

**Knowledge Management
and
Information Assurance
Final Brief
June 2001**

ASB Study Jan-May 2001



The Obvious *is not* so Obvious

- **Two current examples of why Knowledge Management must be taken seriously by the US Army**
 - **War in Chechen**
 - **A Military example – the Russians do not understand!**
 - **World Trade Center**
 - **Asymmetric Threat – We knew!**



Knowledge Management WTC “Scenario”

Knowledge Broadly Available

- **WTC had been a Terrorist Target**
 - Intent was to “Topple” the two towers
 - Domestic USA was a target
- **Suicide Attacks were Terrorist tool**
 - Individuals
 - Teams
 - Truck Bombs
 - Small Boats
- **Aircraft Hijackings were Terrorist tool**
- **Terrorist were capable of developing modestly complex, simultaneous events.**
 - African embassy bombings

Knowledge available in selected groups

- **Design of WTC against a 707**
 - **Architects**
- **Speculation of effect of a 767 collision**
 - Aviation web pages in 2000
- **Probability of collapse of towers**
 - **Architects, Structural engineers**
- **Unlikely an airline pilot could be forced to fly into a structure.**
 - **Airline pilot assoc./ Past hijackings**
 - **Suicide ‘pilot’ would be required and would need to be able to fly the plane**
- **US had no viable, timely response to hijacked commercial airliners if attacks occurred in tens on minutes.**
 - **“Defense” community**
- **Immigration and Naturalization Service watch list of people associated with possible terrorist activity.**



Chechen Wars*

Concerning Availability of Knowledge to Commanders:

- “Leaders were unable to transfer that knowledge to those who had to defend the city a few short months later.”
- “Russians seem to forget painfully learned lessons from one battle to the next.”
- “There was little effort to pass lessons learned and tactics developed un to other soldiers.”
- “They grossly underestimated their enemy and overestimated their own capabilities.”
- “The key mistake the Russian Military made between the wars was in drawing the wrong lessons from urban combat.”
 - “Not only that it should be avoided.”
 - “But that it *could* be avoided, under all circumstances.”
- **Learning under Fire**: “The new leadership had a different, more systematic approach that drew effectively on lessons from the past.”
 - “Lessons were shared.”
 - “The rest of the force studied and copied the actions that led to success.”

Knowledge Management is the path to success with these types of issues



Study Panel Executive Survey

- **The Study Panel drew two global conclusions:**
 - I. The relationships between Knowledge Management and Information Assurance (KM/IA), and combat operations at the operational and tactical levels, are powerful, but not well understood or exploited
 - II. The Army needs an organization to bring KM/IA experts together with war fighters to get these relationships identified and validated quickly
 - In war fighter “territory”
 - With powerful sponsors
 - And adequate resources

- **The Study Panel also applauds the leadership of the Secretary of the Army and the Army Chief of Staff in Army Knowledge Management**



SECARMY White and CSA Shinseki Take the Lead (Memo # 1, Aug 8, 2001)

- **Army KM Guidance:**

“Army Knowledge Management is the Army strategy to transform itself into a network-centric, knowledge-based force.”

- **Goals:**

- **Become a Knowledge-Based Organization**
- **Integrate KM and Best Business Practices into Army processes**
- **Manage the Infostructure at the Enterprise Level**
- **Scale *Army Knowledge Online* as the Enterprise Portal**
- **Harness Human Capital for the Knowledge Organization**

Knowledge Management and Information Assurance

Army Science Board Ad Hoc Study

30 April 2001

John Reese, Chair

Jim Heath, Sponsor Rep.

Miriam Browning, Sponsor Rep.

Randy Woodson, Exec. Sec.

ASB Members & Consultants:

Christine Davis

Gary Glaser

Lynn Gref

Ed Reedy

Dave Martinez

Bill Howard

Stuart Starr

Gary Nelson

Dick Fisher

Government Advisors:

Mike Yoemans

Dale Wagner

Jack Marin

Paul Tilson

Jack Wade

Judy Pinsky

Thomas Rogers

Kevin Wheatley

OSD C3I

NSA

USA West Point

NRO

ARL/SLAD

CECOM

DISC4

DISC4



Terms of Reference

Sponsors: DCSINT and DISC4

Terms Of Reference

The study should be guided by, but not limited to, the following TOR

- (1) Define Knowledge Management and Information Assurance technologies for the Objective Force**
- (2) Define the strategy for conquering the information glut through fundamental soldier/team enabling technologies and processes from conceptual to geospatial**
- (3) Examine technology and operational concepts to mitigate asymmetric threats**
- (4) Provide a 2008-2012 roadmap to enable small, autonomous processing that facilitates knowledge production, sharing and decision making**

Study Duration: Four months



Panel's Key Conclusions

- **The Objective Force can not survive without quality KM.**
- **KM Technologies are emerging; at the tactical level, process reengineering is not yet occurring.**
- **There is no “plan” for developing tactical level KM - there is however, a great opportunity to embed KM in the future force.**

Land Warrior at the AWE
• *Group reconstitution*
• *Sniper counter*

Battle of Midway

FBCB2 Enabled
C2 beyond FM voice range
Bold maneuver at night
Responsive logistics
Rapid passage of lines
Line-of-sight computation
Transition operations
Operations in multiple directions



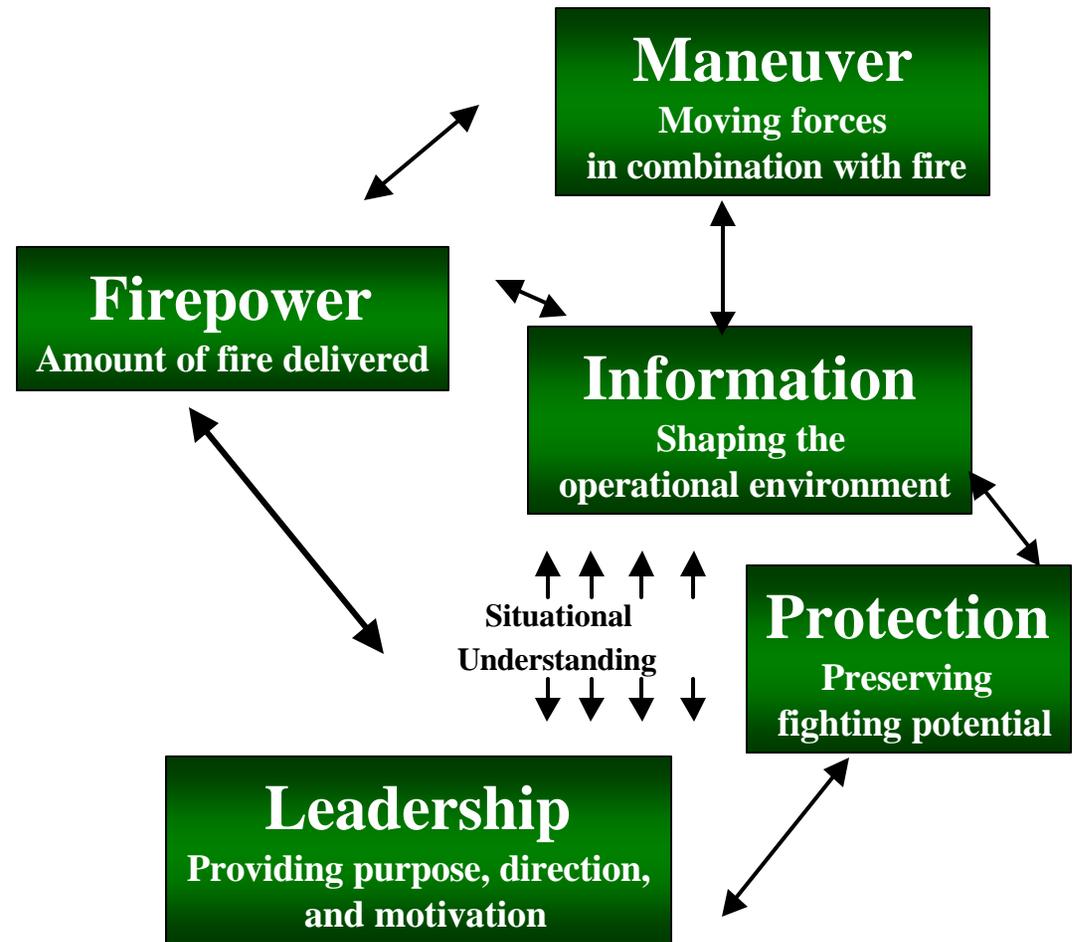
KM and IA Defined

- The Study Panel found appropriate KM and IA definitions for the Study:¹
 - *“The purpose of knowledge management (KM) is to enhance organizational performance by explicitly designing and implementing tools, processes, systems, structures, and cultures to improve the creation, sharing, and use of all . . . types of knowledge that are critical for decision making”*
 - *“Information Assurance (IA) is ‘Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities’”*



Knowledge Management Supports

- Enhancing organizational performance
 - by explicitly designing and implementing tools, processes, systems, structures, and cultures
- Improving the creation, sharing, and use of knowledge that is critical for quality decision making
- Identifying, managing and sharing a combat force's information and knowledge assets,
 - ...including databases, documents, policies and procedures,
 - ...as well as previously unarticulated (or tacit) expertise and experience resident in individual soldiers and other experts



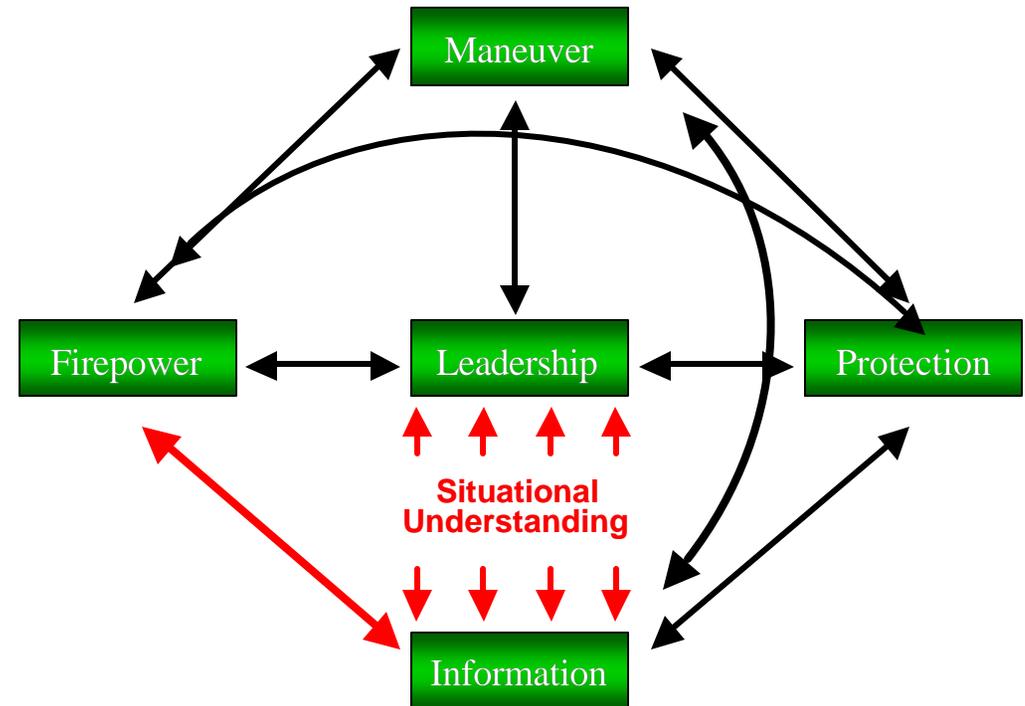
FM 3.0 Operations



Information Superiority & Firepower

US ground forces in Desert Storm employed counter battery radar to determine the locations of Iraqi heavy artillery as it fired.

Within seconds US MLRS rocket artillery had accurate digital information enabling counter battery rocket fire before the first enemy rounds landed.



The result was that Iraqi heavy artillery increasingly declined to fire, for fear of the immediate and deadly arrival of US “steel rain.”



Panel's Key Findings and Resultant Questions

- **Knowledge Management is a key enabler for the Objective Force**
 - **Tactical Knowledge-driven processes span the entire range of Tactical Forces (*Training - Deployment - Combat - Post combat*) and the entire breadth of DTLOMS**
 - **The Army Transformation to the Objective Force provides the opportunity to engineer an integrated knowledge-driven set of tactical processes. **Who is the process owner....TRADOC?****
- **The Army is a leader in Knowledge Management in the sustaining base and beginning to focus on Tactical opportunities. **How can Army leverage this experience to accelerate Tactical KM....?****
- **Commercial industry is designing and developing some important processes and technology that can support Objective Force Army efforts.**
 - **The Army will need to adapt and tailor requirements and research activities to fill R&D specific voids. **Potential Lead! ARL?****



Some Observations Regarding Current Army *Tactical* KM Initiatives

- Learned of many excellent, independent, small efforts focused on the Objective Force.....**who's orchestrating these efforts....no center of expertise.....**

No Center of Expertise

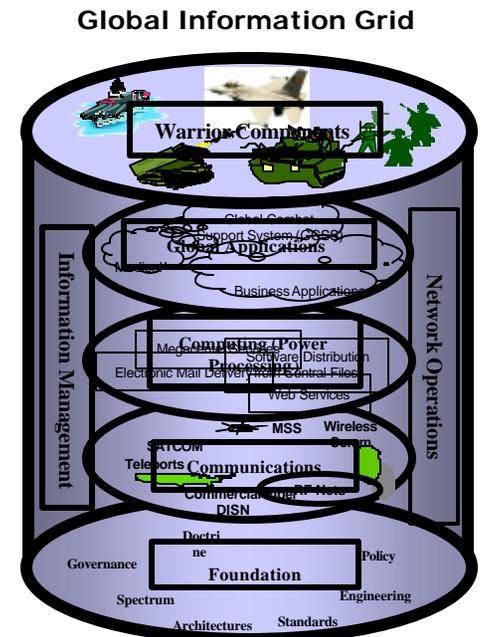
- Initiatives @ DISC4, PEO C3S, and CALL are excellent enterprise level KM programs
 - Not governed by an overarching plan
 - Significantly under funded
 - Excessively focused on legacy systems
- Potential for engineering KM into future systems not being considered

- Expansion to tactical level must be considered

NOTE THAT -

- *KM cannot be done well if it is not done in a system of systems construct*
- *The information infrastructure is a critical enabler—it needs to be resourced adequately in order to be the foundation for KM*

WKN
Warrior Knowledge Network





Technologies

Technology Readiness Levels

<u>Enabling Technologies</u>	<u>2004</u>	<u>2008</u>	<u>Commercial</u>
------------------------------	-------------	-------------	-------------------

Aided ATR	3	3	2
Smart Portals to push pull	6	9	9
Mobile Wireless (pagers, PDA)	6	9	7
Malicious Mobile Code	1	2	3
Visualization - Presentation	4	7	6
Data Extraction	6	8	8
Virtual environment	3	6	6
Automatic routers, priorities	5	8	5
Data fusion, information fusion	2	3	
Secure Intelligent Agents	2	5	7
Encryption and authentication	4	7	6
Exploitation Algorithms and assist	2	2	2
RTIC	5	8	
Future Internet	6	9	9
Individual Soldier Tech.	4	8	5
Collaboration Technologies	6	9	8
Sync Distributed Secure Data base	4	7	5
Secure Access Technology Biometrics	3	8	5
Translingual language transcription	4	6	7
Soldier Education	6	8	7
Associates	6	7	5
Next Generation Internet	6	9	9

TRL=Technology Readiness Levels

Commercial- % commercial R&D (1-10)



ASB Recommended Tactics

- **Designate Knowledge Management and Information Assurance technologies as essential to Army *Knowledge Dominance* (Lead: CSA) ..and the opportunity to degrade the enemy's Knowledge Management system - Counter Knowledge Management (Lead: DCSOPS)**
- **Build tactical level Knowledge Management on Army's excellent enterprise applications – e.g., Army Knowledge Online (Lead: DISC4)**
- **Write new Army doctrine requiring developers to integrate Knowledge Management and Information Assurance technologies into the design and development of Objective Force Combat Battalion and Soldier Systems. (Lead: TRADOC)**
- **Implement: (With ARL and TRADOC)**
 - A “Center of Excellence” for Army combat applications of KM
 - An integrated plan for Information Assurance, including a strong technical and operational “Red Team”
- **Invest in Process, Technology and Training to ensure Army tactical forces have *Knowledge Dominance* (Lead: TRADOC)**



ASB Recommended Tactics (con't)

- **Develop Standard Risk FACTORS to assess information assurance, asymmetric threats, and survivability (Lead: DISC4)**
 - Use of approved Information Assurance tools
 - Conduct Red Teams & Technical Vulnerability Analysis
- **As a part of Army Transformation establish initiatives to:**
 - Adopting and adapting commercial KM technologies
 - Identify residual requirements and pursue R&D to satisfy the complete Army need
 - Invest now in the *tactical infosphere* infrastructure recommended by previous ASB studies (Lead: Army Transformation Office)
- **Embed Knowledge Management as a *new process* in the Organization and Operation (O&O) for the Objective Force, ensuring O&O Owner drives KM acquisition capabilities (Lead: TRADOC)**



Strategy for the Objective Force

- **Develop an overarching Strategic KM Plan for the Tactical Army**
 - Use the “draft” Strategic KM Plan as a point of departure
 - Impacts all aspects of DTLOMS
 - Facilitates development of the Technology Roadmap
- **Embed KM into the Combat Battalion through a system of systems architecture**
 - Information routing (sorting, prioritizing, manipulating) is essential to the architecture
- **Establish Center of Excellence**
 - To provide an S&T focus and central expertise in KM to support Army programs, research and experimentation
- **Leverage COTS and focus R&D for robustness and survivability**
- **Plan for “block” upgrades**
 - Build a little; test a little; learn a lot
- **Leverage the GIG (Tactical Infosphere)**



Technology Roadmap

