected in the operational architecture. The operational architecture must formally prescribe warfighter use of the Tactical InfoSphere technical capabilities. Normally TRADOC is responsible for assigning developments of operational architecture and should consider establishing a team with membership from TRADOC, FORSCOM and CECOM RDEC to include domain knowledge of operational concepts and technology. The operational architecture provides detailed warfighter needs or “requirements” for systems architecture development by the systems engineer. The system engineer will use the operational architecture to support development of conceptual systems architecture during S&T. The systems engineering will provide the operational architecture and conceptual systems architecture to PEOs for EMD. Development of the operational architecture should be initiated immediately to support on going S&T. To support rapid development, the operational architecture should be developed in multiple drafts of increasing detail. Focus should be on critical mission threads, rather than comprehensive tasks that may get modified with evolving concepts. The operational architecture drafts should be provided to the enterprise of Tactical InfoSphere organizations (e.g., DARPA, FORSCOM, and contractors) for review and comments.

Established and prioritized requirements are considered during the approval and funding of S&T and EMD programs. TRADOC and HQDA DCSOPS are responsible for establishing and prioritizing requirements. These organizations need to continue examining requirements for the Tactical InfoSphere to provide clear and unambiguous guidance to the Army S&T community which is currently realigning its programs to FCS. Established and prioritized requirements will support assessment of planned C4ISR S&T programs for their relevance to the Tactical InfoSphere. Gaps in the S&T programs can be filled based on the understanding of requirements. The evolving operational architecture can also be used with

requirements in assessing on going S&T projects. Acquisition planning and scheduling should commence to support technology demonstrations.

Recommendation: Commercial-Based Acquisition Strategy

- **Tactical InfoSphere environment:**
 - Must be robust enough to support a 25+ year lifecycle
 - Capitalize on commercial hardware/software technology
 - Commercial lifecycle is an order of magnitude shorter than DoD's
 - Out of production parts, evolving commercial standards and technically obsolete equipment will be a continuous problem.
- **Approach**
 - Use an open architecture with abstraction, intelligent and real time adaptable interfaces and no proprietary communication networks.
 - Use Internet Protocol as the architecture baseline.
 - Plan each system element with minor and major technology insertions using spiral development
 - Include architecture baseline upgrades to adopt, if prudent, the next generation Internet Protocol
- **AAE should assign responsibility for formalizing and institutionalizing strategy**

It is critical that Tactical InfoSphere is able to support our Army for a minimum of 25 years. This is a significant challenge because of the system will be based on commercial standards and capabilities with commercial software and hardware. The technologies needed to create a robust Tactical InfoSphere are commercially available and the Army will need to take advantage of the commercial capability to reduce cost and to meet the stated needs in a timely manner. But, the commercial life cycle is an order of magnitude shorter than the Army life cycle. The Tactical InfoSphere must be acquired and designed to minimize any negative impact from speed of the commercial cycle and, instead, use it as a competitive advantage. The speed of the Army's Objective Force is the one of the most critical factors to its success.

The challenge to create a communications network that is robust and capable of evolving as technology evolves is not unique to the Army or the DoD. All corporations and institutions are very dependent upon their information technology systems and networks and are dealing with increasing requirements and the need for speed. Bandwidth continues to be strained due to the increasing appetite of all the users for voice, data and video in real time and with high quality images. The commercial world is also challenged by the issues of balancing cost, demand and competitive advantage. The Army can use commercial approaches and strategies to take on this challenge as it system engineers the Tactical InfoSphere.

The System Engineering organization, which must include highly qualified leading edge commercial system engineers, will need to first establish the principles required to ensure that the Tactical InfoSphere is robust and able to quickly take advantage of technology upgrades where prudent. The commercial world has also had to address these issues and has developed architectural approaches that are supported in both hardware and software. The use of open systems architectures which uncouple system elements though the use of abstraction and intelligent, real time adaptable interfaces are critical. The first year of this development needs to be spent focusing on the specification of the architectural design and principles.

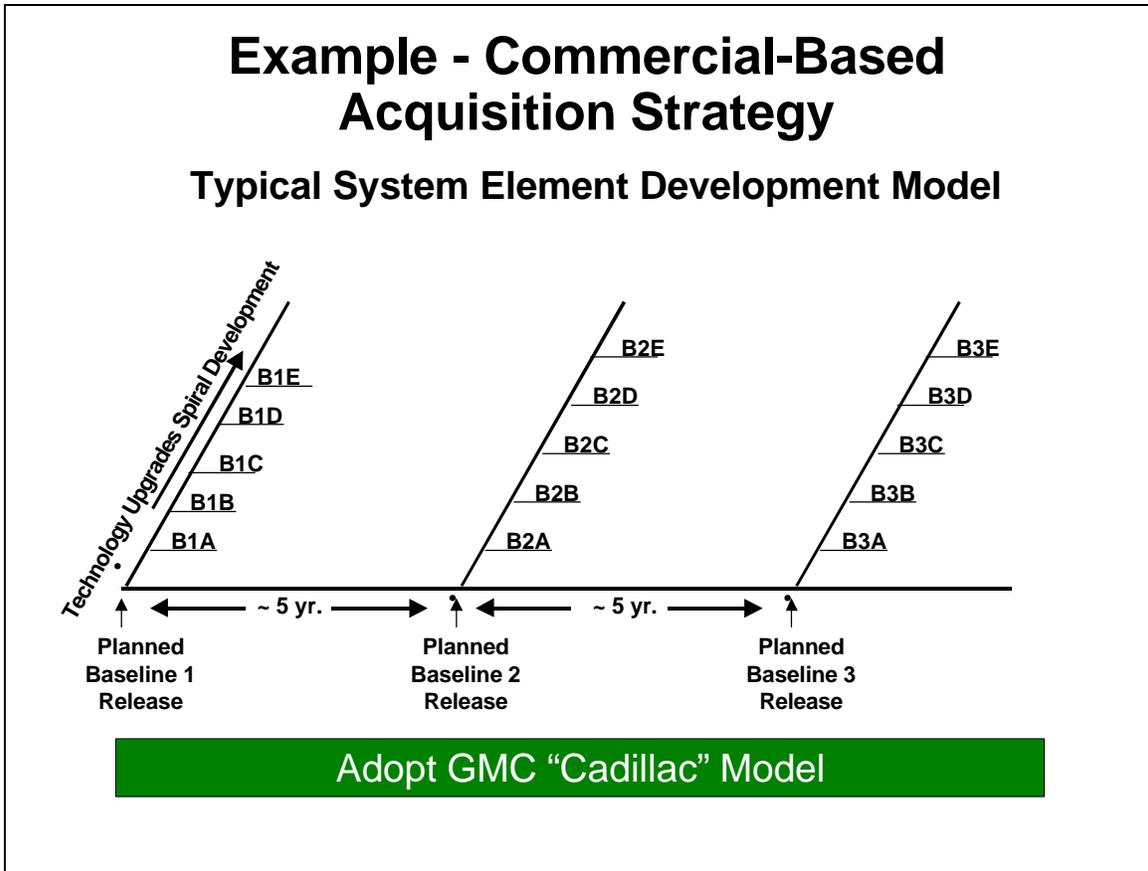
This will be the key to making the Tactical InfoSphere increase its useful life span and easily address needed technology upgrades. The Internet Protocol has become the defacto standard and commercial innovations have led to both hardware and software products that will allow this architecture to handle voice, data and video. The timing of the development of the Tactical InfoSphere is well suited to take advantage of this progress.

The Tactical InfoSphere is composed of many system elements and will be connecting a system of systems. The system elements will require both minor and major technology upgrades to meet increasing needs and keep the system from becoming technically obsolete. The defacto standards evolve over time and the Army must be prepared to make baseline changes to the system elements as commercial capabilities are developed and made available. It is predictable that the Internet Protocol will evolve into either enhanced Internet protocol or an innovation will be made to a brand new protocol that becomes the commercial standard. The Systems Engineer will need to manage both minor and major technology insertions and make decisions as to whether to upgrade the system and when it should be done. But, if the Army is not able to keep up with the commercial pace, they will be dealing with severe problems of out of production parts and obsolete communications equipment. This could be more expensive than the investment needed to keep technically current, as well as, decrease the competitive advantage that the Army has in the field.

The AAE should assign responsibility for formalizing and institutionalizing a strategy to be adopted for the Tactical InfoSphere and all of its system elements

Example - Commercial-Based Acquisition Strategy

Typical System Element Development Model



A system development model that is being widely used in industry to manage product development for competitive advantage is one which uses planned platform baseline upgrades and allows for minor technology upgrades to be inserted within a platform baseline. The platform baselines are planned for periodic releases and the system engineers are responsible for deciding whether a desired technology upgrade can be addressed within the current baseline or if it needs to be included in the next baseline release. This strategy is critical to both keeping competitive advantage and meeting necessary release timelines.

Many automobile manufacturers use this model for managing their model year car releases. Cars are becoming high technology platforms with many complex digital systems. They plan for a specific car model platform to be kept for several years and during that time frame they are designing the next platform. They are very careful to not introduce new technology or systems into a platform that has not been structured to support it. A significant change or new system will be targeted for the next platform, avoiding technical and reliability problems in the existing platform. Of course, if changes are not managed well, the car model will not be released in time for the model year resulting in lost business. Designers must also stay technically current and deal with obsolescence.

An excellent example of this is GMC Cadillac's Product Development strategy for the 2000 DeVille. Cadillac wanted to introduce a Night Vision system to its Cadillac line, but it required that a Heads-Up Display be inserted into the dash. They could not accommodate this technology/design change within a platform release as an annual upgrade feature due to the architecture and design impact to the current platform. They had to wait to include this feature until a platform upgrade year to minimize the impact on the model year since the dash had to be redesigned. The Army will need to have a similar integrated platform baseline upgrade plan for each system element of the Tactical InfoSphere and closely manage any minor technology insertions between platform releases. And, it needs to start during EMD, not after.

The typical EMD is so long that there can be multiple commercial technology cycles during the EMD phase.

This product development model is well documented in two books written by Dr. Steven C. Wheelwright and Dr. Ken Clark, Harvard Business School professors, called Revolutionizing Product Development and Managing New Product and Process Development.

Models, Simulations, and Virtual Test Beds

- **Initiate activities to incorporate all elements of C4ISR into combat models supporting FCS and Objective Force analysis**
 - Example models: JANUS, VIC, and CASTFOREM
 - Develop appropriate measures
- **Modify/expand/create simulations and test beds with virtually-linked C4ISR elements to support soldier - in - the - loop investigations**
 - Example simulation: Close Combat Tactical Trainer (CCTT)
- **Develop a Tactical InfoSphere Simulation Support Plan**
- **Create a 'Central Technical Support Facility'-like capability to forge system-to-system interoperability**
 - Explicitly include ISR capabilities
- **DUSA(OR) should assign these responsibilities**

The complex and inter-dependent nature of the elements of the Tactical InfoSphere present a daunting engineering challenge. In order to capture the contributions and effectiveness of Blue's C4ISR Infrastructure, models and simulations that allow for Objective Force analysis must incorporate detailed and accurate functional representations of the systems that comprise the Tactical InfoSphere. JANUS, VIC and CASTFOREM, as well as models used by the other services do not adequately capture the essence of the essentiality of C4ISR to combat operations in the Objective Force timeframe. Thus these models should be enhanced to reflect C4ISR's role in combat effectiveness. Furthermore, measures that can relate the value of C4ISR contributions to other offensive and defensive Objective Force systems must be developed and evaluated.

Simulations and test beds such as the Close Combat Tactical Trainer need to be developed, and/or modified to capture the functionality of the Tactical InfoSphere. These test beds can be distributed among various locations, but should be virtually linked to provide system of systems insights. For example, virtually linking test beds to refine sensor to shooter command and control timelines, or to robustly broadcast NBC warnings to the Objective Force should be enabled by the creation of flexible links among these test beds and simulations.

Simulation Support Plans are required elements of all major acquisition programs. For the Tactical InfoSphere, this plan should be developed by the Systems Engineer, in advance of the decisions to acquire individual elements of the Tactical Internet. This will support early definition of the simulation challenges and opportunities inherent in the development of the Tactical Internet. By giving the Systems Engineer authority to develop the Simulation Support Plan, early identification of C4ISR modeling and simulation shortfalls can be developed.

The Central Technical Support Facility, established at Ft Hood in support of Force XXI digitization activities, has proven to be a successful means to facilitate communications interoperability solutions. This concept, when applied to the Tactical InfoSphere, must be expanded to address Reconnaissance, Surveillance and Target Acquisition systems, but is vital to successful development. Therefore, creation of a similar capability to that established at Ft Hood is recommended. The Army should co-locate this facility with the Bn Test Bed called for in this report.

To guide the implementation of these recommendations, the DUSA (OR) should be given responsibility for -- and funding authority over -- these actions.

Vulnerability Assessments With Independent Red Team

- **Independent organization to challenge the Tactical InfoSphere solutions during entire lifecycle**
- **Technical assessments of weakness and vulnerability of all C4ISR**
- **Support Functions:**
 - Advise & Challenge “System Engineer” , Developer, User
 - Advise on tactics to counter & protect
 - Advise acquisition Decision Makers
 - Collaborate on realistic training (e.g. with OPFOR, Battlelabs)
 - Improve offensive & defensive IO with technical assessments
- **DCSINT, DISC4 and DCSOPS should assign these responsibilities**
 - The ARL, Survivability, Lethality and Analysis Directorate (SLAD) is capable of becoming the core of this activity

The “red team” activity must be independent. It cannot either report to the developer or have to rely on the developer for funding. Funding for the Red team and the oversight/prioritization of Red team tasks is a critical aspect of the organization. The ASB recommends a senior level HQDA steering/review group consisting of the DUSA(OR), ASA(ALT), and as appropriate DCSOPS, DCSINT, and DISC4. Although the Red Team must be chartered by and its work prioritized by HQDA it is not mandatory that the Red Team report directly to HQDA—as long as it is **sufficiently isolated** from influence by the developer and user by management and funding.

The primary responsibility of the Red Team is to identify and assess the weakness and vulnerability of all C4ISR elements, whether embedded in a combat system, or a sensor or command and control system. Simultaneously challenging and then helping:

- the “*System Engineer*”, and materiel developer identify and correct vulnerabilities during the design process;
- working with TRADOC to develop tactics to minimize the effects of remaining vulnerabilities;
- supporting acquisition decision makers to ensure they know the limitations and capabilities of the systems;
- providing the capability for realistic training in a challenging Information Operations environment; and
- Providing feed back to US offensive Information Operations developers the identified vulnerabilities of COTS/GOTS systems.

Today the ARL, Survivability, Lethality, and Analysis Directorate (SLAD) is capable of becoming a core of the needed “Red Team” activity. Independent funding along with an expanded and independent charter to challenge the “Objective Force” C4ISR and related elements needs to occur. The Army will then have an excellent foundation to develop the Tactical InfoSphere, ensuring battlefield Information Dominance.

Building the Tactical InfoSphere: A Serious Management Challenge

The Army will need:

- **A systems engineer responsible for architecture design, systems engineering and integration for S&T and development - AAE**
- **An operational architecture and established requirements - TRADOC, HQDA DCSOPS**
- **A flexible acquisition strategy focused on leveraging commercial technologies and processes - AAE**
- **Models, simulations, and virtual test beds with a Central Technical Support Facility to examine concepts, experiment, and address information usage and decision times - DUSA(OR)**
- **An independent Red Team to validate the Tactical InfoSphere throughout its lifecycle - DCSINT/DCSOPS/ DISC4**

Management challenges inherent in the development of such a complex system of systems may present the Army with more difficulty than the technical aspects of creating the Tactical InfoSphere.

The Army Acquisition Executive (with support from DA DCSOPS) should rapidly determine the composition and structure of this system engineering organization, to allow it to conduct the planning activities needed to create the Tactical InfoSphere. The entailed focus should be on establishing a preliminary Systems Architecture to help focus the S & T programs.

Deploying a Tactical InfoSphere will help the Army to overcome the inherent information advantages that our adversaries enjoy from fighting on their own ground. To do so with the Objective Force, new concepts and requirements must emerge from TRADOC and be vetted by HQDA to enable Army forces to operate to the potential that the Tactical InfoSphere's new technology and systems will allow. TRADOC must create an Operational Architecture for the Objective Force that exploits the potential of the Tactical InfoSphere.

The Army Acquisition Executive must insure that the Army adopts commercial standards, approaches and strategies in the development and acquisition of the Tactical InfoSphere. The AAE should institutionalize this commercial development model to enable the Tactical InfoSphere to evolve rapidly as new technologies merit incorporation.

The Deputy Under Secretary of the Army, Operations Research, should be assigned oversight responsibility for the development and modification of Army models, simulations and test beds, to include a Central Technical Support Facility, needed to analyze and develop the Tactical InfoSphere.

Lastly, an independent Red Team activity should be chartered to challenge the robustness of the Tactical InfoSphere to a range of threats. By conducting vulnerability assessments, while working in concert with

the Systems Engineer and systems developers, this organization can help ensure the viability of the Tactical InfoSphere across the threat spectrum.

APPENDIX K

TECHNOLOGY ASSESSMENT

Appendix K
Technology Assessment



Technology Assessment to Support Objective Force Capabilities



Core Capability	Technology	EMD Risk (Tech Readiness Level \geq 7 at FY2006)		
		Required	Technology	Programmatics
Info Mgmt	Intelligent Data Mgmt	<input checked="" type="checkbox"/>	Green	Yellow
	Common Operating Picture	<input checked="" type="checkbox"/>	Yellow	Yellow
	Human Machine Interface	<input checked="" type="checkbox"/>	Yellow	Red
Comm	Secure Mobile Networks	<input checked="" type="checkbox"/>	Green	Yellow
	Radios (DSP, waveforms, networks, etc.)	<input checked="" type="checkbox"/>	Yellow	Red
RSTA	EO, IR, Radar, RF, LIDAR Sensors	<input checked="" type="checkbox"/>	Green	Yellow
	Micro-acoustic, seismic, etc. Sensors	<input checked="" type="checkbox"/>	Green	Yellow
	Sensor Fusion – deconflict, Template	<input checked="" type="checkbox"/>	Green	Red
	Multi Sensor Fusion		Red	Red
	ATR-Detection and Recognition	<input checked="" type="checkbox"/>	Yellow	Red
UAV	Long Endurance	<input checked="" type="checkbox"/>	Green	Red
	Medium Endurance		Green	Yellow
	Mini/Micro		Yellow	Red
Pos/Nav	Receivers	<input checked="" type="checkbox"/>	Green	Red
	Antennas	<input checked="" type="checkbox"/>	Green	Red
	Pseudolites	<input checked="" type="checkbox"/>	Green	Red
Counter & Protect	Counterspace		Yellow	Red
	Information Assurance	<input checked="" type="checkbox"/>	Yellow	Yellow
	Sensor CM (RSTA)	<input checked="" type="checkbox"/>	Green	Yellow
	Offensive I.O.	<input checked="" type="checkbox"/>	Yellow	Red
RDA	Modeling, Simulation and Test Beds	<input checked="" type="checkbox"/>	Yellow	Red

Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015-2025 Era

Page 1

InfoSphere Management

Brief Definition of the Technology Area

We define InfoSphere Management as *the design, manipulation, and control of information throughout its life cycle in order get the right information to the right person at the right time to facilitate better decision-making*. In short, employing, managing, and monitoring the InfoSphere and its connections to the Global Information Grid will be unlike anything the Army or commercial industry has ever experienced. We cannot state strongly enough that providing information is only part of the requirement of InfoSphere Management. Designing systems to optimally use the information provided by the InfoSphere and the GIG are equally important as, if not more important than, designing systems to manage the flow of information.

As stated in *The Army Vision*, the essence of command will remain unchanged; however, the staggering amounts of information that will be available to commanders and their staff will necessitate new systems to manage and utilize this information. In addition to hardware and software systems that will be needed to manage the InfoSphere, the design of the commander’s staff should also be reengineered to take advantage of the InfoSphere. The InfoSphere must allow planning processes that are parallel and collaborative, to include the concept of a *virtual staff*. Technologies, such as white-boarding and collaborative decision support systems are currently available in rudimentary form, and these systems will continue to evolve over the timeframe of this study.

InfoSphere managers will be required to create information support packages for the tactical commanders. This process will require innovative software that will recommend an appropriate system configuration and configuration changes that will occur rapidly as the battle situation evolves. Additionally, InfoSphere

Managers will have to dynamically prioritize the information content, particularly within moving echelons where available bandwidths will be much smaller than at the higher echelons where land lines and fiber optics will be extensively used.

The presence of the InfoSphere and its tie to the Global Information Grid must be as transparent as possible to the Commander and staff. This will require exceptionally well-qualified personnel that understand both technology and the Military Decision Making Process. Additionally, there will exist a strong need for security, both in the traditional and information assurance areas. Since enemy penetrations of databases and communications links would have far reaching and disastrous effects, the security responsibility of the InfoSphere Manager will require monitoring of software and hardware systems for suspicious behavior, as well as oversight for security policy determination and implementation.

Rationale for the Technology Maturity Score

InfoSphere Management, as an Army functional area or academic discipline, simply does not exist. The technology needed to build and manage the InfoSphere should be available within the timeframe of this study. Intelligent data management tools, plug and play hardware, intelligently configurable systems, smart routers, and thin clients are all devices that will continued to be developed by the commercial industry and adapted for battlefield use. Data fusion tools, however, and methodologies required to create a common picture of the battlefield will not be developed by industry. In fact, the requirement for a system that integrates all information sources into one common picture will probably not be realized within the time frame of this study, and it is strongly recommended the overzealous definition of the commanders' information needs be reassessed.

Evidence that the program is not currently supported

Probably the single biggest indicator regarding the lack of support given to InfoSphere Management is the Army personnel management system. The Army has not figured out how to retain qualified, technologically competent enlisted personnel, warrant officers, officers, and civilians. The Army Acquisition Corps is almost completely void of officers with technological backgrounds; rather, the Army has opted to staff the Acquisition Corps with product managers. Promotion rates for officers in technology fields are usually lower or at best equal to the average promotion rates. If the Army does not address the personnel problems associated with the technology fields, there will no soldiers to manage the InfoSphere.

Further evidence regarding the lack of support for InfoSphere Management is the fact the Army and its staff is not configured to take full advantage of the InfoSphere and GIG. Large amounts of money have been spent automating the way the Army did business in the past rather than looking at new ways of implementing and managing the InfoSphere. For example, the Army Battle Command Systems still mirrors traditional staff functions, and the information flow between different-type systems is limited if it exists at all. In order to make a successful transition from our legacy systems to the Tactical InfoSphere, we must conduct a thorough, detailed scrub of the requirements within each battlefield functional area. The implementation of FBCB2 is a stopgap measure and further evidence InfoSphere management is minimally supported.

Communications

Brief Definition of the Technology Area

Current Army C4ISR systems are a highly complex collection of stovepipes supported by a myriad of communications systems normally designed to meet very specific requirements. The result is information exchange through point-to-point connectivity, fixed services and pre allocated resources, which results in inefficient use of bandwidth and radio frequency spectrum. The goal of the Tactical InfoSphere is to

provide a military capability equivalent to the merger of the wired Internet with PCS wireless technology which is taking place today in the commercial world.

Two distinct areas, however, distinguish the requirements for the Tactical InfoSphere from the commercial capability. First, the security requirements for the military far exceed what is envisioned for commercial wireless. Secondly, the commercial wireless industry operates off of a fixed infrastructure of fixed base stations that are unlikely to be available to an expeditionary force, in the area of operations. Thus the Army, based upon current and projected commercial technology, must engineer secure mobile networks as part of, and compatible with, the Global Information Grid (GIG).

Although the key to the Tactical InfoSphere is the ability to work communications capitalizing on the Internet Protocols, a vital mechanism for the transport of information through the network at the Brigade and Below level will be a new generation of tactical radios. Radios for the Tactical InfoSphere will need to be more "intelligent;" able to join and leave the InfoSphere at will and able to assist in the routing of information.

We assessed several radio technology areas necessary for the InfoSphere. The DOD has mandated that all future radios will be part of the Joint Tactical Radio System (JTRS) family. Thus the review and assessment of radio technology was made within the context of the JTRS program as it was briefed to the study team by the Joint Program Office, CECOM and the PM responsible for JTRS-Army acquisition. The JTRS will be multi-band, software programmable radios capable of operation in a frequency range of 30MHz-2.0GHz. Key technology areas for this next generation of radio capability are: Digital Signal Processors (DSP); the development of wideband waveforms to handle increase data rate requirements; network software to provide ad hoc mobile network capability, power management and efficient frequency spectrum utilization; multiband antennas and multiplexers; and wideband power amplifiers.

Rationale for the Technology Maturity Score:

The study team examined the availability of commercial wireless technology and the trend of technology development leading to convergence of PCS voice capability with data on the Internet. Given the billions being invested in R & D by the commercial sector and the rapid success achieved as of this report, there is little doubt that the Army can position itself to capitalize on this technology to achieve the secure mobile network capability required for the Tactical InfoSphere. Thus we have given a "Green" designation for the availability of the technology.

Programmatics:

The team was able to identify activities at CECOM and DARPA to indicate that programs were underway to engineer and adapt the available technology to satisfy the unique Army military requirements. The team was however concerned with the bare bones, single thread nature of these efforts which are critical if the TI is to be available in the target time frame. Thus, we have designated this category "Yellow" programmatically because additional funding resources should be applied to reduce risk.

Much of the basic radio technology delineated above such as DSP's will come from the commercial wireless industry. However the DOD JTRS program has requirements not yet envisioned by the commercial sector or the consuming public. Thus software development, multiplexers, multiband antennas, etc. will initially come from government sponsored efforts. The study team identified on-going programs at CECOM and DARPA in these areas in support of the JTRS JPO and concluded that they represented medium risk and were given a "Yellow" designation. Programmatically, however, the team was much less comfortable with the progress of the mainstream JTRS program that has responsibility to develop the radio architecture and the wideband waveforms. The team was concerned that program acquisition strategy, with emphasis on developing legacy waveforms prior to a full blown effort to develop the next generation ad hoc mobile networking wideband waveform, could jeopardize fielding of radios in the 2006 time frame. Hence the score for programmatics is "Red".

RSTA

Brief Definition of the Technology Area

Remote sensors used for collecting data from standoff platforms such as satellites, UAV's or a ground vehicle. These include the imaging sensor such as electro-optical sensors, infrared imaging sensors, laser imaging sensors and synthetic radars. They also include SIGINT collectors; radar ground moving target indicators, spectrometers, and interferometers. Unattended sensors require being in the environment being measured. Examples include the acoustic sensors, seismic sensors, and air sampling chemical spectrometers and weather sensors. The sensors form the basis for RSTA systems.

Sensor fusion refers to the combining of data from multiple sensors to produce an information product. The simplest fusion occurs in combining data from like sensors. An example of this is to combine track data from two or more tracking Radars at physically separated locations to form a complete track, to improve the accuracy of the track, or to avoid allocating redundant assets to respond to an alias of a tracked object. The more difficult challenge is to combine disparate data sets from multiple sensor types. An example of this is the combining of unit locations derived from imagery with RF emissions data using force templates to derive knowledge about the unit type and echelon. Most multi-sensor fusion occurs today with humans "analyzing" the data sequentially. To provide the real time knowledge that the future fighting force requires, it will be necessary that automated fusion of multiple sensors be accomplished.

Automatic Target Recognition (ATR) refers to the process of detecting and classifying targets using computers to process sensor data. This has been the "Holy Grail" for some time. Most of the efforts to date have been to "machine process" imagery. Complications include orientation, clutter and partial obscuration. More promising techniques involve a triage process – one sensor for possible "object of interest" detection, others to eliminate decoys, and yet possibly different data for classification. The required computing capability to solve this problem has only recently become available.

Rationale for the Technology Maturity Score

The technology base for sensors of all types is very great and growing rapidly. Many government organizations and industry are pursuing all aspects of sensor technology over the entire physical spectrum. It is almost the case that if there is a physical signal present it can be detected and measured – a relevant sensor technology is available. Hence the classification of the sensor technology as "green". Except for a few sensor areas such as FLIR the Army does not have strong programs for engineering and packaging sensors to meet the unique Army needs. The Army needs a comprehensive, integrated systems approach to RSTA development to support the Army's future fighting system. This area is too important to leave to the SPO as a "add on" after the future fighting system is developed. Hence the sensor area is classified as "yellow" programmatically.

Again, there is a large body of technology in the areas of deconfliction, templating and fusion of data from sensors of the same type. This technology continues to be pursued by many and the technology appears to be available to support the Army's needs. Hence the technology base is classified "green". On the other hand, the Board did not find any programs within the Army to implement this technology into Army systems supporting ground combat. This led to the programmatic classification of "red".

Disparate multi-sensor fusion has not received much support in the past. It has only recently become a topic of research for scientific applications. It is an emerging technology that holds great promise of providing the necessary battlefield awareness in support of the future fighting system. The Army has only embryonic research efforts underway. Hence both the technology and programmatics are classified as "red".

ATR has been an area of research for at least 20 years and is being pursued relatively vigorously. Recently programs at DARPA and elsewhere have shown some real progress and demonstrated possible solution areas. Multi-sensor fusion as mentioned above has only recently been recognized as a possible means of solving this very

difficult problem. For these reasons the technology readiness is classified “yellow”. The ASB found no evidence of a program in the Army to incorporate this technology into the force. Thus the programmatic has been classified as “yellow”.

In general, the Army does not treat RSTA as a major subsystem of the ground combat system. The approach is fragmented falling into multiple branches, SPO’s and organizations. The need for timely and accurate battlefield awareness based on automated RSTA is not really recognized. Hence, in an overall context the RSTA programmatic need to be considered as “red”.

UAVs

Brief definition of the technology area

UAVs fall into three operating zones: high flyers with the capability to fly autonomously at 55,000 ft or beyond; medium altitude flyers typically considered tactical UAVs operating in the 5,000 -15,000 ft altitudes; and low flyers in the 0 to 5,000 ft regimes.

Examples of high flyers are the USAF Global Hawk and the HELIOS electric powered platform. HELIOS is under development by AeroVironment Inc., with sponsorship from NASA. The high flyers will have the capability to support multiple functions within the context of C4ISR. Examples of this organic battlefield support are over the horizon communication, area sensing and staring, and satellite link. The high flyer UAVs will likely be joint assets linking information to multiple units in the battlefield.

The next tier of UAVs is the medium altitude flyer. The medium flyer is capable of supporting altitudes up to 15,000 ft. The USAF Predator is an example of this tier UAV. Another example of a UAV under development by DARPA is the long endurance Hummingbird A-160. The Hummingbird has as its goal to achieve a range of 4,800 Km, with on-station endurance in excess of 40 hrs. A medium altitude flyer will provide over the horizon sensing, but will also be able to focus its field of regard much precisely on valuable targets than a high flyer UAV. On the other hand, the high flyer UAV will be able to search a much larger field of regard region.

Finally, the lower tier of UAVs are Micro Air Vehicle (MAVs). These platforms operate at heights less than 5,000 ft. However, they would be maintained and launched at the level of a company and scout platoon. The troops can afford to lose several of them in battle due to their expendable design. Most MAV development is under the auspices of DARPA. MAVs can be used for both defense and attack. In a defense mode, the micro air vehicles will focus reconnaissance and surveillance over a much smaller region than either the medium or high flyers, but at a much lower latency providing information to the tactical fighter. In an offensive mode, the MAVs can carry small munitions and jam enemy electronics.

These altitude classifications correspond roughly to the endurance ratings from the Technology Assessment slide in the Information Dominance presentation.

Rationale for the technology maturity score

Technology maturity for the UAVs is simple. For the long endurance and the medium endurance UAVs, the technology to support the platforms is essentially the same at that that supports manned aircraft (autopilot, navigation systems, flight controls, and aerodynamics). The main improvements needed have been in flight planning and in autonomous navigation and control. These are essentially solved problems, since generations of UAVs have been flying since the Vietnam War.

The realm of MAVs is a new area of platform development. Progress has been made in the last several years of DARPA-sponsored research. These are not hobby aircraft, which have a wingspan approximately a foot or larger, these are aircraft with maximum dimensions in any direction of half a foot. This means parts available for the hobby market will not do. Electronics, flight controls, actuators, and other on-board systems have to be designed specifically for the platform. Flight stability and system weight constraints are particularly difficult problems. Technology maturity for the MAVs is yellow, as there are still missing pieces, such as small form factor inertial

guidance systems and micro turbine engines, but much of the supporting technology has already been proven and is available for use.

For long and medium endurance platforms, there is still development to be done for known limitations, such as sensor resolution and weight and cost reduction (or self-protection), but the technology for valuable mission application exists. The same cannot be said for the MAVs, where the lack of engines and stability control systems, still limits practical application. Much of the technology to support all classes of UAVs will come from developments in the commercial sector, but will need to be adapted for military uses (less commercial development will support the MAVs than for the larger, longer endurance platforms).

Evidence that the program is not currently supported

There is a long history of failure to support either a tactical UAV or MAVs for forward units. Successive failures in fielding a tactical UAV should point to the need for better strategy if the TUAV program is to be successfully. In the area of MAVs to support forward troops, the Army has had Pointer available for years, but has been unable to act to deploy readily available technology.

Pos/Nav/Time

Brief Definition of the Technology Area:

The DoD's Pos/Nav/Time capability is provided by a system-of-systems. The core of the systems mix is GPS. It provides global Pos/Nav service that is seamless, consistent, and uniform, as well as a precise global timing/synchronization standard. However, it is widely recognized that GPS has significant limitations in robustness (e.g., it is extremely vulnerable to adversary efforts to jam the system and to employ the system to satisfy their own needs for precision Pos/Nav/Time).

There are several potential actions that the Army should pursue in the near- and mid-term, in conjunction with the other Services, to ameliorate these deficiencies in GPS. First, to enhance resistance to potential enemy actions, enhance coverage, and compensate for the fragility of the GPS constellation, the system could be augmented with Psuedolites in a variety of basing modes (e.g., high altitude; low-to-medium altitude; ground-based). These Psuedolites would transmit more powerful GPS signals that are less susceptible to jamming. This technique is the only near-term, force-wide mitigation technology because it recapitalizes legacy equipment. CECOM and DARPA have demonstrated that most current receivers can be used with Psuedolites with only a software load to the receivers.

In addition to augmenting GPS with Psuedolites, there are several other technical means of enhancing the performance of GPS in a jamming environment. These include augmentation of GPS receiver equipment with A/J antennas, filters, and other A/J processing electronics. The primary antenna technologies of interest are controlled-radiation pattern antennas (CRPA). These are multi-element arrays that, when coupled with the proper electronics, can reduce reception sensitivity in the direction of the jammers. As an illustration, mini-CRPAs are being developed for USN aircraft that use 4" footprint, space-time Adaptive Processing (STAP), and beamforming. These new units would be compatible with Army vehicles and greatly enhance their resistance to jamming. In addition, various signal-processing techniques are being developed for use in next generation and notional receivers. For example, Frequency Domain Interference Suppression circuits have been developed for use in adaptive narrow-band filters for aircraft receivers. These units can defeat multiple first generation jammers. This technology is appropriate for hand-held users with A/J performance traded for battery life under jamming conditions.

Technology Maturity:

Although much work remains to be done to mature and transform these technologies into operationally suitable systems, there are no major technological barriers to either of these endeavors. In the area of Psuedolites, it is important to leverage the prior efforts of DARPA and CECOM. In the area of enhanced

A/J user equipment, the Army should exploit the technology developed by the Air Force and the Navy. Based on these activities, this area is assessed as “green.”

Programmatics:

The Army should expand the Battlespace Tactical Navigation Program from its current funding levels of \$1M - \$2M per year to at least \$10M per year. The Air Force and the Navy are pursuing complementary RDT&E activities, but they are not addressing many of the issues that confront the Army (e.g., battery life; logistics and operational challenges). In addition, action should also be taken to transition DARPA’s pseudolite development programs to the Army. Since all of these initiatives are inadequately resourced, this area is assessed as “red”.

Counter and protect - Counter space

Brief Definition of the Technology Area:

The rapid development of Surveillance, Communications, Navigation, Weather, Environmental Sensing, Intelligence systems based in space and available both as dedicated “National Systems” by numerous countries. International / commercial systems present a significant challenge to the survival of US forces which can be compromised by these systems capable of worldwide operations and direct support of hostile forces. Technologies to counter these systems across the spectrum of hard kill (ASAT) to the temporary effect of denial (Jamming, blinding) which allows restoration of service when the denial effect is removed are required to provide US forces an Information edge on the battlefield. The National Politics on Counterspace continue to be a key element of this discussion.

Technology Maturity:

Many of the technologies required to support Counter space actions are relatively mature, but are not being inserted into technology applications which can lead to operational capability in the timeframe necessary to support US Objective force timeframes. These technologies need to be integrated into systems concepts that can support battlefield operations. Specific system applications of technologies with high value are:

1. ASAT hit to kill test and validation,
2. EW, HPM and Optical Jamming and Blinding of space based surveillance and communications systems,
3. Denial (with EW or precision attack) of ground based elements supported by space systems such as GPS, Communications, Weather, Missile Warning, ATC, etc.

In all cases the Army has technology programs in place, but is not moving to the EMD, prototype phases to provide direct battlefield support necessary to the objective force support. In some cases, the mission is assigned to other services and needs to be integrated into objective force ops concepts. Protection of US systems is less mature than the technologies of counter hostile systems.

Programmatics:

The Army needs a comprehensive counterspace concept of operations to support objective force concepts of operations and the development of systems to accomplish the requirements- the basic technology programs need then to be tuned to this overall CONOPS for support to objective forces. CINCSPACE needs to engage in developing the support to forces CONOPS. Current technologies might provide the required capabilities if developed and integrated into operationally viable systems to be deployed.

Information Assurance

Brief Definition of the Technology Area:

Information Assurance is technology for ensuring Objective forces Communications, Information Systems and Sensors are secure from denial, disruption, degradation or deception by hostile forces. As is obvious in today’s IT

world this is a massive problem requiring extensive application of technologies associated with communication and sensor hardening, security and protection of software and hardware systems, intrusion detection systems and intrusion monitoring systems as well as intrusion response systems, authentication systems both for access and content, self forming and healing networks responsive to denial and disruption, psychological attack denial and detection, sensor deception and denial recognition and response as well as a broad range of traditional countermeasures and counter-countermeasures.

Technology Maturity:

The USA is the world leader in the development of Information Assurance technologies. That by no means implies that our technology is fully capable of denial of Information Attacks, but we do lead the world. The maturity of the technology also leads the world, but needs to grow as the IT technology evolves which requires constant development of new technology- and IT technology generation may be only 2 - 5 years. The Army is not the major sponsor of the technology, nor is the overall USG, but is in fact a primarily user of the technology. Some specific technologies, uniquely applicable to military systems, are being developed by DARPA, DISA, NSA and the Services. These technologies are also leading edge technologies and provide US Forces an advantage in I.O. Over hostile forces. It will be increasingly necessary to apply (and in some cases develop) advance information assurance technologies as the Objective Force capitalizes on Information superiority to dominate the battlefield. A critical need will be the establishment of a superior technical vulnerability and assessment organization to ensure US Army Communications, Information Systems and Sensors are secure from denial, disruption, degradation or deception by extensive vulnerability testing and assessment in an unbiased independent activity.

Current Programmatic:

Between ARL (SLAD), CECOM, and INSCOM (LIWA) much of the Information Assurance mission is being accomplished. The ability of the Army to integrate the USG wealth of I.A. Activities (including CINC space's new role) and the vast amount of I.A. Technology being developed in the US and international commercial community is overwhelming. The system Engineer responsible for objective forces will require a much stronger ability to ensure technology is applied, upgraded and maintained as leading edge. The establishment of a superior technical vulnerability and assessment organization to ensure US Army Communications, Information Systems and Sensors are secure from denial, disruption, degradation or deception by extensive vulnerability testing and assessment in an unbiased independent activity will be essential

Sensor Countermeasures

Brief Definition of the Technology Area

The US Army has the need to counter a broad range of hostile RSTA and weapon homing sensor on the battlefield. These range all the way from space Based sensor to hand held battlefield sensor and smart mine sensors. The technologies range from lethal attack, active jammers/deception, to passive signature management and deception and signature reduction. Similarly it is necessary to "Harden" US Army objective force sensors against similar CM effects. Typical technologies include Precision munitions, Jammers, O.A., HPM, Signature reduction and modification, passive detection systems (ESM, warning), deception and decoys.

Technology Maturity:

US technology is very mature in this arena (must continue to be funded to remain mature), but is not applied in a uniform manner against the current or "future" threat. The development of good threat data and the demonstration of the vulnerability of hostile force capabilities with application of these technologies (OPFOR exercises) are important. Similarly "hardening" of US sensors is not uniformly accomplished. A key missing element of the technology maturity equation is the establishment of a superior technical vulnerability and assessment organization to ensure US Army Sensors are secure from denial, disruption, degradation or deception and that hostile forces sensors are exploited by US technologies for denial, disruption, degradation or deception by extensive vulnerability testing and assessment in an unbiased independent activity. In general, the US Army technology to counter hostile sensors is more mature than our ability to protect US sensors.

Programmatics:

The base technologies are well funded, but the application of the technologies into an “integrated” survival suite for the FCS is not. It is essential to develop an integrated approach to the defeat of hostile sensor which includes lethal attack, Active CM and O.A., passive warning and signature management to defeat enemy detection, acquisition and targeting of US forces. The development of an Intelligence threat is also critical to this activity- CM are most capable when the threat is well defined and the “Red Team” is an on-going technically challenging activity.

RDA

Brief Definition of the Technology Area

RDA will integrate radically new technologies from the other Information Dominance Core Capabilities. This technology integration is necessary to implement a comprehensive information architecture for the Objective Force. The variety and magnitude of technologies in the Information Dominance Core Capabilities demands a RDA effort far exceeding the complexity and scale of any effort previously undertaken by the Army. Modeling, simulation and test beds are crucial aspects of today's generally accepted RDA approaches. The use and application of modeling, simulation and test beds for the RDA of this extensive and sophisticated information dominance environment is required to meet Army planned timelines for fielding of Objective Force capabilities.

Modeling and simulation (M&S) will support all design, development, systems engineering and integration, and testing efforts that must be undertaken. Virtual, constructive and live techniques should be employed for RDA; development of tactics, techniques and procedures (TTP) and doctrine; and training. Test beds will specifically support software development. The Central Technical Support Facility (CTSF), initiated for digitization, can provide lessons learned for establishing a test bed for Objective Force information dominance. All M&S and test bed capabilities and facilities should be integrated into an integrated data environment (IDE) supporting FCS developments.

Rationale for the Technology Maturity Score

Today's M&S technologies that can support Objective Force RDA are scored yellow. Today's technologies can provide for M&S of force-on-force engagements, but lack fidelity in representations of C4ISR capabilities. Today's M&S technologies can support evaluation of C4ISR performance, but can not directly support force effectiveness metrics. These limitations are known, and current efforts are attempting to identify approaches for needed M&S technologies. If it were not for M&S efforts conducted over the last four years supporting the 1997 and 2001 Quadrennial Defense Reviews (QDRs), the score would be red. Further, M&S capabilities do not exist which can represent the advanced information systems and concepts being considered for the Objective Force.

In support of digitization, the Army has established test beds for C4ISR developments. The test bed efforts for the First Digitized Division (FDD), Joint Contingency Force (JCF) Advanced Warfighting Experiment (AWE), and first Initial Brigade Combat Team (IBCT) should provide sufficient lessons learned for developing test beds for Objective Force information dominance. However, additional research into test bed technologies is needed to address the intimate interdependency between the FCS/Objective Force weapon platforms and C4ISR platforms

Evidence that the Program is not Currently Supported

Programmatics for modeling, simulation and test beds are scored red. There does not exist any capability which can support integration of the Information Dominance Core Capabilities. At the time of the ASB briefout to GEN Shinseki in July 2000, there were no plans for addressing this shortcoming. Subsequent to the ASB briefout, CECOM RDEC initiated a FCS Virtual Simulation effort. The CECOM RDEC effort is integrating RSTA models that could be used for Objective Force information dominance. There continues to be a void of any effort to develop a comprehensive modeling, simulation and test bed capability to support RDA for the Objective Force. The longer the Army delays initiation of such an effort, the greater risk the Army must overcome for its S&T and EMD activities.

APPENDIX L

ACRONYMS

Acronyms

A2C2	Army Airspace Command and Control
AAC	Army Acquisition Corps
AAE	Army Acquisition Executive
AAFIF	Automated Air Facilities Information File
AARs	After Action Reviews
ABCS	Army Battle Command Systems
ABN	Airborne
ACAT	Acquisition Category
ACOM	Atlantic Command
ACR	Armored Cavalry Regiment
ACTD	Advanced Concept Technology Demonstration
ADO	Army Digitization Office
AEF	Air Expeditionary Force
AF	Air Force
AFSAB	Air Force Scientific Advisory Board
AFSS	Advanced Fire Support System
AJ	Anti Jamming
AGCCS	Army Global Command and Control System
AGS	Armored Gun System
AI	Artificial Intelligence
ALP	Advanced Logistics Project
AMC	Army Materiel Command
AMCOM	Aviation and Missile Command
AMSAA	Army Materiel Systems Analysis Activity
AOR	Area of Responsibility
APFSDS	Armor-Piercing, Fin-stabilized, Discarding Sabot
APC	Armored Personnel Carrier
APOD	Aerial Port of Debarkation
APOE	Aerial Port of Embarkation
APS	Active Protection Systems; Army Prepositioned Stocks
ARDEC	Army Research, Development, and Engineering Center
ARL	Army Research Laboratory
ATT	Advanced Tactical Transport
ARTY	Artillery
ASA(ALT)	Assistant Secretary of the Army for Acquisition Logistics and Technology
ASB	Army Science Board
ASD C3I or ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASTMP	Army Science and Technology Master Plan
ASTWG	Army Science and Technology Working Group
AT	Anti Tank
ATD	Advanced Technology Demonstration
ATG	Anti-Tank Gun

ATGM	Anti-Tank Guided Missile
ATR	Automated Target Recognition
AWE	Advanced Warfighting Experiment
B2C2	Battalion and Below Command and Control
BAT	Brilliant Anti-Tank
BCIS	Battlefield Combat Identification System
BDA	Battle Damage Assessment
BDE	Brigade
BITS	Battlefield Information Transmission System
BLOS	Beyond Line of Sight
BN	Battalion
C2	Command and Control
C2E	Command Center Element
C2OTM	Command and Control On-The-Move
C2SID	Command and Control System Integration Directorate
C2T2	Commercial Communications Technology Testbed
C2V	Command and Control Vehicle
C2W	Command and Control Warfare
C3	Command, Control and Communications
C3I	Command, Control, Communications and Intelligence
C3IEW	Command, Control, Communications Intelligence and Electronic Warfare
C4	Command, Control, Communications and Computers
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CASCOM	Combined Arms Support Command
CASTFOREM	Combined Arms and Support Task Force Evaluation Model
CBW	Chemical and Biological Warfare
CC&D	Concealment Camouflage and Deception
CDR	Critical Design Review
CDT	Commercially Driven Technologies
CE	Chemical Energy
CECOM	Army Communication-Electronics Command
CHP	Controlled Humidity Preservation
CINC	Commander-in-Chief
CINCTRANS	Commander-in-Chief, Transportation Command
CKEM	Compact Kinetic Energy Missile
CM	Countermeasures
CONOPS	Concept of Operations
CONUS	Continental United States
COA	Course of Action
COTS	Commercial Off-The-Shelf
CPX	Command Post Exercise

CRAF	Civil Reserve Air Fleet
CSA	Chief of Staff, Army
CSSCS	Combat Service Support Computer System
CTC	Combat Training Center
DARPA	Defense Advanced Research Projects Agency
DAS	Director of Army Staff
DAS(R&T)	Deputy Assistant Secretary for Research and Technology
DBBL	Dismounted Battlespace Battle Lab
DCS(RDA)	Deputy Chief of Staff Research Development and Acquisition
DCSD	Deputy Chief of Staff Combat Development
DCSDOC	Deputy Chief of Staff Doctrine
DCSINT	Deputy Chief of Staff Intelligence
DCSLOG	Deputy Chief of Staff Logistics
DCSOPS	Deputy Chief of Staff Operations
DDR&E	Director, Defense Research and Engineering
DE	Directed Energy
DEW	Directed Energy Weapons
DISA	Defense Information Systems Agency
DISC4	Director, Information Systems, Command, Control, Communications and Computers
DL	Distance Learning
DLA	Defense Logistics Agency
DMSO	Defense Modeling and Simulation Office
DoT	Department of Transportation
DPG	Defense Planning Guide
DPICM	Dual Purpose Improved Conventional Munitions
DS	Direct Support
DSB	Defense Science Board
DSWA	Defense Special Weapons Agency
DSP	Digital Signal Processing
DTAP	Defense Technology Area Plan
DTLOMS	Doctrine, Training, Leader Development, Organization, Materiel, and Soldiers
DTO	Defense Technology Objective
DU	Depleted Uranium
DUSA-OR	Deputy Undersecretary of the Army - Operations Research
EAD	Echelons Above Division
EFOGM	Enhanced Fiber-Optic Guided Missile
EFP	Explosively Formed Penetrator
ELINT	Electronic Intelligence
EM	Electro-Mechanical, Electro-Magnetic
EMD	Engineering and Manufacturing Development
EML	Electro-Magnetic Launch
EMPRS	En Route Mission Planning and Rehearsal System

EO/IR	Electro-Optical/Infrared
ERA	Extended Range Artillery, Explosively Reactive Armor
ETC	Electro-Thermal Chemical
EW	Electronic Warfare
F&M	Firepower and Mobility
FBCB2	Force XXI Battle Command Brigade and Below
FC	Fire Control
FCS	Fire Control Systems; Future Combat System
FCV	Future Combat Vehicle
FCVT	FCV Team
FLIR	Forward Looking Infra-Red
FOB	Forward Operating Base
FOG-M	Fiber-Optic Guided Missile
FORSCOM	Forces Command
FTR	Future Transport Rotorcraft
FSCS	Future Scout and Cavalry System
FSV	Future Scout Vehicle
FTX	Field Training Exercise
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GCSS-A	Global Combat Support System – Army
GIG	Global Information Grid
GIS	Global Information System
GOSC	General Officer Steering Committee
GPS	Global Positioning System
GVW	Gross Vehicle Weight
HE	High Explosive
HEAT	High Explosive Anti-Tank
HHH	Hand-Held Heat
HIMARS	High Mobility Artillery Rocket System
HMMWV	High Mobility Multi-purpose Wheeled Vehicle
HNS	Host Nation Support
HPM	High Power Microwave
HQAMC	Headquarters of the Army Materiel Command
HSS	High-Speed Shipping
HVAP	High Velocity Armor Penetrating
I2R	Imaging Infrared
IA/IW	Information Assurance/Information Warfare
ICM	Improved Capabilities Missile, Improved Capabilities Munitions
IFSAR	Interferometric Synthetic Aperture Radar
III	Integrated Information Infrastructure(s)
IO	Information Operations

IPT	Integrated Product Team
IR	Infra Red
IR&D	Independent Research and Development
ISC/R	Individual Soldier's Computer/Radio
ISR	Intelligence Surveillance Reconnaissance
IT	Information Technology
IW	Information Warfare
IWS	Individual Warfighter System
J3	Operations Directorate, Joint Staff
J4	Logistics Directorate, Joint Staff
JCF	Joint Contingency Force
JCS	Joint Chiefs of Staff
JIT	Just-in-Time
JOPEs	Joint Operation Planning and Execution System
JROC	Joint Requirements Oversight Council
JS	Joint Support, Joint Staff
JSTARS	Joint Surveillance Target Attack Radar System
JTA	Joint Technology Architecture(s)
JWCA	Joint Warfighting Capability Assessment
KE	Kinetic Energy
KE/CE	Kinetic Energy / Chemical Energy
KEM	Kinetic Energy Missile
LAM	Land Attack Missile
LADAR	Laser Radar
LAV	Light Armored Vehicle
LAW	Light Anti-tank Weapon
LCLO	Low Cost Low Observable
LCMS	Laser Counter Measures System
LCPK	Low Cost Precision Kill
LIDAR	Light Detection and Ranging
LIWA	Land Information Warfare Activity
LLNL	Lawrence Livermore National Laboratory
LMSR	Large Medium Speed Roll-on/roll-off
LO	Low Observables
LOS	Line of Sight
LOSAT	Line-of-Sight Anti-Tank
LOTS	Logistics Over-the-Shore
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LRIP	Low Rate Initial Production
LTL	Less-than-Lethal
LW	Land Warrior

M&S	Modeling and Simulation
MAGTF	Marine Air-Ground Task Force
MANPADS	Man-portable Air Defense System
MANPRINT	Manpower and Personnel Integration
MAVs	Micro-Autonomous Vehicles, Micro Air Vehicles
MEM	Micro-Electro-Mechanics
MEMS	Micro Electric Mechanical System
MEP	Mobile Electric Power; Mission Equipment Package
METT-T	Mission, Enemy, Troops, Terrain, Time
MEU	Marine Expeditionary Unit
MHE	Materiel Handling Equipment
MILDEP	Military Deputy
MLRS	Multiple Launch Rocket System
MMCS	Multi-Mission Combat System
MMUAV	Multi-Mission Unmanned Air Vehicle
MNS	Mission Needs Statement
MOUT	Military Operations in Urban Terrain
MPIM	Multipurpose Infantry Munition
MPS	Maritime Prepositioning Ship
MRDEC	Missile Research, Development and Engineering Center
MSTAR	Moving and Stationary Target Acquisition and Recognition
MTI	Moving Target Indicator
MTI-SAR	Moving Target Indicator – Synthetic Aperture Radar
MTMC	Military Transportation Management Command
MTMC-TEA	Military Transportation Management Command – Transportation Engineering Agency
MVMT	Movement
MW	Mounted Warrior
NBC	Nuclear, Biological and Chemical
NDF	National Defense Features
NG APS	National Guard - Army Prepositioned Stocks
NGB	National Guard Bureau
NGIC	National Ground Intelligence Center
NL	Non-Lethal
NLT	No Later Than
NLW	Non-Lethal Weapons
NMD	National Missile Defense
NRAC	Naval Research Advisory Committee
NRDEC	Natick Research, Development and Engineering Center
NSA	National Security Agency
NTC	National Training Center
NVESD	Night-Vision/Electronic Sensors Directorate
O&O	Operational and Organizational
OCAR	Office of the Chief, Army Reserve

OCONUS	Outside Continental United States
ODCSOPS	Office of the Deputy Chief of Staff for Operations
OOTW	Operations Other Than War
OPM	Other People's Money
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
P3I	Preplanned Product Improvement
PAM	Precision Attack Munitions
PDR	Preliminary Design Review
PDRR	Program Definition/Risk Reduction
PEO	Program Executive Office (Officer)
PEO/3C	Program Executive Officer for Command, Control and Communications
PGM	Precision Guided Munitions
PGMM	Precision Guided Mortar Munitions
POD	Point of Debarkation
POL	Petroleum, Oil and Lubricants
POM	Preparation for Overseas Movement
POS/NAV	Position/Navigation
PREPO	pre-positioned stocks
RHA	Rolled Homogenous Armor
RHAE	Rolled Homogenous Armor Equivalent
R/S	Reconnaissance/Surveillance
RC	Reserve Component
RDA	Research Development and Acquisition
RDT&E	Research Development Testing and Evaluation
RFPI	Rapid Force Projection Initiative
RHA	Rolled Homogenous Armor
RORO	Roll-on Roll-off
RPG	Rocket Propelled Grenade
RRF	Rapid Reaction Forces
RSTA	Reconnaissance Surveillance, Target Acquisition
S&T	Science and Technology
SA	Situation Awareness
SAALT	Secretary of the Army for Acquisition, Logistics and Technology
SACLOS	Semi-Automated Line of Sight
SADARM	Sense and Destroy Armor
SAR	Synthetic Aperture Radar
SARDA	Secretary of the Army for Research Development and Acquisition – outdated, now SAALT – Secretary of the Army for Acquisition, Logistics and Technology
SAS	Situation Awareness System
SBIR	Small Business Innovation Research

SES	Surface Effect Ships
SIGINT	Signal Intelligence
SIMNET	Simulation Network
SINCGARS	Single Channel Ground and Airborne Radio System
SIPE	Soldier Integrated Protective Ensemble
SLAD	Survivability and Lethality Directorate
SLID	Simple Low-cost Interception Device
SM	Signature Management
SRO	Strategic Research Objective
SSCOM	Soldier Systems Command
SSTOL	Super Short Take-Off & Landing
STARC	State Area Command
STI	Stationary Target Indicator
STO	Science and Technology Objective
STOW-E	Synthetic Theater of War-Europe
SUO	Small Unit Operations
SUOSAS	Small Unit Operations Situation Awareness System
SUSOPS	Sustained Operations
SWA	South West Asia
T&E	Test and Evaluation
TAA	Tactical Assembly Area
TAAD	Theater Area Air Defense
TACOM	Tank Automotive and Armaments Command
TAP	Technology Area Plan
TARA	Technology Area Review and Assessment
TARDEC	Tank Automotive Research Development and Engineering Center
TDA	Table of Distribution and Allowances
TENCAP	Tactical Exploitation of National Capabilities (program)
TERM	Tank Extended Range Munitions
TES	Tactical Engagement System; Tactical Engagement Simulation
TEU	20-foot-equivalent unit
TF	Task Force
THAAD	Theater High Altitude Defense System
TOC	Tactical Operations Center
TOR	Terms of Reference
TOW	Tube-Launched, Optically Tracked, Wire Command-Linked Guided
TPFDD	time-phased forces deployment data
TRADOC	Training and Doctrine Command
TRANSCOM	Transportation Command
TTP	Tactics, Techniques, and Procedures
TWG	Technology Working Group
TWS	Thermal Weapon Sight
UAV	Unmanned Aerial Vehicles
UGS	Unattended Ground Sensors

UGV	Unmanned Ground Vehicles
UHF	Ultra-High Frequency
USMA	United States Military Academy
USMC	United States Marine Corps
UV	Ultra-Violet
UWB	Ultra-Wide Band
UXO	Unexploded Ordinance
V/STOL	Vertical or Short Take-off and Landing
VCSA	Vice Chief of Staff of the Army
VISA	Voluntary Intermodal Shipping Agreement
VSAT	Very Small Aperture Terminal
VTOL	Vertical Take-off and Landing
VTOL JTR	Vertical Take-off and Landing – Joint Tilt Rotor
WARSIM	Warfighter Simulation
WIN	Warfighter Information Network
WMD	Weapons of Mass Destruction
WRAP	Warfighting Rapid Acquisition Program

For Acronyms not found here, consult:

<http://www.adtdl.army.mil/atdl/search/acronym.htm>

or

<http://www.sew-lexicon.com/>

APPENDIX M

FINAL REPORT DISTRIBUTION

Addressee	Copies
ARMY	
Secretary of the Army, Pentagon, Room 3E700, Washington, DC 20310-0101	1
Under Secretary of the Army, Pentagon, Room 3E732, Washington, DC 20310-0102	1
Deputy Under Secretary of the Army (Operations Research), Pentagon, Room 2E660, Washington, DC 20310-0102	1
Assistant Secretary of the Army (Manpower and Reserve Affairs), Pentagon, Room 2E594, Washington, DC 20310-0111	1
Military Deputy to the ASA(ALT), Pentagon, Room 2E672, Washington, DC 20310-0103	1
Deputy Assistant Secretary for Plans, Programs and Policy, OASA(ALT), Pentagon, Room 3E432, Washington, DC 20310-0103	1
Deputy Assistant Secretary for Procurement, OASA(ALT), Pentagon, Room 2E661, Washington, DC 20310-0103	1
Deputy Assistant Secretary for Research and Technology, OASA(ALT), Pentagon, Room 3E374, Washington, DC 20310-0103	1
Deputy for Systems Management and International Cooperation, OASA(ALT), Pentagon, Room 3E448, Washington, DC 20310-0103	1
Deputy for Ammunition, OASA(ALT), Headquarters, Army Materiel Command, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Deputy for Combat Service Support, OASA(ALT), Headquarters, Army Materiel Command, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Director, Assessment and Evaluation, OASA(ALT), Pentagon, Room 2E673, Washington, DC 20310-0103	1
Director, Army Digitization Office, DACS-ADO, Pentagon, Room 2B679, Washington, DC 20310-0200	1
Director of Information Systems for Command, Control, Communications and Computers, Pentagon, Washington, DC 20310-0107	1
Chief of Public Affairs, Pentagon, Room 2E636, Washington, DC 20310-1500	1
Chief of Staff, Army, Pentagon, Room 3E668, Washington, DC 20310-0200	1
Vice Chief of Staff, Army, Pentagon, Room 3E666, Washington, DC 20310-0200	1
Deputy Chief of Staff for Programs, Army Pentagon, Room 3D652, Washington, DC 20310-0200	1
Director of the Army Staff, Pentagon, Room 3E665, Washington, DC 20310-0200	1
Director, Program Analysis and Evaluation Directorate, Pentagon, Room 3C718, Washington, DC 20310-0200	1
Assistant Chief of Staff for Installation Management and Environment, Pentagon, Room 1E668, Washington, DC 20310-0600	1
Deputy Chief of Staff for Personnel, Pentagon, Room 2E736, Washington, DC 20310-0300	1
Deputy Chief of Staff for Operations and Plans, Pentagon, Room 3E634, Washington, DC 20310-0400	1
Assistant Deputy Chief of Staff for Operations and Plans, Force Development, Pentagon, Room 3A522, Washington, DC 20310-0400	1
Deputy Chief of Staff for Logistics, Pentagon, Room 3E560, Washington, DC 20310-0500	1
Deputy Chief of Staff for Intelligence, Pentagon, Room 2E464, Washington, DC 20310-1000	1
Chief, National Guard Bureau, Pentagon, Room 2E394, Washington, DC 20310-2500	1
Chief, Army Reserve, Pentagon, Room 3E390, Washington, DC 20310-2400	1
Commander, U.S. Army Concepts Analysis Agency, 6001 Goethals Rd., Ft. Belvoir, VA 22060-5230	1
Commander, U.S. Army Evaluation Center, Park Center IV, 4501 Ford Ave., Alexandria, VA 22302-1458	1
Commanding General, U.S. Army Space and Missile Defense Command, P.O. Box 15280, Arlington, VA 22215-0280	1
Chief Scientist, U.S. Army Space and Missile Defense Command, P.O. Box 15280, Arlington, VA 22215-0280	5
Commander, National Ground Intelligence Center, 220 7th St., NE, Charlottesville, VA 22901	1
Director, U.S. Army Research Institute for the Behavioral Sciences, 5001 Eisenhower Ave., Alexandria, VA 22333-5600	1
Commander, U.S. Total Army Personnel Command, Hoffman Building II, 200 Stovall St., Alexandria, VA 22332-0405	1
Commander-in-Chief, U.S. Army Europe and Seventh Army, APO AE 09014	1
Commanding General, Eighth U.S. Army, APO AP 96205	1
Commanding General, U.S. Army South, HQ US Army South, P.O. Box 34000, Ft. Buchanan, Puerto Rico 00934-3400	1

Addressee	Copies
Commanding General, U.S. Army Pacific, Ft. Shafter, HI 96858-5100	1
Commanding General, U.S. Army Forces Command, Ft. McPherson, GA 30330-6000	1
Commanding General, Third United States Army/Army Central Command/Deputy Commanding General, U.S. Army Forces Command, ATTN: AFDC, Ft. McPherson, GA 30330	1
U.S. Army Space Command Forward, ATTN: MOSC-ZC, 1670 N. Newport Rd., Suite 211, Colorado Springs, CO 80916	1
Commanding General, U.S. Army Signal Command, Ft. Huachuca, AZ 85613-5000	1
Commanding General, U.S. Army Special Operations Command, Ft. Bragg, NC 28307-5200	1
Commanding General, U.S. Army Intelligence and Security Command, Ft. Belvoir, VA 22060-5370	1
Commanding General, U.S. Army Medical Command, Ft. Sam Houston, TX 78234	1
Commander, U.S. Army Medical Research and Materiel Command, Ft. Detrick, MD 21702-5012	1
Commanding General, U.S. Army Materiel Command, ATTN: AMCCG, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Commanding General, U.S. Army Materiel Command, ATTN: AMCRDA-TT, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Commander, U.S. Army Chemical and Biological Defense Command, ATTN: AMSCB-CG, Aberdeen Proving Ground, MD 21005-5423	1
Commander, U.S. Army Communications-Electronics Command, ATTN: AMSEL-CG, Ft. Monmouth, NJ 07703-5000	1
Director, Army Systems Engineering Office, ATTN: AMSEL-RD-ASE, Ft. Monmouth, NJ 07703	1
Commander, U.S. Army Aviation and Missile Command, ATTN: AMSMI-CG, Redstone Arsenal, AL 35898	2
Commander, U.S. Army Simulation, Training and Instrumentation Command, ATTN: AMSTI-CG, 12350 Research Parkway, Orlando, FL 32836-3276	1
Commander, U.S. Army Soldier Systems Command, ATTN: AMSSC-CG, Natick, MA 01760-5000	1
Commander, U.S. Army Tank-Automotive and Armaments Command, ATTN: AMSTA-CG, Warren, MI 48397-5000	1
Commander, U.S. Army Test and Evaluation Command, ATTN: AMSTE-CG, Aberdeen Proving Ground, MD 21005-5055	1
Commander, U.S. Army Armament Research, Development and Engineering Center, ATTN: SMCAR-TD, Picatinny Arsenal, NJ 07806-5000	1
Commander, U.S. Army Aviation Research, Development and Engineering Center, ATTN: AMSAT-R-Z, 4300 Goodfellow Blvd., St. Louis, MO 63120-1798	1
Commander, U.S. Army Communications-Electronics Research, Development and Engineering Center, ATTN: AMSEL-RD, Ft. Monmouth, NJ 07703	1
Commander, U.S. Army Missile Research, Development and Engineering Center, ATTN: AMSMI-RD, Redstone Arsenal, AL 35898	1
Commander, U.S. Army Natick Research, Development and Engineering Center, ATTN: SATNC-T, Natick, MA 01760	1
Commander, U.S. Army Tank-Automotive Research, Development and Engineering Center, ATTN: AMSTA-CF, Warren, MI 48397	1
Director, U.S. Army Field Assistance in Science and Technology Activity, 5985 Wilson Rd., Suite 100, Ft. Belvoir, VA 22060-5829	1
Director, U.S. Army Logistics Support Activity, ATTN: AMXLS, Bldg. 5307, Redstone Arsenal, AL 35898-7466	1
Director, U.S. Army Materiel Systems Analysis Activity, ATTN: AMXSY-D, Aberdeen Proving Ground, MD 21005-5071	1
Director, U.S. Army Research Laboratory, ATTN: AMSRL-D, 2800 Powder Mill Rd., Adelphi, MD 20783-1145	1
Director, U.S. Army Research Office, ATTN: AMXRO-D, P.O. Box 12211, Research Triangle Park, NC 27709-2211	1
Commanding General, U.S. Army Training and Doctrine Command, Ft. Monroe, VA 23651-5000	1
Deputy Commanding General, U.S. Army Training and Doctrine Command, Ft. Monroe, VA 23651-5000	1
Deputy Commanding General, U.S. Army Training and Doctrine Command for Combined Arms/Commander, U.S. Army Combined Arms Center/Commandant, Command and General Staff College, Ft. Leavenworth, KS 66027-5000	1
Deputy Commanding General, U.S. Army Training and Doctrine Command for Combined Arms Support/	

Addressee	Copies
Commander, U.S. Army Combined Arms Support Command and Ft. Lee, Ft. Lee, VA 23801-6000	1
Commander, U.S. Army Aviation Center and Ft. Rucker/Commandant, U.S. Army Aviation School/Commandant, U.S. Army Aviation Logistics School (Ft. Eustis), Ft. Rucker, AL 36362-5000	1
Commander, U.S. Army Signal Center and Ft. Gordon/Commandant, U.S. Army Signal School, Ft. Gordon, GA 30905-5000	1
Commandant, U.S. Army War College, ATTN: AWCC-CSL-OG, 122 Forbes Avenue, Carlisle Barracks, PA 17013-5050	1
Commander, U.S. Army Air Defense Artillery Center and Ft. Bliss/Commandant, U.S. Army Air Defense Artillery School, Ft. Bliss, TX 79916-5000	1
Commander, U.S. Army John F. Kennedy Special Warfare Center and School, Ft. Bragg, NC 28307-5000	1
Commander, U.S. Army Quartermaster Center and School/Deputy Commander, U.S. Army Combined Arms Support Command and Ft. Lee/Commandant, U.S. Army Quartermaster School, Ft. Lee, VA 23801-6000	1
Commander, U.S. Army Infantry Center and Ft. Benning/Commandant, U.S. Army Infantry School, Ft. Benning, GA 31905-5000	1
Commander, U.S. Army Ordnance Center/Commandant, U.S. Army Ordnance School, Aberdeen Proving Ground, MD 21005-5201	1
Commander, U.S. Army Field Artillery Center and Ft. Sill/Commandant, U.S. Army Field Artillery School, Ft. Sill, OK 73503-5000	1
Commander, U.S. Army Transportation Center and Ft. Eustis/Commandant, U.S. Army Transportation School, Ft. Eustis, VA 23604-5000	1
Commander, U.S. Army Armor Center and Ft. Knox/Commandant, U.S. Army Armor School, Ft. Knox, KY 40121-5000	1
Commander, U.S. Army Intelligence Center and Ft. Huachuca/Commandant, U.S. Army Intelligence School, Ft. Huachuca, AZ 85613-6000	1
Commandant, U.S. Army Ordnance Missile and Munitions Center and School, Redstone Arsenal, AL 35897-6000	1
Commandant, Army Logistics Management College, Ft. Lee, VA 23801-6053	1
Director, U.S. Army Training and Doctrine Command Analysis Center, Ft. Leavenworth, KS 66027-5200	1
Commander, Battle Command Battle Lab, ATTN: ATZL-CDB, 415 Sherman Ave., Ft. Leavenworth, KS 66027-5300	1
Commander, Battle Command Battle Lab, ATTN: ATZH-BL, Ft. Gordon, GA 30905-5299	1
Commander, Battle Command Battle Lab, ATTN: ATZS-BL, Ft. Huachuca, AZ 85613-6000	1
Commander, Combat Service Support Battle Lab, ATTN: ATCL-B, Ft. Lee, VA 23801-6000	1
Commandant, Depth and Simultaneous Attack Battle Lab, ATTN: ATSF-CBL, Ft. Sill, OK 73503-5600	1
Commandant, Dismounted Battle Space Battle Lab, ATTN: ATSH-WC, Ft. Benning, GA 31905-5007	1
Commander, Early Entry Lethality and Survivability Battle Lab, ATTN: ATCD-L, Ft. Monroe, VA 23651-5000	1
Commander, Mounted Battle Space Battle Lab, ATTN: ATZK-MW, Ft. Knox, KY 40121-5000	1
Commander, Battle Lab Integration, Technology and Concepts Directorate, ATTN: ATCD-B, Ft. Monroe, VA 23651-5000	1
Program Executive Officer, Armored Systems Modernization, ATTN: SFAE-ASM, Warren, MI 48397-5000	1
Program Executive Officer, Aviation, ATTN: SFAE-AV, 4300 Goodfellow Blvd., St. Louis, MO 63120-1798	1
Program Executive Officer, Command, Control and Communications Systems, ATTN: SFAE-C3S, Ft. Monmouth, NJ 07703-5000	1
Program Executive Officer, Field Artillery Systems, ATTN: SFAE-FAS, Picatinny Arsenal, NJ 07806-5000	1
Program Executive Officer, Intelligence and Electronic Warfare, ATTN: SFAE-IEW, Ft. Monmouth, NJ 07703-5000	1
Program Executive Officer, Missile Defense, ATTN: SFAE-MD, P.O. Box 16686, Arlington, VA 22215-1686	1
Program Executive Officer, Standard Army Management Information Systems, ATTN: SFAE-PS, 9350 Hall Rd., Suite 142, Ft. Belvoir, VA 22060-5526	1
Program Executive Officer, Tactical Missiles, ATTN: SFAE-MSL, Redstone Arsenal, AL 35898-8000	1
Program Executive Officer, Tactical Wheeled Vehicles, ATTN: SFAE-TWV, Warren, MI 48397-5000	1
Program Executive Officer, Cruise Missiles Project and Unmanned Aerial Vehicles Joint Project, ATTN: PEO-CU, 47123 Buse Rd., Unit 1PT, Patuxent River, MD 20670-1547	1
Program Executive Officer, Combat Support Systems, ATTN: AF PEO CB, 1090 Air Force Pentagon, Washington, DC 20330-1090	1
Superintendent, U.S. Army Military Academy, West Point, NY 10996	1

Addressee	Copies
<u>NAVY</u>	
Secretary of the Navy, Pentagon, Room 4E686, Washington, DC 20350	1
Under Secretary of the Navy, Pentagon, Room 4E714, Washington, DC 20350	1
Assistant Secretary of the Navy (Research, Development and Acquisition), Pentagon, Room 4E732, Washington, DC 20350	1
Chief of Naval Operations, Pentagon, Room 4E674, Washington, DC 20350	1
Vice Chief of Naval Operations, Pentagon, Room 4E636, Washington, DC 20350	1
Commandant, U.S. Marine Corps, Pentagon, Room 4E714, Washington, DC 20380	1
Naval Research Advisory Committee, 800 N. Quincy Street, Arlington, VA 22217-5660	1
President, Naval War College, Code 00, 686 Cushing Rd., Newport, RI 02841-1207	1
<u>AIR FORCE</u>	
Secretary of the Air Force, Pentagon, Room 4E871, Washington, DC 20330	1
Under Secretary of the Air Force, Pentagon, Room 4E886, Washington, DC 20330	1
Assistant Secretary of the Air Force (Acquisition), ATTN: SAF/AQ, Pentagon, Room 4E964, Washington, DC 20330	1
Chief of Staff, United States Air Force, Pentagon, Room 4E924, Washington, DC 20330	1
Vice Chief of Staff, United States Air Force, Pentagon, Room 4E936, Washington, DC 20330	1
Air Force Scientific Advisory Board, Pentagon, Room 5D982, Washington, DC 20330	1
President, Air War College, 325 Chennault Circle, Maxwell Air Force Base, AL 36112-6427	1
<u>OSD</u>	
Secretary of Defense, Pentagon, Room 3E880, Washington, DC 20301	1
Deputy Secretary of Defense, Pentagon, Room 3E944, Washington, DC 20301	1
Under Secretary of Defense for Acquisition and Technology, Pentagon, Room 3E933, Washington, DC 20301	1
Under Secretary of Defense (Personnel and Readiness), Pentagon, Room 3E764, Washington, DC 20301	1
Assistant Secretary of Defense (Command, Control, Communications and Intelligence), Pentagon, Room 3E172, Washington, DC 20301	1
Deputy Under Secretary of Defense for Advanced Technology, Pentagon, Room 3E1045, Washington, DC 20301	1
Deputy Under Secretary of Defense for Environmental Security, Pentagon, Room 3E792, Washington, DC 20301	1
Principal Deputy Under Secretary of Defense for Acquisition and Technology, Pentagon, Room 3E1006, Washington, DC 20301	1
Chairman, Joint Chiefs of Staff, Pentagon, Room 2E872, Washington, DC 20318-9999	1
Vice Chairman, Joint Chiefs of Staff, Pentagon, Room 2E860, Washington, DC 20318-9999	1
Director, Defense Research and Engineering, Pentagon, Room 3E1014, Washington, DC 20301-3030	1
Director, Defense Advanced Research Projects Agency, 3701 N. Fairfax Dr., Arlington, VA 22203-1714	1
Director, Defense Information Systems Agency, 701 S. Courthouse Rd., Arlington, VA 22204-2199	1
Director, Defense Logistics Agency, 8725 John J. Kingman Rd., Suite 2533, Ft. Belvoir, VA 22060-6221	1
Director, National Imagery and Mapping Agency, 4600 Sangamore Road, Bethesda, MD 20816-5003	1
Defense Science Board, Pentagon, Room 3D865, Washington, DC 20301	1
Commandant, Defense Systems Management College, 9820 Belvoir Rd., Suite G-38, Ft. Belvoir, VA 22060-5565	1
President, National Defense University, 300 5th Avenue, Ft. McNair, Washington, DC 20319-5066	1
Commandant, Armed Forces Staff College, 7800 Hampton Blvd., Norfolk, VA 23511-1702	1
Commandant, Industrial College of the Armed Forces, 408 4th Ave., Bldg. 59, Ft. McNair, Washington, DC 20319-5062	1
Commandant, National War College, Washington, DC 20319-5066	1
National Security Space Architect, 2461 Eisenhower Avenue., Suite 164, Alexandria, VA 22331-0900	1
<u>OTHER</u>	
Defense Technical Information Center, ATTN: DTIC-OCP, 8725 John J. Kingman Rd., Suite 0944, Ft. Belvoir, VA 22060-6218	1
National Research Council, Division of Military Science and Technology, Harris Bldg Rm. 258, 2101 Constitution Avenue NW, Washington DC 20418	1
Director, Institute for Defense Analyses, ATTN: TISO, 1801 N. Beauregard St., Alexandria, VA 22311-1772	1
Library of Congress, Exchange and Gift Division, Federal Document Section, Federal Advisory Committee Desk, Washington, DC 20540	1