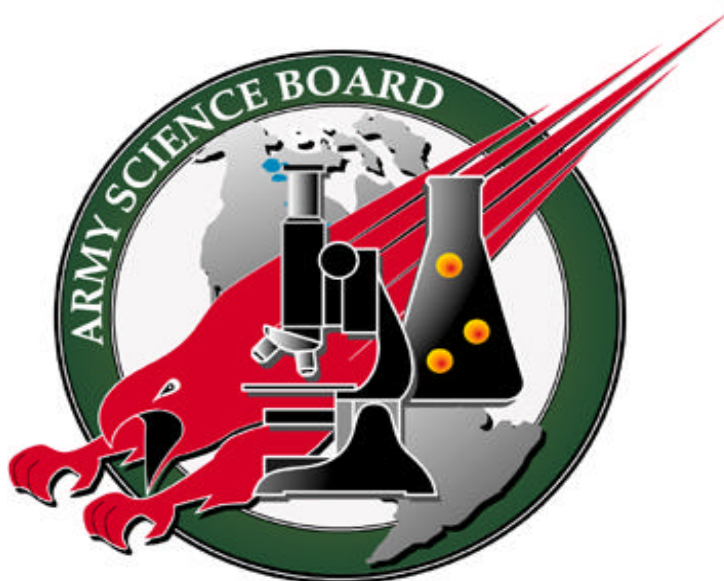


ARMY SCIENCE BOARD

FY2003 SUMMER STUDY

FINAL REPORT



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

“Force Protection Technologies for the 2010-2020 Timeframe”

November 2003

Distribution Statement:
Approved for public release;
distribution is unlimited

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 Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 00 NOV 2003		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Force Protection Technologies for the 2010 - 2020 Timeframe				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of the Army, Assistant Secretary of the Army, (Acquisition, Logistics and Technology), Washington, DC 20310-0103				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 382	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

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 2003 Summer Study Panel on “Force Protection Technologies for the 2010-2020 Timeframe” 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.

Force Protection Technologies for the 2010-2020 Timeframe

Table of Contents

Executive Summary	ES-1 to ES-4
Executive Briefing	1 to 40
Prior Studies Panel Report	Prior Studies – 1 to 4
Threat-Ops Panel Report	Threat-Ops –1 to 70
Technology Solutions Panel Report Technology Solutions Slides Appendix Sensor Narrative Section	Technology Solutions 1 to 37
Analysis and Modeling Panel Report A&M Annex & Appendices	Analysis and Modeling 1 to 88
Interfaces with Local Governments, Commerce and Infrastructure Panel Report	Interfaces 1 to 26
Appendices	
Appendix A – Terms of Reference	
Appendix B – Participants List	
Appendix C – Acronyms	
Appendix D - Distribution	

Force Protection Technologies for the 2010-2020 Timeframe

Executive Summary

At the request of multiple sponsors, the Army Science Board (ASB) conducted a study entitled “Force Protection Technologies for the 2010-2020 Timeframe”. The study was conducted by over 40 ASB Members, Consultants, and Government Advisors between November 2002 and July 2003. The terms of reference tasked study participants to review prior force protection (FP) studies, address FP issues during and after deployments, identify key FP technologies in the 2010-2020 timeframe, use analysis and models to evaluate potential contributions of FP technologies in specific scenarios, and to address FP opportunities and risks associated with the interactions with non-Army organizations. Based upon sponsor input and current events, the study was expanded to address near term options to improve force protection.

The study concluded that force protection has always been a priority but is now even more central to Army mission success. We found that there are many existing technology solutions to address force protection needs, with other technologies under development that offer greater advances. We identified the technology gaps that should be addressed with focused S&T investments, and discussed the importance of other areas, e.g., intelligence and civil affairs, which have high leverage and are of equal importance to effective force protection. We concluded that an integrated systems approach to force protection is essential, and discussed an opportunity for improving how the Army is organized with respect to force protection. We also found that while improved technologies and procedures are important, effective force protection requires constant diligence from the individual soldier to the commander.

Approach and Organization

Force protection is a key issue facing the US Army, and is a priority for every commander at every level, and everywhere US forces are stationed or deployed. Threats to US forces are equally as broad. To cover all situations and treats would be beyond the resources of the study, so our first step was to define a study scope appropriate for an ASB study. We defined the scope to include CONUS bases, deployment, peacekeeping, stability operations, and rear area security. We considered a threat ranging from terrorists trying to cause mass casualties to groups trying to cause sustained low-level casualties. We did not address conventional force maneuver operations, missile defense, homeland defense/security, or CONUS critical infrastructure.

A significant number of relevant studies have been conducted both prior to and after the events of 9/11. We performed an extensive review of studies by the Joint Staff, other advisory boards, independent and contract entities, reports on ongoing stability operations, and reports regarding the Khobar Towers and the USS Cole. We completed this task prior to initiating the discovery component of our study. We found that many common conclusions exist among the studies, including the utility of COTS technologies, the importance of intelligence (esp. HUMINT), and the need for an effective transition to local civil control. We concur with these conclusions. We also made an effort to focus our analysis on areas that have not been addressed by multiple other studies.

We assessed the present state of Army force protection. We found that in CONUS, there is a strong emphasis on physical security and access controls, with a goal of deterring attack without over-penalizing access to bases. We also found high but difficult to measure manpower costs, and a strong reliance upon Reserve and National Guard mobilization for force protection, including 9,000 mobilized for CONUS Air Force Base force protection. OCONUS, there seems to be an emphasis on using organic tactical assets, with a large fraction of deployed forces dedicated to force protection. The emphasis on force protection seems to impact the effectiveness of civil affairs stability operations.

We organized into panels addressing the key elements of force protection: Vulnerability and Threat Assessment; Operations; Technology Solutions; Analysis & Modeling; and Interfaces with Local Governments, Commerce, and Infrastructure. We developed a study methodology and iterative analytical approach that required frequent cross-panel interactions. This approach addressed force protection as a continuum involving pre-attack, trans-attack, and post attack actions, and led to the development of generic cases that were “solved” by systems solutions involving technologies and operational procedures. This method helped to ensure a link between the proposed technology and operational solutions and real-world scenarios.

Generic Cases and Systems Solutions

Our analytical approach yielded four generic cases: CONUS Base, OCONUS Base, Small Team or Detachment, and Convoy. For each of the generic cases, we developed an integrated systems solution involving a mix of technologies and operational procedures. We assessed the technology solutions against existing technologies and funded programs. From this assessment, we determined the technology gaps. Using a Delphi method, we prioritized the technology gaps.

For the CONUS Base, the systems solution emphasized deterrence while maintaining reasonable tenant access. This resulted in a layered physical security systems using COTS technologies with an integrated C2 system. Effective access controls to facilitate access to authorized personnel and perform contraband detection are required, as is coordination and cooperation with local/state/federal law enforcement agencies.

The OCONUS systems solutions emphasized layered detection and defense with a lesser reliance on COTS technologies and greater reliance on organic tactical assets. We believe there is a need for beyond perimeter surveillance technologies, including UAV and UGV based sensors, and an integrated C2 system with decision support aids. There is also a strong need for effective HUMINT and close coordination with local civil authorities.

Both the Small Team/Detachment and Convoy systems solutions called for vehicle defensive aid suites, UAV recon and relays, fixed base C2 and intelligence support, and support from tactical response forces. The Small Team/Detachment also required personal protection systems, while the convoy called for an armed UGV.

We found that there exist many commercial technologies that could be immediately applied to force protection, especially in CONUS. The DoD, in partnership with other agencies, has done an excellent job of coordinating the demonstration of these technologies in the bi-annual Force

Protection Equipment Demonstration (FPED) at Quantico, VA. We strongly endorse this activity, and believe that this activity should be expanded and possibly turned into an annual event.

We concluded that the following technologies could be fielded quickly: Initial decision support systems; Blue SA for individual vehicles; radio and GPS for all vehicles; digital maps/digital tracking; dynamic RF tags; beyond fence enhanced surveillance; UAV/UGV; UGS; radar, EO/IR; surveillance detection; UAV support for convoys; communication and GPS for individual soldiers; smart access controls; ballistic appliqués (blankets) for soft vehicles; and sniper detection systems.

We concluded that the following technologies could be fielded after 2010: Advanced decision support and training systems; enhanced UAV-based surveillance systems, including Chem/Bio detectors; standoff explosives detection systems; assured communications and Blue SA; mine detection/neutralization on the move; automated threat detection and response; robotic ground vehicles; and non-lethal technologies.

Because force protection needs are situation dependent, we recommend that specialized force protection equipment not be issued to every unit a priori. Rather, we recommend that vehicles be designed to accept force protection equipment, and that units be issued force protection equipment “kits” when needed. The selective issue of such equipment would dramatically limit total inventory costs.

Opportunities Beyond Direct Technology Investments

While the development and deployment of force protection technologies is essential, we found that there are many other opportunities for improving force protection beyond technology solutions. Opportunities exist in Intelligence, Doctrine and Training, Civil-Military Operations, Modeling and Simulation, and Leveraging Other Investments.

The highest operational leverage is in pre-attack threat identification, which comes from effective intelligence, especially HUMINT. Evolving doctrine from an emphasis on physical security to precluding attacks and proactive threat response is important. Training that emphasizes this doctrine, and collaborative distributive simulations for force protection would also have a high payoff.

An effective civil military operation supports HUMINT, improves situational awareness and understanding, and engenders good will. CMO provides the stability necessary for the transition from military to civilian authorities, which reduces force protection requirements. Modeling and simulation supports the full range of force protection activities, including education and training, operational support, assessment and experimentation, and acquisition.

We believe that the Army could improve its organization for force protection management by creating single leads within the requirements, S&T and acquisition communities. We also believe that cost-benefit analysis is not being uniformly applied to Army force protection investments.

During our investigation, we found three major investment areas by other entities that should be leveraged by the Army. The Physical Security industry invests billions annually to support commercial and government demands. This is increasing due to Department of Homeland Security investments. There are also major federal investments in multiple agencies focused upon the weapon of mass destruction threat. Army leadership of the Joint Chem/Bio Defense program will ensure the appropriate focus of DoD investments, but the Army must coordinate with other initiatives to ensure Army specific needs are met. The third investment area that must be leveraged is the FCS. Many of the technologies are directly applicable to force protection, but force protection requirements beyond combat operations have not generally been defined and integrated into FCS requirements.

Recommendations and Conclusions

Overarching Recommendations: Direct an Army-wide effort led from HQDA to improve Force Protection, including the implementation of the recommendations of this study; Designate a lead for Force Protection requirements, S&T, and Acquisition.

Requirements and Integrated System Concepts: Develop Integrated Force Protection Systems Operational Concepts and define Army Force Protection requirements including impacts on FCS and other pending or ongoing programs (WMD, FTTS, etc.).

Intelligence: Develop and begin implementing a plan to increase proactive intelligence capabilities during the threat's pre-attack phase with focus on HUMINT

Doctrine and Training: Develop revised doctrine/TTP and training tools across the full spectrum of Force Protection activities with emphasis on the threat pre-attack phase

Post Conflict Planning and Capabilities: Develop revised tasks, conditions and standards for Army CMO and Phase IV capabilities including the adequacy of Civil Affairs, planning, and force structure; Request a Joint/Interagency Review of post conflict planning processes to be led by the Army with goal of replacing the current ad hoc process.

Modeling and Simulation: Develop a plan to address shortfalls in modeling and simulation support of Force Protection needs

Force Protection Asset Management: Develop a plan to implement non-TDA, non-TOE inventory planning for FP Integrated Systems Components

Technology and Development: Implement the Integrated Systems Concepts defined by TRADOC; Focus Force Protection S&T resources on integrated FP C2, countering specific FP threats and weapons, decision support systems and training systems, automation and robotics, and non-lethal response.

The study concluded that force protection has always been a priority but is now even more central to Army mission success. We found that there are many existing technology solutions to address force protection needs, with other technologies under development that offer greater advances. We identified the technology gaps that should be addressed with focused S&T investments, and discussed the importance of other areas, e.g., intelligence and civil affairs, which have high leverage and are of equal importance to effective force protection. We concluded that an integrated systems approach to force protection is essential, and discussed an opportunity for improving how the Army is organized with respect to force protection. We also found that while improved technologies and procedures are important, effective force protection requires constant diligence from the individual soldier to the commander.



Army Science Board 2003 Summer Study



Force Protection Technologies for the 2010-2020 Timeframe



Terms of Reference

- Review prior Force Protection studies
- Address FP issues during and after deployments
- Identify advanced technologies for the 2010-2020 timeframe to support Force Protection mission
- Use analysis and models to evaluate potential contributions of Force Protection technologies in specific scenarios
- Address FP opportunities and risks associated with the interactions with non-Army organizations
- Based on sponsor input and current events the study is also addressing near term options to improve Force Protection ASAP



Force Protection Study Organization

CO-CHAIRS

SA to Study Chairs
LTC Al Klee, OFTF



Dr. Marygail K. Brauner

Mr. Gilbert V. Herrera

Mr. Frank Kendall

Review of Prior Studies

Dr. Roberta-diane J. Perna

Dr. Lynn Gref
Mr. John Reese

Technology Solutions

Dr. Peter Swan

Dr. Edward C. Brady

Mr. Gary Glaser
Dr. Mark A. Hofmann
Dr. Don Kelly
Dr. Ira Kohlberg
Dr. Steven E. Kornguth
Dr. Peter Lee
Ms. Ginger E. Lew
Dr. Richard Montgomery
Dr. Reed L. Mosher
Mr. Mike Toscano
Dr. Jack Wade
Mr. Randy Woodson
Dr. Al Grum
Dr. Prasanna G. Mulgaonkar
Mr. John Reese
Mr. Paul Tilson
SA Mr. Jim Wisniewski
CDT Heather Ritchey
CDT Adam Tritsch

Vulnerability and Threat Assessment / Intel Requirements

Dr. Anthony K. Hyder

Dr. Seth Bonder
Mr. Milt Finger
Dr. Roberta-Diane J. Perna
Dr. Elizabeth Stanley-Mitchell
Dr. Michael D. Krause
SA LTC John Fitzpatrick

Analysis / Modeling

Dr. Stuart H. Starr

Mr. Dan Rondeau*
Dr. Ira Kohlberg
Dr. Mike Macedonia
Mr. Dell Lunceford *
Maj. Ted Dugone
Ms. Sarah Johnson *
Mr. Cal Jaeger *
Dr. Tommy Woodall *

Operations

GEN David M. Maddox (USA, Ret.)

Dr. Seth Bonder
Mr. Herb Gallagher
VADM William J. Hancock (USN, Ret.)
LTG Charles P. Otstott (USA, Ret.)
LTG Randall Rigby (USA, Ret.)
SA Ms. Sheryl Ward

Interfaces With Local Governments, Commerce And Infrastructure

Mr. Alan R. Schwartz

Mr. Jerome S. Gabig, Jr.
LTC Ferdinand Irizarry
Mr. Richard Ladd

RED TEAM

Dr. Michael A. Wartell

Dr. Amy Alving
Mr. John McDonald
Dr. Joan Woodard

Force Protection

* Corporate Advisor

Co-Chairs in bold

Gov Advisors in Italic



Outline



- **Study Vision and Scope**
- **Prior Studies of the Problem**
- **Our Approach and Key Conclusions**
- **The Force Protection Problem: Threats, Environments and the Operational Needs**
- **Opportunities to Apply Technologies to the Problem: Generic Cases and Integrated Systems**
- **Seeking Leverage: Opportunities Beyond Direct Technology Investments**
- **Recommendations and Conclusions**



Force Protection Vision



Soldiers, civilian employees, dependents, facilities, information, and equipment are protected in all locations/situations at acceptable manpower/costs while successfully performing missions

This vision can be achieved through the following:

- ❖ **Broad, immediate, and thoughtful application of available technologies**
- ❖ **Army S&T program focused upon on gaps, and leverage S&T work from other agencies/entities**
- ❖ **Force protection requirements/technologies integrated into FCS and other new platforms**
- ❖ **Stability and Support Operations that improve force protection effectiveness**
- ❖ **Reliance upon improved technologies/procedures, but continued diligence from the Soldier to the Commander – *Every Soldier is a Sensor***



Scope of This Study

- Threats ranging from terrorists trying to create mass casualties to groups trying to cause sustained low level casualties
- Situations we addressed
 - CONUS
 - Deployment
 - Peacekeeping
 - Stability Operations
 - Rear area security
- Situations we did not address
 - Large scale organized conventional force maneuver operations
 - Global Missile Defense (Theater and National)
 - Broader Homeland Defense and Security issues, and Critical CONUS Infrastructure



Previous Force Protection Studies



- We reviewed documents from the following sources:
 - Selected Joint Staff task force findings
 - Selected Department of the Army regulations and guides
 - Commission reports pertaining to Khobar Towers and USS Cole attacks
 - Previous and ongoing studies completed by DoD Science Boards
 - Studies completed by other governmental entities including Allies
 - Studies at the national security level completed by think tanks and other research institutions
 - Professional publications
 - Reports on peacekeeping and stability operations, including Kosovo, Bosnia, Afghanistan, and Iraq; and reports on the role of contractors

Our Conclusions Are Consistent With And Expand Upon Prior Studies



Our Common Conclusions With Prior Studies



- Existing COTS technologies fill many Force Protection requirements
- Training and doctrine to exploit new Force Protection technologies must be developed
- Force protection is an ongoing training requirement
- Reliable intelligence (particularly HUMINT and interaction with local populace) is critical component of Force Protection
- During operations, Force Protection is largely the responsibility of the individual soldier and commander
- Force Protection must be an integral part of tactical operations
- In post-conflict operations, Force Protection has been impacted by the mixed success in transitioning to stable and secure civilian authorities



We Gathered Information from a Wide Variety of Sources

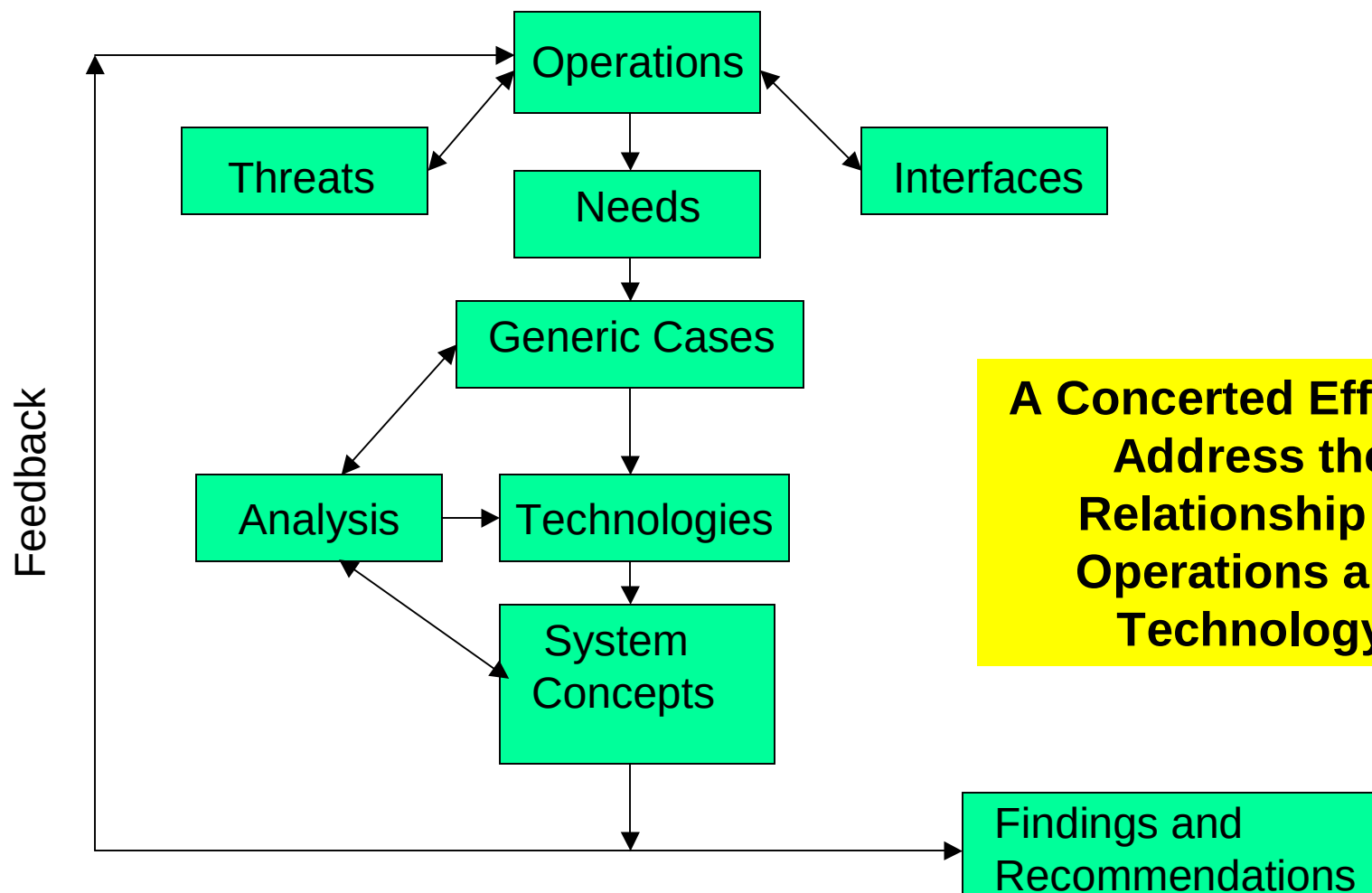


In addition to reviewing past studies, we:

- Received briefings from a wide range of organizations involved in FP including
 - Sponsors
 - DIA, CIA, DTRA, OSD, NGIC
 - G3, National Guard, Army Reserves
- Visited many activities involved in technology development
 - DARPA, Sandia, UT Austin, ARL, NVL, ICT, JPEO/CBD, etc.
 - Force Protection Equipment Demonstration—Quantico
- Visited Ft. Myer, Kirtland AFB, and Ft. Hood



Force Protection Study Methodology



**A Concerted Effort to
Address the
Relationship of
Operations and
Technology**



Principal Conclusions of the Study



- Force Protection has always been a priority and is now even more central to Army mission success
- Technology offers great opportunities for improving Force Protection
 - Integrated system solutions should be pursued
 - Existing technology offers significant opportunities now and technologies in development offer even greater advances
 - There are a small number of capability gaps that need to be addressed by S&T investments
- Additionally, actions beyond direct technology applications have high leverage and are equally important
- The Army has an opportunity to improve the way it is organized to address Force Protection



Characteristics of the Threat



- Types of threats considered: terrorists, military and paramilitary forces, independent actors
- Threat objectives vary; but generally have a political (not military) focus
 - Increase their political power, image and influence
 - Destroy U.S. political commitment to the mission
 - Gain attention by inflicting casualties or destroying high value targets
- Threat methods also vary widely
 - Some conduct detailed pre-attack planning and surveillance
 - Some attack opportunistic targets
 - Weapons range from WMD to conventional to improvised
- Common threat characteristics
 - Has the initiative – the advantage of choosing time, place and method
 - Capitalizes on our predictability and structure
 - Focuses on our most vulnerable assets
- Significantly different problems in CONUS, OCONUS, or post-conflict operations



The Current Force Protection Situation: CONUS



- Strong emphasis on installation physical security and access control
 - Investing in COTS, fencing/barriers, monitoring systems, and gate/access control automation
 - Generally not buying fully integrated security systems; selected improvements
 - Employing manpower-intensive FP measures
- Manpower costs are high but are hard to measure
 - Visible and invisible costs
 - Taking increased manning out of hide
- Strategy seems to be to deter attacks without over-penalizing access
 - Effectiveness of physical security investments is not clear
 - Not clear we are conducting aggressive red-teaming of our defenses



Army Operations Are Manpower Intensive



**MOB CAP
168,003**

FORCE PROVIDER	MOBILIZED ISO NOBLE EAGLE	MOBILIZED ISO ENDURING FREEDOM	ACTIVE FEDERAL SERVICE TOTALS
ARMY NATIONAL GUARD	17,502	50,921	68,423
ARMY RESERVE	3,591	55,488	59,079
IMA SOLDIERS MOBILIZED	430	1,505	1,935
IRR SOLDIERS MOBILIZED	166	527	693
MOBILIZED RC FORCES ON ACTIVE FEDERAL SERVICE	21,689	108,441	130,130

UNIT MISSIONS:	127,502
WARFIGHTER SUPPORT	87,263
C3I	1,683
FORCE PROTECTION	12,153
MOBILIZATION BASE	1,237
TRAINING BASE	444
CONUS BASE SUPPORT	16,214
AIR FORCE SECURITY (9,500)	8,508

Source: MG Chiarelli

as of 11 Mar 03



Current Identifiable Force Protection Investments



	Total Force Protection (\$000)			Army Force Protection (\$000)		
	FY 2002	FY 2003	FY 2004	FY 2002	FY 2003	FY 2004
Physical Security Equipment	811,771	1,499,293	935,148	216,445	627,813	189,880
Physical Security Site Improvements	226,829	1,835,743	275,830	57,086	318,181	40,265
Physical Security Management and Planning	92,583	130,129	120,927	9,469	8,217	9,357
Security Forces and Technicians	2,631,513	3,612,257	3,582,180	303,982	419,482	297,128
Law Enforcement	1,377,258	1,594,866	2,178,077	693,087	708,770	830,164
Security and Investigative Matters	531,597	637,208	592,773	132,106	149,160	132,465
AT Research, Development, Test, and Evaluation	57,368	160,978	109,310		43,900	34,244
Totals	\$5,728,919	\$9,470,474	\$7,794,245	\$1,412,175	\$2,275,523	\$1,533,503

SOURCE: OSD Combating Terrorism Activities FY 2004 Budget Estimates, 28 April 2003

Force Protection



The Current Force Protection Situation: OCONUS



- Strong emphasis on using organic tactical assets
 - Some ad hoc investments tailored to individual problems
 - Not employing integrated protection systems
 - CS/CSS units have limited Force Protection capabilities
- Manpower costs are high and direct
- Strategy seems to be defend and respond to attacks while continuing operations
 - Experiencing attacks frequently
 - Attacks are achieving some degree of success
 - Inflicting casualties
 - Changing interactions with the community
 - Impacting mission performance



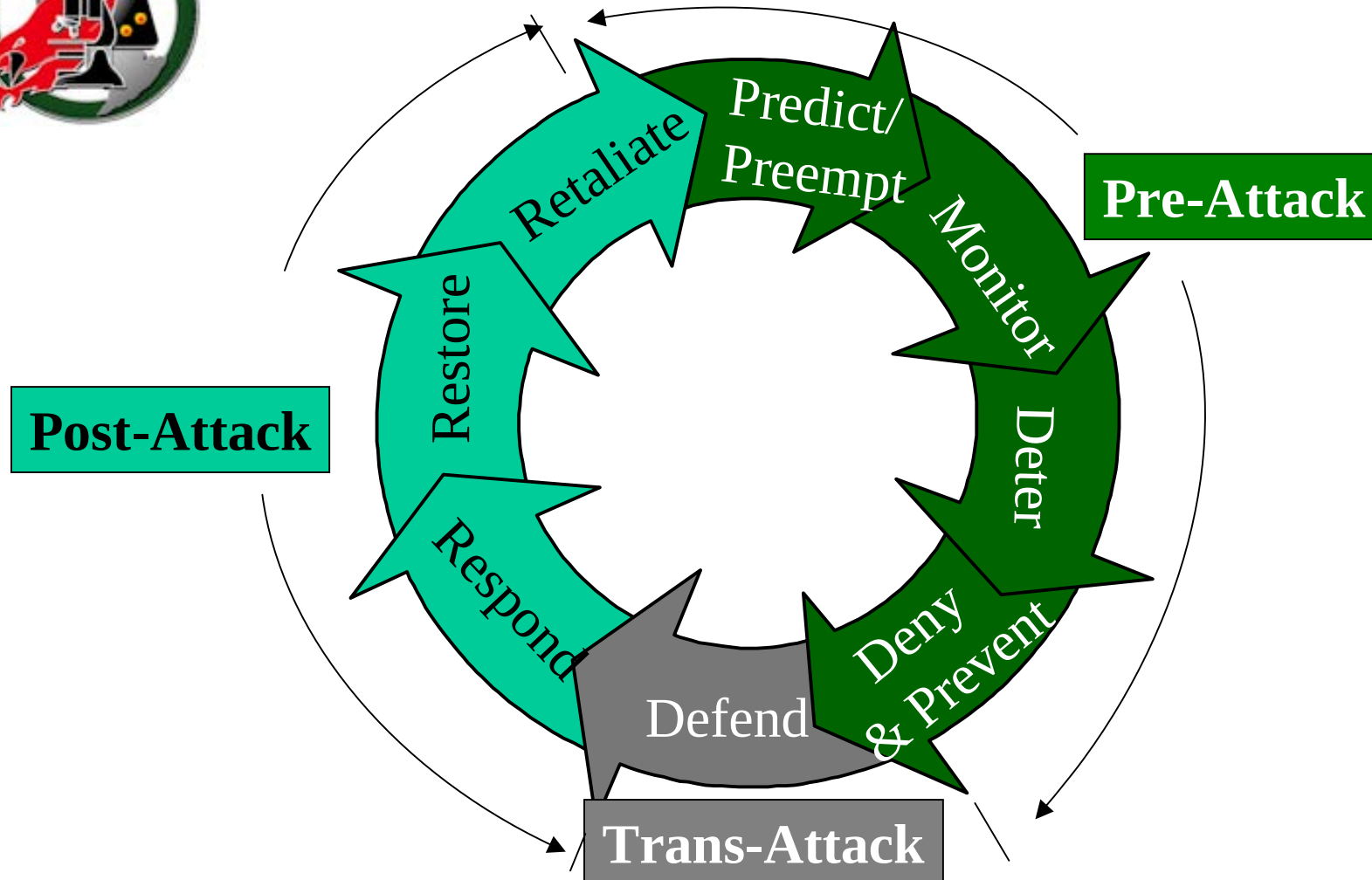
Force Protection In The Post-Conflict and Stability Operations Contexts



- The Force Protection problem is compounded
 - A purely defensive posture is not acceptable
 - Collateral damage is inimical to the core mission
 - Many U.S. and non-U.S. civilian organizations may be present
 - Coalition and indigenous military and constabulary forces may be present
 - There is a dangerous gap between the end of major conflict and when indigenous authorities can provide civil stability
- The problem can not be avoided



The Force Protection Continuum



FP Has To Be Addressed As A Continuum; Not Just Defense
FP Requires An Integrated Systems Response



Generic Cases Were Extracted to Focus Our Work



- A generic case describes an operation with a specific Force Protection environment common to many situations
 - CONUS Base
 - OCONUS Base
 - Small team or detachment
 - Convoy
- Example integrated systems were defined and technologies were applied within those systems



CONUS Base – Integrated FP System



Efficient Access Control



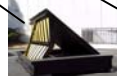
Base Facilities



Perimeter Sensors



Vehicle Inspection



Barriers



HVT



Perimeter Fencing



Integrated C2



Key Features

Emphasis on Deterrence while maintaining reasonable tenant entry during FPCON A&B

Dependence on COTS

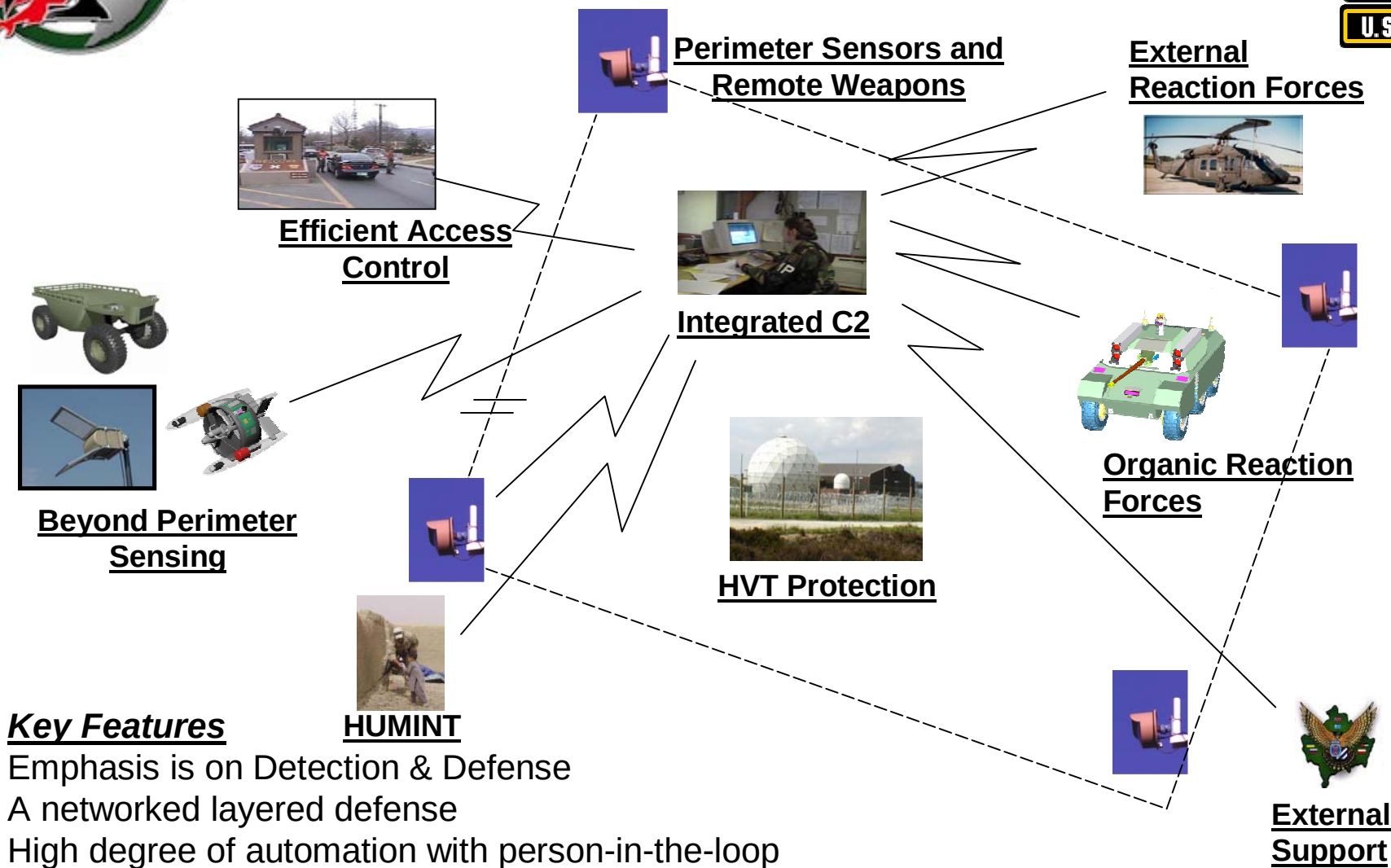
Key relationships with local/federal authorities



Local/Federal Law Enforcement

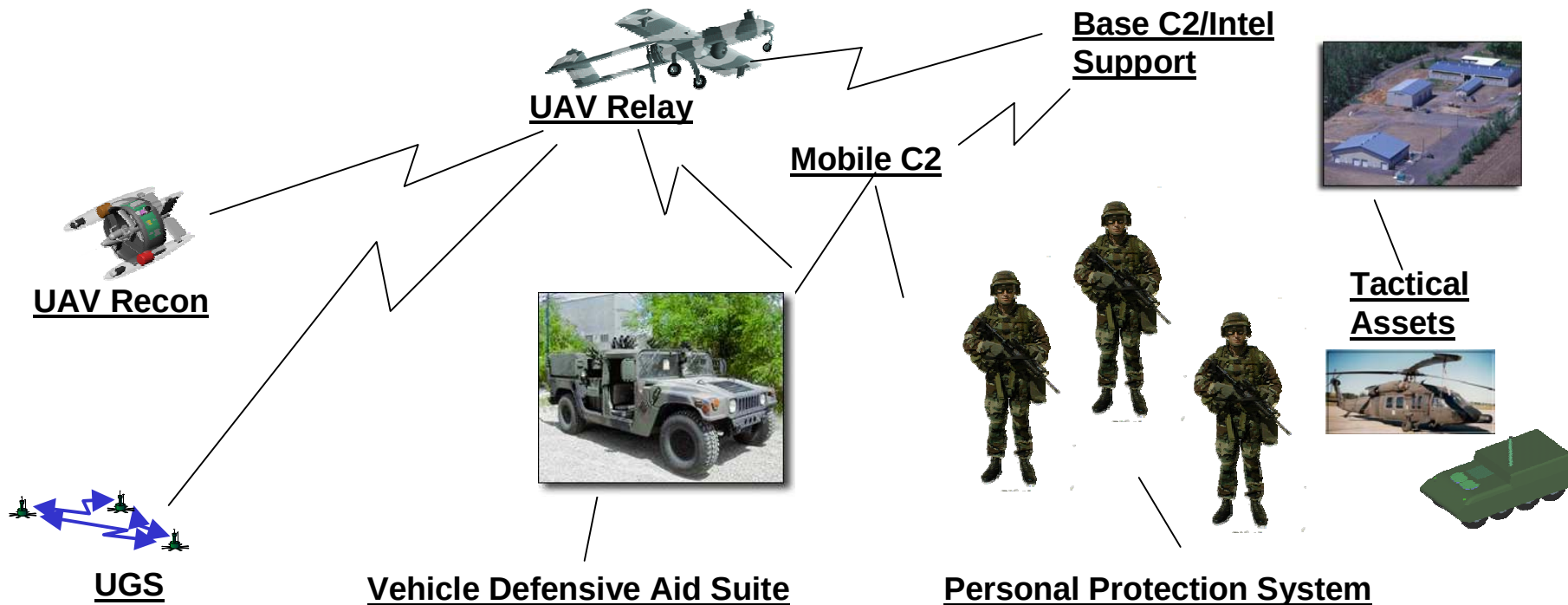


OCONUS Base – Integrated FP System





Small Team or Detachment – Integrated FP System

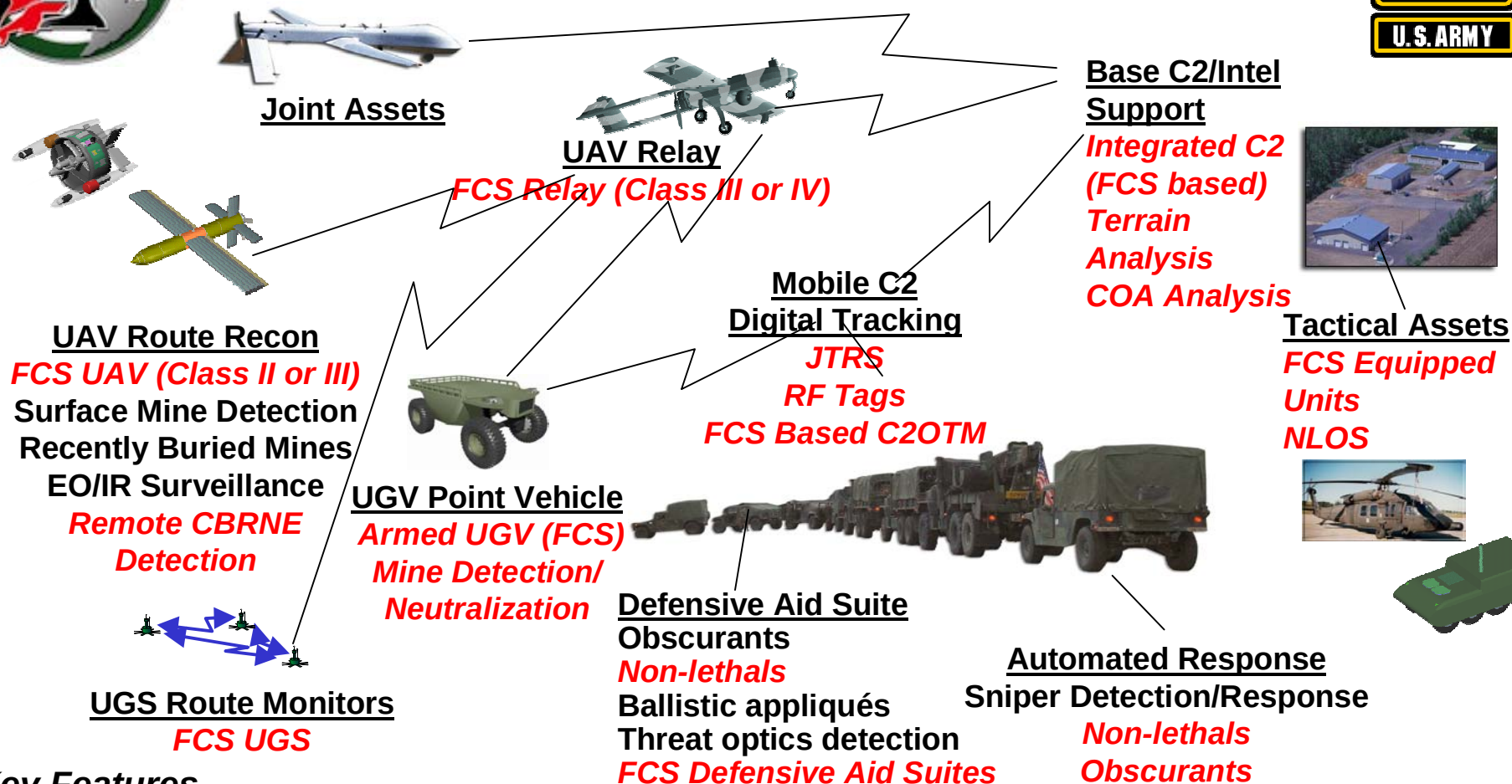


Key Features

- Predict/Detect/Avoid threats with high SA/SU
- Netted-centralized C2 – Base supports multiple teams
- Reliance on assured C2, and defensive suites



Convoy - Long Term Integrated FP System



Key Features

- Predict/Detect/Avoid threats with high SA/SU
- Netted-centralized C2 – Base supports multiple convoys
- Reliance on unmanned systems

* Long term shown in red/ital



Summary of Prioritized Gap-Filling Technologies for All Cases



Can be fielded quickly

- Initial Decision Support System
- Provide Blue SA to individual deployed vehicle level
 - Radio and GPS
 - Digital maps/digital tracking
 - Dynamic RF Tags
- Beyond fence enhanced surveillance
 - UAV/UGV
 - UGS
 - Radar, EO/IR
 - Surveillance detection
- UAV support for convoys
- Comms and GPS for individual soldiers
- Smart access control
- Ballistic appliqués (blankets)
- Sniper detection systems

Can be fielded by 2010

- Advanced DSS and training systems
- Enhanced surveillance with UAVs
 - Advanced sensors
 - Bio/Chem sensors
- Standoff explosives detection
 - Suicide/car bomb detector
- Assured communications and Blue SA
- Mine detection and neutralization on the move
- Advanced surveillance technologies
 - Automated information extraction
 - Micro Bio/Chem detectors
- Automated threat detection and response
- Robotic ground vehicles
- Non-lethals



Semiautonomous/Autonomous Systems for Force Protection



Some systems available now, others could be available within a few years

- Increase the acquisition and insertion of autonomous robotic systems for force protection (for example, MDARS(E) for perimeter defense)
- Create ATDs and sponsor ACTDs with capability to accelerate FP technologies from S&T into operational capabilities
 - Use the ATDs and ACTDs to foster tight coupling between all elements of the S&T community
- Develop the appropriate requirements, metrics, and technology-enabled TTPs
- **Demonstrate air-ground-soldier team in a routine patrol scenario with air-ground robots providing surveillance with minimal human intervention**



Counter Sniper Systems



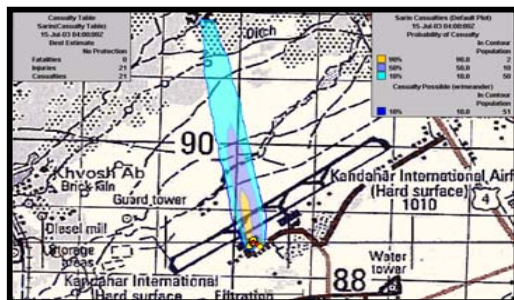
Mobile Counter Fire System



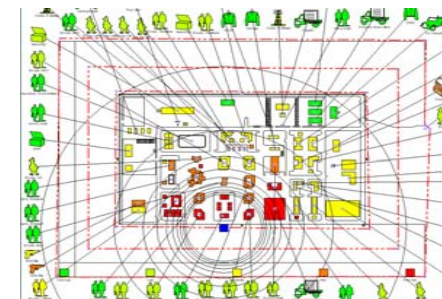
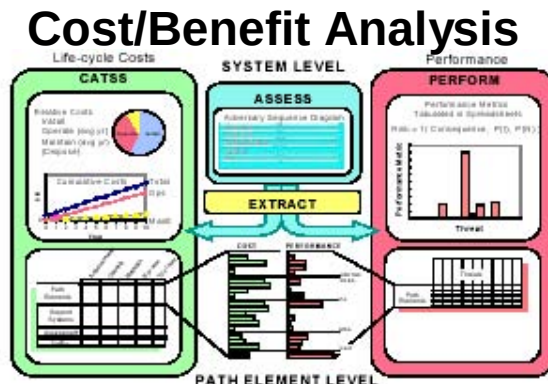
- Systems based upon detection of flash, sound, an/or pressure
- Both counter fires and location detection
- Both Army and Marine R&D programs
- Several foreign systems available



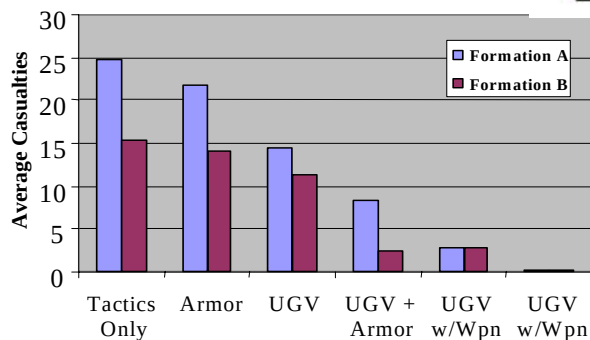
Decision Support Systems Enhance All Aspects of Force Protection



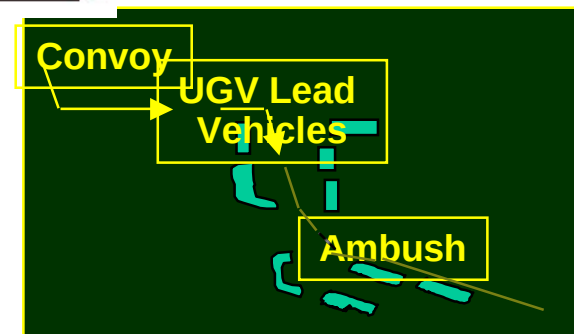
Chem/Bio Attack Effects



Vulnerability Analysis



Technology Options Comparisons



Tactical Operations

A Decision Support System integrates all Force Protection decision tools to assist in Force Protection planning, execution, and training. It utilizes a common architecture to support all levels of Command.



Force Protection Equipment Demonstration



Force Protection Equipment Demonstration IV

Homeland Security: Protecting America's Future

6-8 May 2003
United States Marine Corps Base
Quantico, VA

Office of the Under Secretary of Defense for
Acquisition and Technology and
The Joint Staff

Product Manager, Physical Security Equipment
Fort Belvoir, VA
DSN 654-2416 (703) 704-2416
pmpse@pm-pse.army.mil

PM-PSE
Product Manager, Physical Security Equipment

Logos on the left:
- Army Science Board
- Department of Defense
- Department of Energy
- NIJ
- Transportation Security Administration
- U.S. Department of Transportation
- TSWG



Opportunities Beyond Direct Technology Investment



- High Leverage Opportunities
 - Intelligence
 - Doctrine and Training
 - Civil-Military Operations
 - Modeling and Simulation
 - Management of Force Protection Investments
 - Other Programs



Intelligence

- The three top priority investments in intelligence capability for OCONUS FP are: HUMINT, HUMINT, and HUMINT
 - The highest operational leverage is in pre-attack threat ID and preemptive attack
 - Technical collection has limited utility in anticipating attacks or preempting them
 - The threat's perspective on asset value has to be understood
 - Culture-based analyst training is needed
 - HUMINT operations training and staffing is needed



Doctrine and Training

- Doctrine
 - Current FP emphasis is on physical security and installation security rather than on precluding and responding to attacks
 - There should be more emphasis on integrated Force Protection solutions including pre-, trans-, and post-attack options that include local intelligence, deception, redundancy, unpredictability and effective responses to attack
- Training
 - FP proficiency could be greatly enhanced by increasing its emphasis in all training
 - Real time collaborative distributed simulations for FP would have a high payoff

**Force Protection Improvements Must Include
Doctrine and Training Components**



Civil-Military Operations (CMO)



- Integration with local populations and civilian organizations can be a Force Protection multiplier
 - Particularly important in Phase IV Operations
 - Supports HUMINT
 - Improves situational awareness/understanding
 - Engenders good will
- Increased civil security capacity can assume security burden and lower the threat level
- CMO improvements are needed: better comms (cell phones/radios); training, simulations and exercises; translation capacity

**Effective CMO Provides The Stability Necessary For The Transition
From Military To Civilian Authorities
Which Reduces Force Protection Requirements**



Modeling and Simulation

- Concept Definition and Technology Investment Decision Support
 - Analytical tools to assess investment options
- Education and training
 - Automated tools for FP exercises
 - Collaborative real time simulations for training – soldiers gain from practicing as both blue and red
- Support to operations
 - An integrated family of decision aids
- Assessment/experimentation
 - A flexible tool kit of models and associated data bases for FP experimentation
 - Cost/Benefit, portfolio analysis and risk assessment tools
- Acquisition
 - A Joint FP M&S testbed to support evolutionary acquisition of integrated systems

**There Is Great Potential For Improving
Force Protection Through M&S**



Acquiring Force Protection Equipment: TDA =0, TOE =0



- Force Protection needs are very situation dependent
- Designing modular FP systems for use as appliqué's would permit selective issue to units needing the capabilities
- Units deployed to conduct stability operations should have adequate time to train with issued equipment
- Host systems (vehicles primarily) will have to be modified or designed to accept modular FP systems when issued

**Selected Issue Of Force Protection Equipment Modules
Would Limit Total Inventory Costs Dramatically**



Army Organization for Force Protection Management



- Presently, responsibilities for Force Protection are generally distributed throughout the Army with the exception of the G-3
 - Multiple PM's/PEO's and S&T Managers
 - Multiple branches
 - Generally the local Commander's responsibility
 - Multiple budget accounts without cross-cutting cost-benefit trades
- Some important steps have been taken to centralize management of Force Protection (e.g., the Guardian Brigade, JPEO/CBD, PSEAG and FPAAT), but there are more opportunities
- Cost-benefit analysis is not being applied uniformly to investment decisions
- There are no single leads for Force Protection requirements, S&T, and acquisition

**Force Protection Can Be Improved
Through Additional Organizational Changes**



Other Programs

- Physical Security Industry
 - A multi-billion dollar per year market developing products for commercial sales
 - Significant government investment due to DHS
- WMD:
 - A major investment area for the Country (DoD, DOE, DHS, NIH, etc.)
 - Army priorities have to be communicated and monitored, but there should be little need for additional Army S&T investments
- FCS:
 - The biggest Army technology investment by a large margin
 - Force Protection beyond combat requirements has generally not been defined and integrated into FCS requirements

Army FP Technology Investments Should Be Focused On Gaps, Unique Needs, Integrating COTS/NDI and Leveraging FCS



Recommendations (1 of 3)

Overarching Recommendations:

- Direct an Army-wide effort led from HQDA to improve Force Protection, including the implementation of the recommendations of this study
CSA, now
- Designate a lead for Force Protection requirements
CG TRADOC, 30 days
- Designate leads for Force Protection S&T and Acquisition
ASAALT, 30 days

Requirements and Integrated System Concepts

- Develop Integrated Force Protection Systems Operational Concepts and define Army Force Protection requirements including impacts on FCS and other pending or ongoing programs (WMD, FTTS, etc.)
CG TRADOC with ASAALT, 9 months

Intelligence

- Develop and begin implementing a plan to increase proactive intelligence capabilities during the threat's pre-attack phase with focus on HUMINT
G-2, 6 months



Recommendations (2 of 3)



Doctrine and Training

- Develop revised doctrine/TTP and training tools across the full spectrum of Force Protection activities with emphasis on the threat pre-attack phase
CG TRADOC, 9 months

Post Conflict Planning and Capabilities

- Develop revised tasks, conditions and standards for Army CMO and Phase IV capabilities including the adequacy of Civil Affairs, planning, and force structure
CG TRADOC, 6 months
- Request a Joint/Interagency Review of post conflict planning processes to be led by the Army with goal of replacing the current ad hoc process
G-3, 3 months

Modeling and Simulation

- Develop a plan to address shortfalls in modeling and simulation support of Force Protection needs
DUSAOR, 9 months



Recommendations (3 of 3)



Force Protection Asset Management

- Develop a plan to implement non-TDA, non-TOE inventory planning for FP Integrated Systems Components

ASAALT with G-8, G-4, 6 months

Technology and Development

- Implement the Integrated Systems Concepts defined by TRADOC
ASAALT, 9 months
- Focus Force Protection S&T resources on
 - Integrated FP C2 (including Joint, combined, non–military)
 - Countering specific FP threats and weapons (e.g. indirect fires defense, counter-ambush, stand-off explosive detection, sniper detection and response, countermine, etc.)
 - Decision support systems and training systems
 - Automation and robotics
 - Non-lethal response (Legal and treaty issues must be addressed)

ASAALT with DARPA, 3 months



Principal Conclusions of the Study



- Force Protection has always been a priority and is now even more central to Army mission success
- Technology offers great opportunities for improving Force Protection
 - Integrated system solutions should be pursued
 - Existing technology offers significant opportunities now and technologies in development offer even greater advances
 - There are a small number of capability gaps that need to be addressed by S&T investment
- Additionally, actions beyond direct technology applications have high leverage and are equally important
- The Army has an opportunity to improve the way it is organized to address Force Protection

Past Studies and Select Literature Review Panel Report – Summary

“Men generally die in war when they cannot help it and are defeated by a disadvantaged situation.” --Wu Ch’i

The panel members reviewed and summarized previous studies and other relevant literature at the national security level dealing with Force Protection. Of the thousands of studies and policy papers prepared over the last twenty years, the reviewers only selected those that held relevance to the current study. Unfortunately, time constraints of this 2003 Summer Study precluded the panel members’ review of everything currently in print on the subject.



Previous Force Protection Studies



- We reviewed documents from the following sources:
 - Selected Joint Staff task force findings
 - Selected Department of the Army regulations and guides
 - Commission reports pertaining to Khobar Towers and USS Cole attacks
 - Previous and ongoing studies completed by DoD Science Boards
 - Studies completed by other governmental entities including Allies
 - Studies at the national security level completed by think tanks and other research institutions
 - Professional publications
 - Reports on peacekeeping and stability operations, including Kosovo, Bosnia, Afghanistan, and Iraq; and reports on the role of contractors

Our Conclusions Are Consistent With And Expand Upon Prior Studies

Force Protection

DRAFT - Not for Distribution without Permission from the
Army Science Board (ASB) Executive Secretary

All the literature reviewed identified the following common themes:

- Intelligence Issues and Technology
- Weapon Delivery Issues
- Weapon types Issues
- Classes of Targets
- Technology Status to Counter Threats
 - o Bombs (explosives)
 - o Mines and Booby-traps

- o Rifle – MG and PRG Class
- o Mortar/MRL/Missile
- o SAM/ Anti-air
- o Chem/Bio
- o Chemical Storage and Transportation
- o Contamination of Supplies
- o Information Operations

The panel reviewed documents from Joint Staff task force findings, as well as Department of the Army regulations and guides. The Downing Report on the Khobar Towers attack remains the seminal document in Force Protection and was the genesis of important changes within DoD particularly as they pertain to installations. Similarly, the USS Cole Commission also provided impetus for change in areas directly related to forces in transit.

Previous and ongoing studies completed by other DoD Science Boards, other government entities, think tanks, and other research institutions provided additional background in which to frame the 2003 ASB Summer Study. All studies highlight the importance of the human in the loop for effective Force Protection. As well, the studies stress the importance of synchronized offensive and defensive measures—key enablers for the Army to complete its mission successfully.

While the recommendations contained in prior studies have already been implemented, many represent stand-alone improvements not well integrated into existing procedures. In its review of other documents, additional assessments completed at the HQDA level delineate how the Army must proceed and include:

- Clearly establishing Force Protection responsibility
- Controlling access to installations
- Properly manning, training, and equipping installation Force Protection personnel
- Leveraging technology for rapid information fusion and dissemination
- Continuing how the Army as a whole thinks and acts is crucial to effective Force Protection and includes:
 - o Individual awareness
 - o Offensive mind-set
 - o Direct Command involvement

Additional recommendations from other Science Boards studies included:

- Emphasize Force Protection as a mission responsibility
- Expand scope and breadth of vulnerability assessments
- Demand synergy among policy, plans, and programs
- Create investment strategy
- Frame a 5-year technology plan around architecture study and integrated technology test bed
- Enhance intelligence operations for Force Protection

Of particular interest are four GAO reports issued in the past six years. Two of these reports contain finding and recommendations pertinent to today's security environment. As late as November 2002, the GAO recommended the following actions to guide Services' antiterrorism efforts at installations:

- Performance goals that are objective, quantifiable, and measurable
- Resources to achieve the goals
- Evaluation plan to compare program results with established goals
- Actions needed to address any unmet goals
 - Secretary of Defense direct the Service Secretaries to require installation commanders to document all threat, vulnerability, and asset criticality assessments; and, periodic higher headquarters evaluations of the methodologies used by installations to conduct their threat, vulnerability and asset criticality assessments

An additional GAO study dated July 23, 2002 identified two significant weaknesses associated with the DoD's Force Protection process for deployments through domestic seaports, namely:

- DoD lacks central authority for overseeing, coordinating, and executing force protection measures while military forces deploy from domestic installations through U.S. seaports
- DoD relinquishes control over its military equipment to non-DoD entities, including foreign-owned ships crewed by non-U.S. citizen during some stages of deployment

The two other GAO reports predate 9-11 but contain findings relating to:

- Despite actions taken, considerable risks remain for Overseas Forces (July 19, 2000)
- Testimony relating to overseas locations where U.S. forces are considered to be at high risk of attack such as Bahrain, Kuwait, Saudi Arabia, and Turkey (October 28, 1997)

Additionally, the panel reviewed relevant Force Protection procedures from the Army's Sister Services and the Coast Guard Initiatives implemented in the aftermath of September 11, 2001 attacks. Findings highlighted the need for specific threat identification, threat analysis, and methods for developing performance standards to plan for response to maritime threats. Many of these findings apply to major areas of Army Force Protection for forces in transit and interim staging areas.

Articles in print discuss the belief that Force Protection is a state of mind that requires constant input, analysis, and modification by all leaders, soldiers, and staff to meet the demands of a dynamic operational environment. Most nations, especially those participating in IFOR, SFOR, and KFOR operations have adopted force protection policies based on their individual national doctrine. Some authors suggest that the British posture represents most of these nations' approaches while the U.S. posture is the exception. Evidence suggests that U.S. and British Force Protection doctrine is similar. The major difference is that British doctrine explicitly includes combat while U.S. doctrine covers non-combat operations in a combat zone. However, the points raised in the articles were anecdotal and the panel members could not find any official information to support the views expressed by the authors.



Our Common Conclusions With Prior Studies



- Existing COTS technologies fill many Force Protection requirements
- Training and doctrine to exploit new Force Protection technologies must be developed
- Force protection is an ongoing training requirement
- Reliable intelligence (particularly HUMINT and interaction with local populace) is critical component of Force Protection
- During operations, Force Protection is largely the responsibility of the individual soldier and commander
- Force Protection must be an integral part of tactical operations
- In post-conflict operations, Force Protection has been impacted by the mixed success in transitioning to stable and secure civilian authorities

As the role of the U. S. Army transforms into the future, the future of Force Protection will also change. The Army has already shown that it has innovative and adaptive leaders, but America's enemies are adapting as well. As a result, attacks will become even more asymmetric than previously encountered, and adversaries will target weakness not strength. Force Protection then must remain the focus of numerous intensive studies and provide the subject matter for journal articles. However, recommendations and conclusions are not enough. The Army must also implement those recommendations. The Literature Review panel members reviewed only a finite number in preparing this summary. Nonetheless, we believe that the conclusions reached in the 2003 ASB Summer Study are consistent with and expand upon these prior studies.



Threat and Operations Panels



Army Science Board Summer Study 2003 Force Protection

- There is a premium placed on addressing surprise
- Intelligence must narrow the space (time and place) in which surprise can occur
- Intelligence must iteratively assess the possible responses to a commander's proposed courses of action
- Never learn twice what you can learn once

Force Protection Study

Threat – Operations Panel

1

This report provides the results of the combined Threat and Operations Panels. The inextricable linkage between threat and operations required close interaction between panels. As a result members from both panels worked jointly throughout this study.



Panel Members



• Threat Panel

- Tony Hyder
- Milt Finger
- Robbi Perna
- Elizabeth Stanley-Mitchell
- Michael Krause

• Operations Panel

- David Maddox
- Seth Bonder
- Charley Otstott
- Herb Gallagher
- Randy Rigby
- Bill Hancock

• Support

- LTC John Fitzpatrick
- Sheryl Ward
- Steve White

Force Protection Study

Threat – Operations Panel

2

This chart provides the names of the members of each panel and our support staff.



Force Protection (FP) Definition



Using DOD 2000.16 as a basis, FP is defined as acts designed to protect Service members, civilian employees, family members, facilities, information, and equipment in all locations and situations

Force Protection Study

Threat – Operations Panel

3

Various definitions exist for force protection. For this study, we used the definition of force protection contained in DOD 2000.16.



Current FP Environment



- Rather than prediction and prevention, our major emphasis is on physical protection of assets subjected to attack
- Current solutions to FP are manpower intensive and generally use inadequate low-technology approaches
- The full manpower cost of FP is obscured by soldiers performing this function as an additional duty
- Our structured and predictable methods of operations create vulnerabilities
- Small units and individual soldiers are our most vulnerable elements
- FP efforts often are at the expense of mission accomplishment

Force Protection Study

Threat – Operations Panel

4

Examining force protection requires an understanding of the environment in which new solutions can be proposed. In our assessment, the primary effort of current force protection focuses on the physical protection of an asset . . . an equivalent to considering survivability as only ballistic protection, instead of multi-faceted in which knowledge can be traded for ballistic protection. In

short, the current approach focuses on reducing the probability of kill, given a hit, rather than reducing the probability of a hit.

Currently, the primary method to provide force protection requires large numbers of soldiers. Many of these soldiers perform this function as an additional duty and, as a result, tend not to be counted in the list of people performing this function. Hence, we do not fully understand the total manpower cost.

We pride ourselves with standard and consistent ways of performing military tasks. Unfortunately, this consistent behavior is also a vulnerability because it provides an opponent with an easy way of attacking a U.S. military target. Further, the lack of inherent protection of individuals and small units makes them lucrative targets.

Achieving force protection by diverting additional people to this mission and operating from more secure sites can adversely affect mission accomplishment. Bosnia provides a good example. We isolated our forces in secure areas where they could not accomplish their mission and then required four vehicles to move them around when ordinarily the mission only required one vehicle.

 MILITARY MANPOWER REQUIREMENT BY FPCON 					
Post	Normal & Alpha	Alpha + 33&38	Bravo	Bravo + 33&38	Charlie
All CONUS	9,089	10,263	11,521	14,883	18,289
Hood	771	665	767	1,300	1,402
Lima	55	63	74	77	101
Meade	130	143	155	181	193
Monroe	91	90	102	198	261
Red River	43	86	133	259	334
Rucker	239	77	335	460	559
Sam Houston	173	173	260	377	377
Selfridge	62	82	143	174	209
USMA	26	79	125	137	248
Hunter Liggett	37	54	54	51	86
McCoy	71	93	93	114	160

Force Protection Study
Threat – Operations Panel

5

This chart shows the Army military manpower required for installation security in the U.S. and how it increases as the force protection threat level increases. At FP condition C, the Army must commit the equivalent of more than a combat division to this mission.

The columns showing “33 and 38” reflect added security measures. *Measure 33* requires checking the identification of all personnel entering the installation; visual inspection of the interior of all vehicles, and inspecting the exterior of suitcases, briefcases, and other containers; plus increasing the frequency of searches

Measure 38 requires erecting barriers to control traffic flow and protect buildings.



Vision . . .Where We Want To Be



Soldiers, civilian employees, family members, facilities, information, and equipment are protected in all locations and situations at acceptable manpower and costs while successfully performing missions



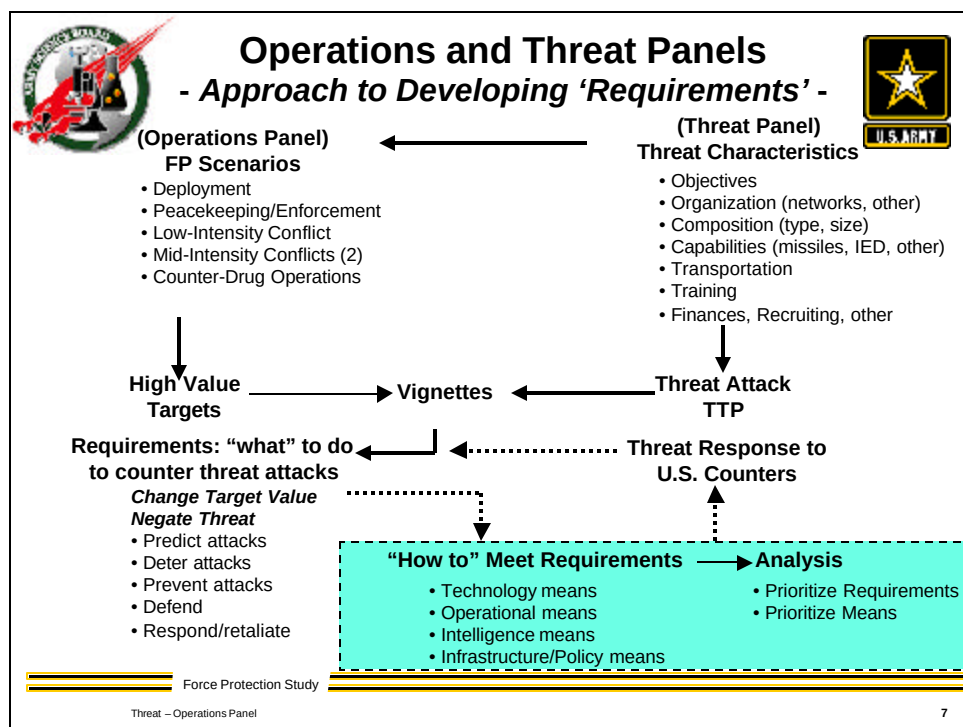





Force Protection Study

Threat – Operations Panel
6

To attain an objective requires a vision of both the objective and the desired outcome. This slide lays out Force Protection visions that we wish to achieve.



This ASB Summer Study is a complex endeavor involving the expertise of operations, threat/intelligence, technology, infrastructure/policy, and analysis professionals. Development of meaningful recommendations required that the deliberations of these experts and panels be carefully integrated during the course of the study. The approach to achieving this integration

was based on the concept of first developing “requirements” (“what is needed?”) to improve FP and then determining the “means” (“how to”) to achieve these requirements. This slide provides an overview of the process used to develop the requirements via an integrated effort of the Operations and Threat panels.

The process began with the Threat Panel identifying threats for a spectrum of regions worldwide and then developing a list of characteristics for each threat. Characteristics included the threat’s objective and specific information regarding the threat’s organization, size, types of weapons, delivery means, etc. This information was used to determine what kinds of U.S. assets the threat might attack to achieve its objectives and how it might prosecute the attacks (i.e., TTP)

Using the threat information, scenarios were developed by members of the Operations Panel to provide the general context to think about the problem of protecting U.S. forces deploying from CONUS installations and operating in an overseas theater. Scenarios were developed for a spectrum of missions (peacekeeping, nation building, low intensity conflict, etc.) and different theaters of operation (Bosnia/Kosovo, Afghanistan, Iraq, etc.). A separate scenario was developed for the deployment phase of an overseas operation. Each scenario further described the general nature of the threat (from the Threat Panel) and the environment (terrain, infrastructure) for each operation. The intent was to develop specific scenarios (with their associated missions, regions, threats, and environments) which would be stressful for FP capabilities so that other possible scenarios would be interpolated realizations and thus less stressful for FP capabilities.

Using the scenarios and information regarding the threat, former senior U.S. Army commanders (on the Operations Panel) identified a set of “high value” targets which, if attacked successfully, would significantly degrade the mission of U.S. forces in the region. Simultaneously, Threat Panel members identified a set of “high value” targets, which if attacked successfully, would greatly enhance threat objectives in the region. Both sets of high value targets (U.S. and threat perspectives) for all of the missions and regions were then combined into a composite set appropriate for the complete scenario space.

Using the high value target to be protected and the threat TTP, the former senior U.S. commanders then developed “vignettes” to understand how the threat could employ its forces, weapons, and delivery means to attack each of the high value targets. The vignettes were then used in a process to develop “requirements” describing “what” the U.S. should do to counter threat attacks against the high value targets (i.e., significantly enhance FP capability). A small set of the requirements addressed ways to reduce the value of a high value target and thus make it less attractive for the threat to attack. Most of the requirements focused on ways to negate the threat’s capabilities by leveraging his vulnerabilities and areas of weakness. This led to requirements across all elements of the “FP cycle” from predicting attacks to responding and retaliating to them.

Although not part of the Operations and Threat Panels’ requirements process, as shown in the exhibit, other panels developed various ways (e.g., technology means, operational means, policy means, etc.) of meeting the requirements. The “means” were then reviewed by members of the Threat Panel to learn if and how a potential threat might respond to degrade these improvements in U.S. FP capability and if such responses warrant changes in the requirements. Finally, it was intended that quantitative analyses be performed to prioritize the requirements and the means of achieving them.



The Threat



- **Consists of military units, paramilitary units, terrorists, and anti-American groups and individuals opposed to the U.S. military action**
- **Includes small regular and paramilitary units assigned specific targets**
- **The regular units can include special operating forces targeted against very specific high value targets, or small units with artillery, air defense, and electronic warfare capabilities**
- **Non-combatants, armed or unarmed, may be in these groups opposing our actions**

Force Protection Study

Threat – Operations Panel

8

The threat is extremely varied, ranging from organized military or paramilitary units to non-combatants. As a result, the threat's composition and modus operandi varies widely, as well. The kinds of threats the United States could face, depending upon the situation include:

Organized regular military units, ranging in size from squads to large unit formations, with conventional military capabilities

Small special operating forces, with sophisticated capabilities in electronic warfare, psyops, explosives and long-range reconnaissance

Paramilitary or rebel police forces or militias

Hostile foreign intelligence services

Organized criminal organizations, including drug traffickers, mafia syndicates, criminal gangs, and smuggling rings

Religious and ethnic extremists or nationalists

Terrorist groups, ranging from small, localized gangs to large, sophisticated international networks with sleeper agents or suicide bombers

Non-combatants, including anti-American sympathizers, dissident groups, computer hackers and villagers pressed into action by other threat organizations



Characteristics of the Threat



- The threat has easy access to a wide variety of modern weapons
- The threat currently focuses on our most vulnerable assets
 - The threat will usually choose an asymmetrical strategy
 - Avoiding our strengths means small units and individual soldiers are a high priority target
- The small-scale attack can have greater strategic impact over the long term than tactical impact (in shaping or diminishing U.S. national will)
 - Threat's major objectives are usually political, not military
- The threat capitalizes on our structured and predictable methods of operations
- The threat has the initiative – the advantage of choosing time, place and method

Force Protection Study

Threat – Operations Panel

9

Given the varied threat, it is difficult to generalize about the various weapons and TTPs that it will employ. Nonetheless, there are some common themes across all of the potential threat groups. First, the threat has access to a wide variety of modern weapons through the commercial marketplace.

Second, the threat is most likely to attack U.S. vulnerabilities with an asymmetrical strategy – focusing on our weaknesses rather than our strengths. Given U.S. Army doctrine, this frequently targeting individual soldiers or small detachments, or our dependence upon communications and computer networks. Most adversaries are aware of U.S. doctrine and methods of operations. As the deployed U.S. force develops routines, this vulnerability becomes even more acute.

Third, even the least sophisticated adversary knows that he can eventually achieve his aims through long-term, small-scale attacks on individual soldiers. While these targets of opportunity do not really affect U.S. tactical effectiveness, they can create fear among the deployed soldiers, lead commanders to take more defensive postures, and whittle away at U.S. national will to continue the operation. From the threat's perspective, each of these reactions is very important, because the threat is rarely interested in achieving military success. Rather, the threat is usually attempting to achieve political goals. The next slide will discuss.



Threat Objectives



- **Increase their political power, image, and influence**
- **Destroy U.S. political commitment to the mission**
- **Impede U.S. force deployment**
- **Degrade effective U.S. military capability once deployed**

Force Protection Study

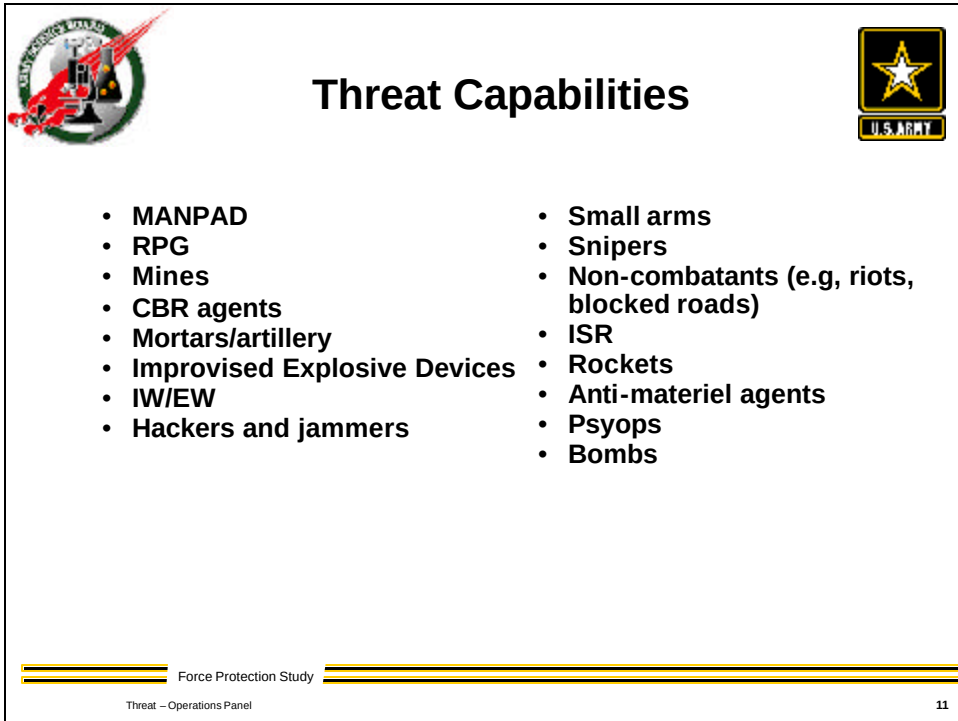
Threat – Operations Panel

10

The threat's major objectives are often not directly related to the U.S. deployment at all. Rather, the threat is usually trying to increase its own political power, image, or influence – locally and sometimes even internationally. Given this objective, opposing the deployed American forces can be very important for achieving other political goals. If the United States leads in the deployed coalition, targeting the leader's troops can send a strong message that the threat does not approve of the reason for the deployment. Alternatively, because much of the international community believes that the U.S. is extremely casualty adverse, targeting American troops can be seen as "sending a shot across the bow" of such an important world power, something that raises the threat's prestige and influence at home and abroad.

Because the threat is so varied, the threat's objectives are also varied. Nationalist groups or military forces may oppose a peace settlement or a newly elected government, or may want to increase international support for their own faction or cause. Terrorist groups may want international recognition for their political or religious beliefs, and use high-profile events to raise money or recruit new members. Criminal organizations may want to make money or create new channels for influence in their local governments. Military and paramilitary units may feel disenfranchised from the new government and oppose being dismantled to create a new national military or police force.

None of these objectives relate directly to the U.S. deployed forces, but targeting the U.S. deployed forces provides a means for achieving the broader objectives. Therefore, the threat will try to destroy U.S. political commitment to the mission and impede U.S. military effectiveness in deploying and carrying out the mission.



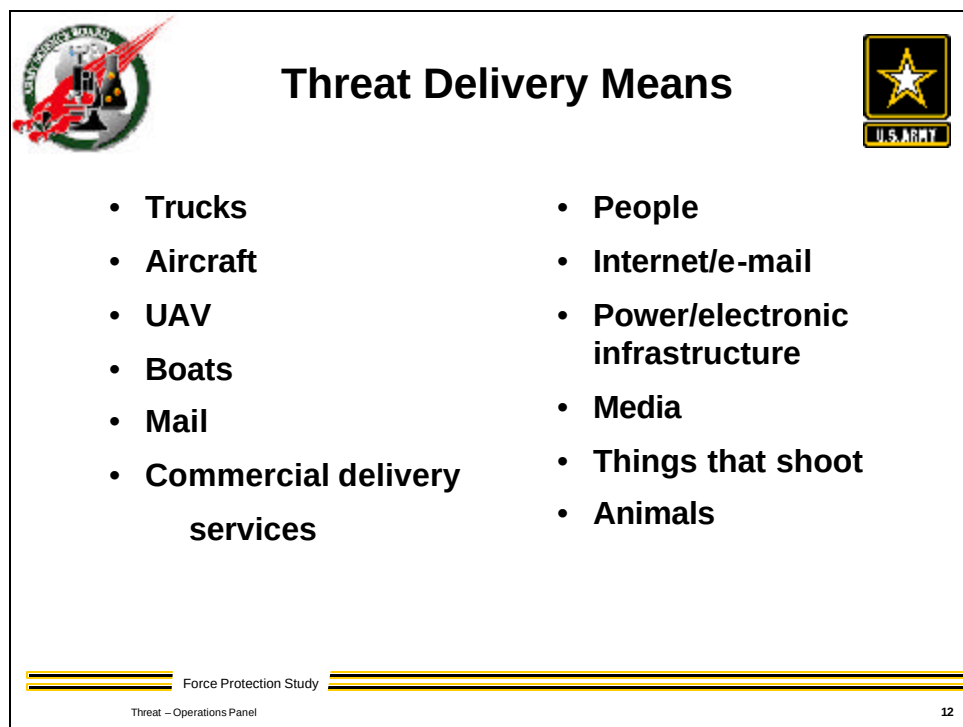
Threat Capabilities

- MANPAD
- RPG
- Mines
- CBR agents
- Mortars/artillery
- Improvised Explosive Devices
- IW/EW
- Hackers and jammers
- Small arms
- Snipers
- Non-combatants (e.g, riots, blocked roads)
- ISR
- Rockets
- Anti-materiel agents
- Psyops
- Bombs

Force Protection Study
Threat – Operations Panel

11

As stated previously, the threat has access to a wide range of modern weapons, including those listed here. Improvised explosive devices include suicide bombers. Non-combatants include demonstrators, human shields and people who have been taken hostage by other threat groups.



Threat Delivery Means

- Trucks
- Aircraft
- UAV
- Boats
- Mail
- Commercial delivery services
- People
- Internet/e-mail
- Power/electronic infrastructure
- Media
- Things that shoot
- Animals

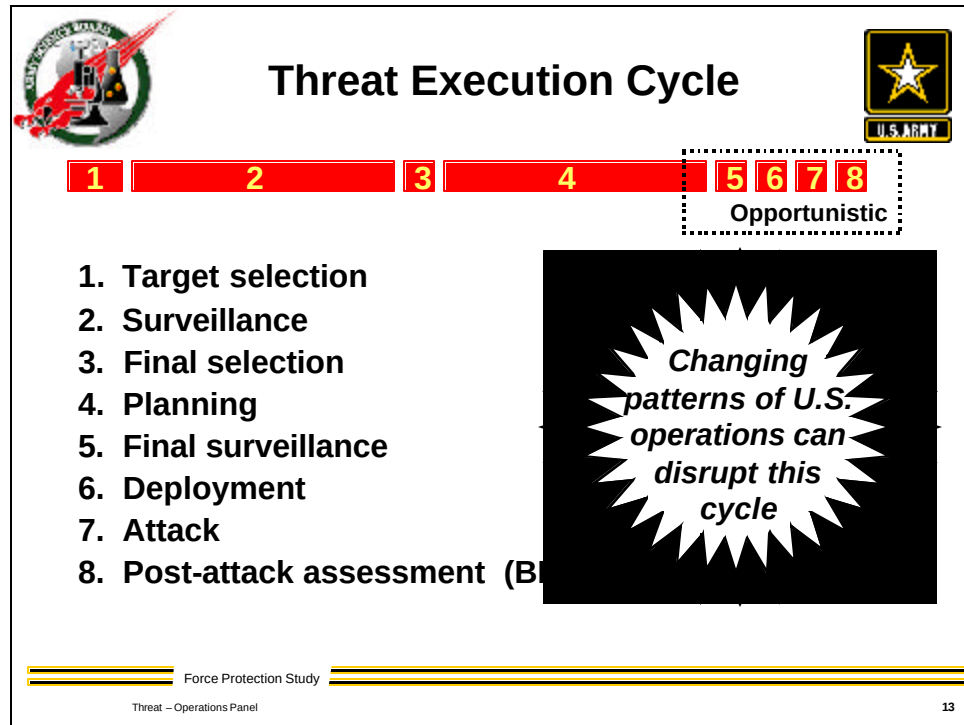
Force Protection Study
Threat – Operations Panel

12

The threat also has a wide variety of means to deliver the weapons and other capabilities shown on the previous slide. In fact, most of the weapons described can be delivered by most of these delivery means, creating a large matrix of potential threat capabilities. For example, bombs can

come by truck, aircraft, UAV, boat, mail or commercial delivery service, animal or human (suicide bombers). This makes the ability to anticipate the attack all the more difficult.

Most of these delivery means are self-explanatory. The “things that shoot” category includes artillery tubes and rockets.



This slide shows the threat’s execution cycle for planning and executing an attack. There are two major points to take away from this diagram.

Some of threats, especially terrorists and organized military or paramilitary forces, engage in a lengthy, deliberate process before they attack. They select targets after careful surveillance and conduct deliberate planning and coordination before the attack. For these threats, phases 1-4 can take a long time, and the threat is vulnerable to U.S. countermeasures during this period. Other kinds of threats, especially individuals or small, disorganized groups, act more opportunistically, without the long lead time of planning and surveillance, as the box around phases 5-8 suggests.

In dealing with the deliberate planning threat, if U.S. forces invest in the capability to predict and monitor, the U.S. can interrupt the threat’s cycle. Moreover, if the U.S. forces change their routines, they can also make it difficult for the threat to act according to its plans. Unfortunately, if the threat’s cycle is interrupted, it may lead the threat to become more opportunistic. This is both good and bad news. The good news is that opportunistic attacks are by their very nature smaller, with fewer casualties and have less operational impact. The bad news, however, is that the U.S. has fewer proactive countermeasures available against opportunistic attacks because they are almost impossible to predict ahead of time.

 Threat Methods of Operations 			
Threat	Terrorists	Paramilitary or military units	Individuals or small groups
Threat execution cycle	Deliberate planning and surveillance; long lead-times; detailed post-attack assessment	Deliberate planning, but with shorter lead-times; limited post-attack assessment	Little if any pre-attack planning; opportunistic encounters
Most likely U.S. targets	Fixed installations, choke points (CONUS or OCONUS friendly nations), and specific key individuals (VIPs)	Military units, fixed installations, choke points (theater of operations), convoys along routine routes	Small detachments, individual soldiers, convoys along non-routine routes, other targets of opportunity
<i>The threat is not monolithic</i>			
Force Protection Study Threat – Operations Panel 14			

This slide builds on the distinction between threats that operate with deliberate planning and those that operate opportunistically. We have grouped the threat into three categories: terrorists, who operate with the most deliberate pre-attack planning and surveillance; paramilitary and military units, who conduct planning and surveillance, but usually over a shorter period of time; individuals and small groups, who operate more opportunistically.

As we suggested on the previous slide, individuals and small groups are generally more disorganized in their operations. They rarely have military objectives in their attacks. Because their attacks are smaller scale, they are generally considered less significant to U.S. mission accomplishment.

Because these threats operate differently, on different planning and execution cycles, they also attack different kinds of targets. The deliberate planners tend to attack targets where long-term, deliberate planning and surveillance can pay off: fixed installations, choke points, VIPs and convoys that follow very routine routes and schedules. In contrast, the opportunistic threats take advantage of targets of opportunity: individual U.S. soldiers or small detachments, like civil affairs teams, guard posts, small patrols, or isolated radio relay sites.



The Threat's Potential Operational Impact



- **Creates casualties which degrades effectiveness and erodes national commitment**
- **Diverts people and equipment from other missions and tasks**
- **Increases “overhead” associated with all operations**
- **Impedes force deployment**
- **Forces commander into a more defensive posture, including asset consolidation**
- **Changes nature of interaction with the community**
- **Decreases soldier confidence and increases anxiety and stress in everyday operations**

Force Protection Study

Threat – Operations Panel

15

This slide outlines some of the direct and indirect ways that the threat can affect U.S. operations. In a direct sense, the potential for attack from the threat increases the overhead associated with all operations, because it diverts people and equipment from other missions and tasks. Commanders also become more reactive and defensive by consolidating their forces into smaller areas. This makes the forces even more vulnerable to attack in the future in two ways. First, it creates a larger high-value target for the enemy to attack because more capabilities are co-located together. Second, it may cause the forces to disengage from the local community as they pull back inside the fence. In turn, this changes the nature of the interaction with the community and makes it even more difficult for the commander to have a sense of the “pulse” of that community. Without that pulse, the commander’s ability to monitor trends in the local community and predict attacks is even further diminished. Although indirect, these effects also impede U.S. operations.

Finally, after an attack has occurred, the threat indirectly affects future U.S. operations. Although individual casualties rarely affect the tactical effectiveness of the deployed force, the fact that an attack has occurred increases fear and anxiety among the deployed forces, which creates emotional and psychological stress that wears on their effectiveness. More importantly, casualties can cause U.S. leaders and the general public to lose their commitment to the operation.



Scenarios



- **The scenarios offer a set of tools dealing with strategic uncertainty**
- **The operational environment is in rapid change preventing a predictable future**
- **The scenarios represent the most stressful dimensions so any subset is less stressful**
- **The basis for identifying high-value targets, and subsequently, requirements for FP**

Force Protection Study

Threat – Operations Panel

16

Developed the scenario outlines to scope the full range of force protection issues across the spectrum of conflict in different geographic environments. Scenario outlines specified the mission of the forces; the threat in that particular area; and a description of the operational environment covering terrain, infrastructure, and any special considerations of the environment. Devised the scenario outlines to reflect recent and current U.S. force deployments, not projections into the future based on some mythical country or situation. It was understood that the issues derived from consideration of these types of scenarios would be applicable to any future scenarios that might develop. It was expected that the scenarios would focus the study panels on a common set of situational requirements that need action to resolve. The scenarios formed the basis for identifying high value targets (HVTs) that require protection, vignettes that described how the threat might attack those HVTs, and the subsequent requirements that need to be addressed to achieve the goal of force protection.



Dimensions for Scenario Construction



- **The Nature of the Adversary**
 - **Motivation**
 - Religious/diffuse Traditional/focused
 - **Organization**
 - Individuals/loose bands..... Sovereign states/armies
 - **Capability**
 - Unsophisticated but lethal..... SOA/WMD
- **The Conflict Environment**
 - Open/logistically accessible..... Urban/logistically difficult
- **Our Objectives**
 - Obtuse/diffuse/debated Clear/defined/embraced
- **The Intensity of the Engagement**
 - Humanitarian Full-scale combat

Force Protection Study

Threat – Operations Panel

17

The selection of scenarios within which force protection requirements could be assessed presents a difficult problem: which scenarios depicting future force protection requirements are most likely to be encountered, most representative of the future environment, most realistic in their construction, etc.?

Rather than just select scenarios randomly, the panel attempted to look at the drivers of the future in an effort to identify a full range of scenarios with the aim of being able to future challenges rather than simply extrapolate from the scenarios.

Four such drivers were identified: the nature of the adversary; the physical characteristics of the environment in which the conflict occurs; the clarity of our national objectives associated with the operation; and finally, the level of intensity of the engagement. Several additional characteristics of the adversary's nature were considered: the adversary's motivation, organization, and capabilities.

As an example, the engagement in Afghanistan might be characterized as one with a religiously motivated adversary with a relatively loose organization but access to modern weapons. The major engagements took place in a relatively open environment (desert and mountains, as opposed to cities) and began with combat but included a humanitarian component that increased with time. Our national objectives were clear and generally embraced at the onset (in response to the events of September 11).



Scenarios



Five different scenarios span the spectrum of missions and geographic areas to inform the scope of the FP problems. The deployment scenario applies to all five.

- #1 Low-intensity conflict-- Afghanistan**
- #2 Peace keeping and peace enforcement-- Bosnia and Kosovo**
- #3 Mid-intensity conflict-- Kuwait and Saudi Arabia supporting forces in Iraq**
- #4 Counter-Drug operations-- Colombia**
- #5 Mid-intensity conflict-- Korea**

Deployment scenario—applies to all five

Force Protection Study

Threat – Operations Panel

18

The selected scenarios spanned a large portion of the spectrum of conflict from counter-drug operations against paramilitary forces to mid-intensity conflict against modern armies. The threats in each of the scenarios are markedly different. The geographical areas cover the gamut from South America to Southwest Asia to the Korean peninsula. The first scenario is applicable to all of the other five scenarios as it provides the basis for addressing the force protection issues encountered during the deployment of forces from CONUS bases to theaters of operation. The outline scenarios are explained individually on subsequent charts in this briefing.



Scenario Summary Low intensity conflict



- **Area: Afghanistan**
- **Threat**
 - Al Queda and the Taliban
 - Small arms, machine guns, RPGs, mines, mortars, light artillery, MANPADS as primary delivery method
 - Suicide bomber potential high
- **Environment**
 - Land-locked, 500-1000 miles from usable port
 - Rugged terrain to 15,000 feet
 - Few airfields
- **Primitive infrastructure**
 - Import all supplies
 - Support from U.S. forces in neighboring countries essential

Force Protection Study

Threat – Operations Panel

19

Mission- Low intensity conflict

Threat- Threat consists of scattered groups of combatants and terrorists armed primarily with small arms, light and heavy machine guns, RPGs, mines, mortars, rockets, and some light artillery. The possibility of suicide bombers using individually carried explosives or employing car, truck, or boat bombs exists. Some threat individuals and small elements are indistinguishable from members of various armed groups headed by locally powerful warlords, and indeed may have the ability to operate in both camps at will.

Nature of the Environment- Land-locked operational area 500-1000 miles from a useable seaport. Terrain ranging from high desert and plains to rugged mountains rising to 15,000 feet. Cities consist of urban sprawl of poor quality construction and few multi-story buildings. Primitive villages throughout the countryside have been bombed and rubble extensively. Poor road net with single lane trails only at higher elevations. No working rail lines. No potable water supply. Extremely limited and undependable electrical and communications networks, basically in a handful of medium sized towns and cities. Few airfields available without significant improvement work. Support from U.S. Forces operating in neighboring countries is essential. Sea access to long surface lines of communications and supporting airfields in an allied country compounds the force protection issues. All food, fuel, ammunition, spare parts, building materials must come into the operational area from outside over this primitive and vulnerable supply line.



Scenario Summary Peacekeeping and Peace Enforcement



- **Area:** Bosnia and Kosovo
- **Threat**
 - Disgruntled members of highly-motivated ethnic groups
 - Attacks by fire using small arms, machine guns, RPGs, mines, and mortars, and assassinations
 - Suicide bomber potential high
- **Environment**
 - Urban complexes have generally modern infrastructure
 - Road nets include modern highways and semi-improved farm roads
 - Terrain varies from forested and mountainous to open, rolling farmland
 - NATO allies border and provide support base for U.S. operations
 - Most U.S. forces live in, and operate out of, contractor-built base camps
 - Local civilians employed to provide services within the base camps

Force Protection Study

Threat – Operations Panel

20

Mission- Peacekeeping and peace enforcement, election monitoring/nation building

Threat- The threat consists largely of disgruntled members of warring ethnic groups that recent events forced into cessation of open hostilities. Many members of these groups view the conflict

as a zero-sum game, since generally only one faction can control the new government and its resources. As such, many faction members are interested in seeing the conflict continue or, at best, in seeing the other parties disarm first. Latent hatred still exists and the danger of individual direct actions such as ambushes, assassinations and other terrorist activity must be suppressed by the peace keeping/enforcement forces. Threat elements are capable of employing small arms, mortars, grenades, explosive devices, and mines of various kinds. The use of threats and assassinations of opposition leaders are standard occurrences. The threat views U.S. loss of resolve leading to withdrawal as a desired outcome. U.S. and coalition forces must protect themselves as they seek to keep the opposition groups from employing lethal means against each other.



Scenario Summary Mid-Intensity Conflict



- **Area:** Saudi Arabia and Kuwait Supporting Combat Operations in Iraq
- **Threat**
 - Modern conventional forces and guerrilla/terrorist elements
 - Small arms, machine guns, RPGs, mines, mortars, light artillery, MANPADs are the primary methods of delivery
 - Suicide bomber potential high
 - CBR dispersal weapons potential
- **Environment**
 - Modern infrastructure in large cities
 - Multiple useable ports and airports in relatively secure areas
 - Modern highways augmented by good off-road mobility for many vehicles
 - Long surface lines of communications
 - Local populations generally friendly, but some caution advisable

Force Protection Study

Threat – Operations Panel

21

Mission- Mid-Intensity conflict

Threat- The threat consists of modern conventional forces employing a full range of modern weaponry including high performance aircraft, helicopters, cruise missiles and ballistic missiles capable of impacting in our rear areas. The threat possesses WMD which could be delivered via artillery, missiles, or UAVs. The threat has some small contingent of special operations forces which could conduct raids and attacks of small scale against critical rear area installations or individual leaders. Threat elements may have access to religiously motivated suicide bombers, so protection against that type of threat cannot be ignored. Additionally, they can facilitate demonstrations by elements of the local population.



Scenario Summary Counter-Drug Operations



- **Area: Colombia**
- **Threat**
 - Well-armed and well-funded paramilitary group employed by drug cartels
 - Small arms, machine guns, RPGs, mines, mortars, light artillery, MANPADs primary methods of delivery
 - Likely threats include ambushes, mines and assassinations
- **Environment**
 - Rugged country with mountains to 20,000 feet
 - Jungle and forest covers most of terrain
 - Good seaports on both coasts
 - Primitive road net in country's interior
 - U.S. forces cooperate with Colombian armed forces and police
 - U.S. forces live inside urban complexes and in small base camps on or near forward operating bases

Force Protection Study

Threat – Operations Panel

22

Mission- Counter-drug operations

Threat- The threat consists of a well armed and well funded paramilitary force employed by the drug cartels to protect the drug production and transport industry. The main threat is from ambushes by small elements, mining incidents along roads, and terrorist acts such as assassinations of local leaders. The Colombian Armed Forces campaign against the opposition forces with the assistance of U.S. SOF forces and aircraft. Surveillance missions are regularly flown and the coca crops are regularly sprayed from the air when identified. The cartels would like to disrupt counter drug operations and have the U.S. contribution removed. Colombian armed forces provide the majority of the force protection assets to support the counter drug activities of U.S. and Colombian forces.



Scenario Summary Mid-Intensity Conflict



- **Area: Korea**
- **Threat**
 - Modern conventional forces with full range of modern weapons
 - WMD threat capability
 - Enemy air threat neutralized
 - Increased guerrilla-style attacks on LOCs during campaign
 - Enemy guerrilla forces operate out of mountain redoubts and often blend into the civilian population
- **Environment**
 - Poor, but modern nation
 - Modern infrastructure in large cities damaged by air campaign
 - Many small towns rubble by military operations
 - Hostile population toward U.S. invaders
 - Numerous refugees complicate military operations

Force Protection Study

Threat – Operations Panel

23

Mission- Mid-intensity conflict

Threat- The threat consists of modern conventional forces employing a full range of modern weaponry including high performance aircraft, helicopters, cruise missiles and ballistic missiles capable of impacting in our rear areas. The threat possesses WMD which could be delivered via artillery or a variety of missiles. The threat from enemy air has been all but eliminated in the course of the campaign. Guerrilla warfare is on the rise and some soldiers of the NKA have infiltrated behind our lines and are conducting hit-and-run raids after mingling with the civilian population. Lines of communications are at risk and a number of losses have been suffered due to ambushes of convoys and mining incidents along the roads in the forward base areas. Mortar, RPG, and automatic weapons attacks by fire are common in and near the ports and the LOCs.

Environment - North Korea is a poor, but fairly modern nation. The road nets are good. The infrastructure is fairly modern, but has been damaged in the recent air and ground campaigns. Major cities have sustained extensive damage and many towns and villages have been rubble. Refugees have streamed into the major towns and have clogged the roads to the south and safety in South Korea. The populace is generally outraged at the U.S. for bringing war to their country and there is an unexpected amount of popular sentiment in favor of the crumbling regime. Attempts to gain the support of the populace for this “war of liberation” from an oppressive regime have not gone well. As a consequence, there is a great deal of concern for the force protection issues of having our log facilities in the heart of the North Korean industrial and population centers.



Scenario Summary - Deployment -



- **Mission-** Force deployment from CONUS bases
- **Threat**
 - Sabotage from terrorist sleeper cells, or
 - Primarily armed with small arms and explosives
 - Employ MANPADs, IEDs, RPGs or suicide bombers
 - Computer hackers
 - CBR agent dispersal
- **Environment**
 - United States has open society vulnerable to infiltration by terrorist cells
 - Opposition groups can be exploited to be disruptive to attempts to deploy smoothly

Force Protection Study

Threat – Operations Panel

24

While each vignette was constructed on the basis of a single scenario outline, it soon became apparent that many vignettes could be applied to several scenarios.

HVTs were selected based on their essentiality to mission accomplishment. In this regard, a special exception must be made with regard to the individual soldier. Casualties in war are inevitable. Casualties in operations at the lower end of the spectrum of conflict are expected, but certainly the numbers will be fewer at the lower end of the spectrum as in humanitarian or peace-keeping missions. While every life is precious, loss of any specific soldier or small group of soldiers does not usually threaten mission accomplishment. The exception must be raised in the circumstance wherein continuous loss of a few soldiers a week threatens the national will to continue the mission. In this circumstance, one may wish to view individuals and small groups as HVTs as we did in this body of work.

The HVTs that we considered were grouped conveniently into five groups as shown. The matrix on chart_ shows the HVTs in the five groups, and it is noteworthy that the only HVT which appears in all five groups is the one labeled “individuals and small teams.”



High-Value Target Determination



High-Value Targets derived by

- **Former senior operational commanders**
 - Examined each of the scenarios and threat attack TTP
 - Identified entities (targets) which, if attacked, would adversely impact U.S. mission accomplishment
- **Threat experts**
 - Identified those entities (targets) which, if attacked, would significantly enhance the threat's mission accomplishment

Force Protection Study

Threat – Operations Panel

25

The value of a target may be viewed differently depending on whether it is viewed from the perspective of the threat or that of the U.S.. In this determination of the list of high-value targets, we used a two-fold evaluation: the impact an attack on the target would have on our ability to accomplish the mission (from the U.S. perspective) together with the assessment of the value of an attack on that target in furthering the objectives of the threat. The U.S. perspective on mission accomplishment was done by former operational commanders who examined detailed scenarios and vignettes within those scenarios to identify U.S. targets whose loss would seriously impact U.S. mission accomplishment. From the threat's point-of-view, threat experts identified those targets, which, if attacked, would be viewed as meeting the threat's mission needs. Most often, the two views are not congruent. A single casualty may not impede mission accomplishment, but a single soldier may be viewed as a high-value target by the threat if their objective is to undermine morale or national will, for example.



High-Value Targets



- APOD/APOE
- SPOD/SPOE
- Interim Staging Bases (ISB)
- Troop concentrations
- Individual combatants and support personnel
- Convoys
- Air/Missile Defense (AMD) Site
- Air Operations Base (AOB)
- Troop Billets
- Hospitals
- Food, Water, Fuel, Medical and Ammunition Supplies

- Command and control centers
- Communications nets
- ISR assets
- Navigation systems (GPS)
- Railways
- Tunnels and bridges
- Waterways
- Roads
- Home posts/bases
- Host government cooperation

Force Protection Study

Threat – Operations Panel

26

Having taken the scenarios and the vignettes based on those scenarios as the starting point, the task was then to extract those high-value targets from both the U.S. and the threat's perspectives. The targets presented here are a composite taken from all of the scenarios collectively, and are not presented in any priority order.



High-Value Target Mapping into FP Objectives



	a	b	c	d	e
High Value Targets	Protect Fixed Installation CONUS*	Protect Theater Installations OCONUS	Protect Resources in Transit	Protect C ¹ ISR	Protect Individuals & Detached Small Units
APOD/APOE	X	X	X		
SPOD/SPOE	X	X	X		
Troop concentrations	X	X	X		X
Air Operations base	X	X			
C ² concentrations	X	X		X	
Communication nets	X	X		X	
Billeting	X	X			
Individual combatants & support personnel	X	X	X	X	X
Fuel		X	X		
Ammunition	X	X	X		
Water		X	X		
Food		X	X		
Medical Supplies		X	X		
Convoys			X		X
Hospitals	X	X			
AMD sites		X			
Intermediate staging base		X	X		
ISR assets	X	X		X	X
Navigation systems				X	
Railways			X		
Tunnels and bridges			X		
Waterways			X		
Roads			X		
Home posts/bases	X				X
Host-government cooperation		X			X

Force Protection Study

Threat – Operations Panel

27

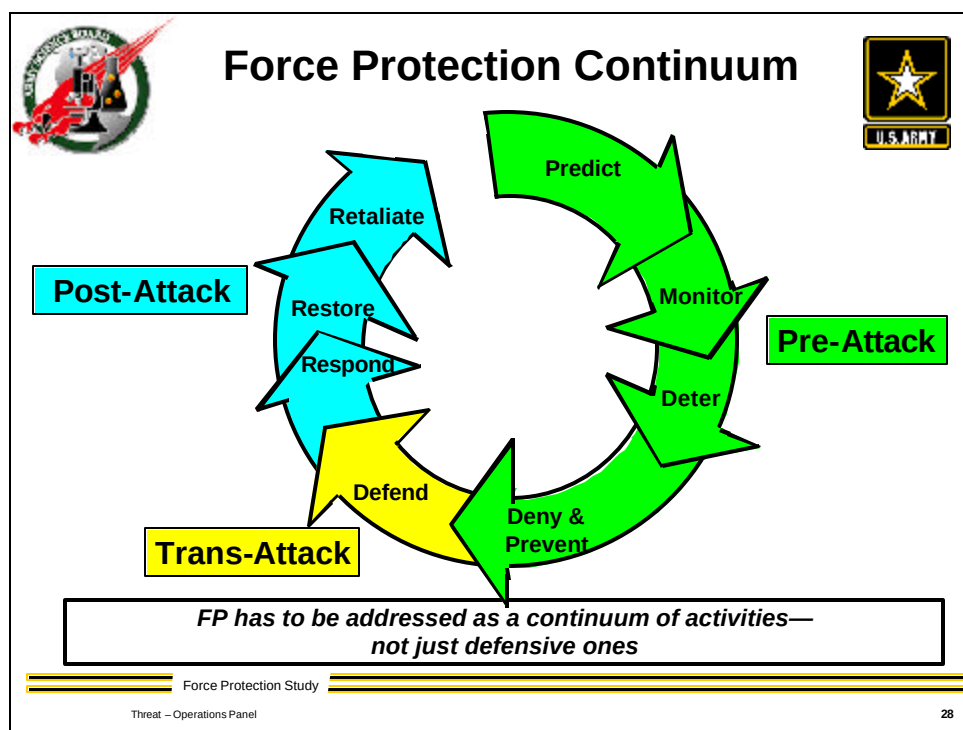
*These "CONUS" targets include permanent, fixed OCONUS installations used during peacetime, e.g., Heidelberg, OSAN AFB

There are several integrated targets which were developed: fixed installations CONUS and OCONUS, theater installations OCONUS, convoys, and individuals/small units. These

aggregated targets were used so that a manageable number of requirements could be discussed; otherwise, requirements for each of the more than two dozen high-value targets would need to be addressed.

It was also noted early in the study that C4ISR was common to each of these aggregated targets, and rather than define requirements for C4ISR within each of the aggregate targets, the C4ISR capability that underpins them all was discussed as a separate aggregated target. Within each of these cases were a number of high-value targets that were identified in one or more of the scenarios or vignettes. This chart provides the mapping of these high-value targets into the various objectives of providing protection to the five classes of aggregated targets.

Note that only a single high-value target is seen to be present in all five cases: individual combatants and support personnel. Protection of the individual or small unit will be seen later as the most difficult of all force protection challenges and remains the single most vulnerable part of force protection.



Earlier in this briefing, we showed how the threat uses a planning and execution cycle when attacking U.S. forces. This slide shows that the United States can have a concurrent cycle in reacting to those potential attacks. The threat's cycle is shown here in the labels of pre-, trans- and post-attack. The arrows convey the kinds of actions that the United States should do during those phases to provide force protection against those attacks. These actions are defined in the next two slides.

During the long pre-attack phase, U.S. forces should (1) predict attacks and monitor trends and changes in the local environment; (2) deter attacks by creating credible threats of retaliatory action should the attack occur; and (3) deny and prevent the attacks by precluding the threat's actions. This includes taking preemptive measures to interrupt the threat's planning and execution cycle.

During the attack itself, U.S. forces should defend against that attack.

During the post-attack phase, U.S. forces should (1) respond to the attack by taking immediate actions to mitigate the effects of the attack, gathering and distributing lessons learned, and informing the public and other parties through the media; (2) restore operations and equipment as soon as possible; and (3) retaliate against the attacker to provide a deterrence against any future attacks.

Today, force protection is predominantly viewed as the process of defending physical assets and people. Yet as this slide demonstrates, there are many other actions that can play a part in force protection. U.S. forces should capitalize on some of these other actions to make its force protection efforts more robust.



FP Continuum Definitions



Predict and Monitor

- To estimate, calculate, and notify in advance the threat's probable course of action
- To observe, surveil, record, and report changes in the threat environment

Deter

- To prevent threat actions by creating fear of retaliatory consequences or the belief that the proposed actions would be unsuccessful

Deny and Prevent

- To hinder or preclude the threat from prosecuting its course of action through security measures or friendly pre-emptive actions

Force Protection Study

Threat – Operations Panel

29

This is the first of two slides that define the component parts of the force protection continuum presented on the previous slide.



FP Continuum Definitions

(Continued)



Defend

- To actively resist hostile actions directed against friendly personnel, physical assets, or information in order to preserve operational readiness

Respond, Restore and Retaliate

- To immediately act during a hostile act to mitigate its effects
- To restore friendly personnel, physical assets, or information to full operational readiness
- To demonstrate to the threat and other third parties through punitive measures that the attack was unacceptable, so as to preclude future attacks

Force Protection Study

Threat – Operations Panel

30

This is the second of two slides that define the component parts of the force protection continuum slide.



Vignettes



- Illustrative examples showing the employment of threat weapons and delivery means to attack the high value targets in the scenarios described
- All vignettes apply to almost all scenarios
- Value of target assessed by the immediate impact of its loss.
- High value targets grouped into
 - Individual soldiers and detached small units
 - Fixed facilities CONUS
 - Theater installations OCONUS
 - Convoys (Resources in transit)
 - C⁴SR Networks

Force Protection Study

Threat – Operations Panel

31

While each vignette was constructed on the basis of a single scenario outline, it soon became apparent that many vignettes could be applied to several scenarios.

HVTs were selected based on their essentiality to mission accomplishment. In this regard, a special exception must be made with regard to the individual soldier. Casualties in war are inevitable. Casualties in operations at the lower end of the spectrum of conflict are expected, but certainly the numbers will be fewer at the lower end of the spectrum as in humanitarian or peace-keeping missions. While every life is precious, loss of any specific soldier or small group of soldiers does not usually threaten mission accomplishment. The exception must be raised in the circumstance wherein continuous loss of a few soldiers a week threatens the national will to continue the mission. In this circumstance, one may wish to view individuals and small groups as HVTs as we did in this body of work.

The HVTs that we considered were grouped conveniently into five groups as shown. The matrix on chart shows the HVTs in the five groups, and it is noteworthy that the only HVT which appears in all five groups is the one labeled “individuals and small teams.”



Vignette- Attack on CONUS Deployment Base

- **Vulnerabilities-** Food and water supplies, contract personnel working in base services
- **The Plan-** Contaminate food supplies with anthrax spores covertly
- **Execution**
 - Sleeper cell terrorists, working as Norfolk dining facilities contractors that support deploying forces, obtain anthrax spores and place them in parmesan cheese shakers on the salad bar
 - Deploying forces use the cheese on salads the day before embarkation on ships and planes
 - Sickness symptoms appear enroute on the ships and after aircraft arrival
 - Disease spreads before accurate diagnosis made, but is brought under control with drugs and without loss of life
- **Impact-** Rumors abound and stories of “deaths caused by enemy agents in the dining facilities” never totally refuted. Significantly raises stress levels of deployed troops.

Force Protection Study

Threat – Operations Panel

32



Vignette - Attack on Kandahar APOD -



- **Vulnerabilities-** Aircraft in air and on ground, fuel supplies, radar capability, runways, communications capability
- **The Plan**
 - Extremist group of 20 men paid by Al Queda
 - Two groups attacking bi-directionally to disrupt C-17 flight operations at night
 - Hit-and-run attack employing small arms, RPGs, mortars and MANPADs

Force Protection Study

Threat – Operations Panel

33

Deter Deployment- Attack on APOD at Kandahar

The Plan- A small group of about 20 armed militiamen working for a friendly warlord in Afghanistan, are paid handsomely by Al Queda operatives to conduct a raid on the APOD at Kandahar Air Base. After infiltrating into the local villages over a period of several days, they gather up cached weapons and conduct a night raid on the airbase. Blending in with normal vehicular and foot traffic outside the air base, they establish two groups after dark. Group A is a dismounted group which moves to within 800 meters of the wire perimeter in an area of rubble from a nearby village without being detected armed with 12 RPG rounds and 4 launchers, two light machine guns, two sniper rifles, several anti-personnel mines, and several AK-47s. They select a position on the side of the airfield closest to the buildings that house the operations area and the control tower. Group B moves by truck to a position 4 Km away on another side of the airfield within range of the parking ramps for their two 82 mm mortars and twenty rounds of ammunition. They also have two MANPADS which they position one kilometer from the mortar positions.



Vignette - Attack on Kandahar APOD -

(Continued)



- **Execution**
 - C-17 lands and taxis to parking ramp to unload
 - Terrorists, near operations center, launch 12 RPG ripple fire rounds at max range while firing light machine guns into operations complex
 - Noise of exploding RPGs and general confusion covers sound of 20 82mm mortar rounds firing from two tubes, 3000 meters away
 - C-17, struck by near-miss of mortar round, burns furiously on parking ramp
 - Terrorist attack completed within 5 minutes
 - Reaction force attack helicopters scramble to respond and one shot down by MANPAD team left behind
- **Impact-** APOD shut down for more than 24-hours, deployment interrupted, moderate casualties

Force Protection Study

Threat – Operations Panel

34

Execution- A fully-loaded C-17 lands at night and taxis to the parking ramp to begin unloading operations. The attack begins with Group A pouring sniper and machine gun fire into the heart of the operations complex which is separated from the parking ramp, but includes the control tower. The 12 RPG rounds are launched in measured ripple fire over the space of one minute using high angle fire largely unaimed in the general direction of the same operations complex. In the ensuing chaos of the opening rounds from Group A, Group B launches all twenty mortar rounds into the aircraft parking area using traverse and search techniques from pre-calculated data and with pre-cut charges. The noise and flashes from the exploding RPG rounds and automatic weapons fired from across the base distracts the defenders and covers the noise of the distant mortars firing. Within two minutes, all 20 82mm rounds have been fired; and the truck departs the area carrying the mortars and their crews within 5 minutes. The parked C-17 takes a near hit from mortars and burns furiously on the ramp. Reaction forces deploy within ten minutes. Attack helicopters converge on both areas vectored by the personnel in the tower who observed the flashes of the fire coming from both attack positions. One attack helicopter is engaged and destroyed by the MANPADs gunners. Ground reaction elements combing the area from which fire was received some two hours later take casualties from an anti-personnel mine left behind with the residue of the expended RPGs.

Impact- Casualties among personnel are moderate. The base is shut down for at least 24 hours. The deployment is interrupted and delayed.



Requirements: Protect Fixed Installations (I)



Predict and Monitor

- Establish baselines to determine status of the local environment
 - Collect and store data
 - Establish local-national linkages locally
- Monitor and verify changes in the status of the local environment
 - Analyze patterns
 - Integrate with community to establish local trust
 - Infiltrate the local community with intelligence assets
- Forecast threat attack in a timely manner: what, where, and when

Force Protection Study

Threat – Operations Panel

35

One of the key components of Force Protection is the requirement to predict and monitor external and internal activities, movements, changes, and personnel, in and around fixed installations. To accomplish this, baselines should be established and data bases created to allow for change detection, monitoring baseline, and potential attack identification. Much of the technology to accomplish these tasks, has yet to be developed. Once established, installation personnel may have the ability to monitor and verify changes in the status of the local environment. Ultimately, the ability to predict, with accuracy, an attack or a potential weakness in the defense of the installation will be an essential element in a commander's fixed installation defense plans.



Requirements: Protect Fixed Installations (II)



Deter

- Cue, verify, localize, and interdict local attacks
- Integrate in the local community
 - Establish local trust
 - Maximize goodwill

The next requirement is to deter potential attackers from attempting to attack a fixed installation. Effective deterrence can be achieved by overwhelming force; a sound defensive plan, to include technology and strong physical security; measures and assurance to a potential attacker that his attack will be defeated and his objectives not met.

Another key to deterrence is establishing strong enduring relationships with the local community. Local leaders and community members can be especially useful in deterring attacks if their objectives for success are in line with that of the local installation. These relationships must be developed over time and the goal here is to establish good will between the personnel on the fixed installation and the surrounding community.



Requirements: Protect Fixed Installations (III)



Deny and Prevent

- **Secure the perimeter**
 - Establish multiple dynamic perimeters
 - Minimize troop requirements
 - Use stealth techniques to enhance the perimeter
- **Control access**
 - Permit easy friendly access
 - Provide rapid IFFN for people, vehicles, boats, aircraft, and electrons
 - Deny access to possible threats
 - Military and civilian people, vehicles, boats, aircraft, electrons

Force Protection Study

Threat – Operations Panel

37

Installation commanders have a responsibility to deny and prevent potential attackers from attempting an attack. A secure perimeter is a fundamental element of force protection and currently, considerable personnel and materiel resources are devoted to this task. There is a growing recognition that technology enhancements could aid commanders by assisting in establishing multiple and dynamic perimeters and possibly reducing the requirement for large numbers of physical security personnel to do these tasks.

Additionally, controlled access to the installation can be enhanced through technology insertion by easing known friendly personnel's ability to enter and exit an installation, providing rapid and secure identification of personnel, vehicles, contents of vehicles, boats and aircraft. Finally, installation firewalls can be established to assure the communication systems are less vulnerable to attack.



Requirements: Protect Fixed Installations (IV)



Defend

- Harden facilities/personnel against
 - Cyber attacks
 - NBC weapons
 - IEDs/bombs
 - Other HE/KE weapons
 - EW
 - Thermobaric weapons
 - Incendiary weapons
 - DE weapons
 - RPGs and mortars
- Employ decoys
- Employ countermeasures
- Introduce unpredictability

Force Protection Study

Threat – Operations Panel

38

Requirements exist to protect and defend fixed installations from a variety of potential attacks. Different components of fixed installations have varying degrees of vulnerability to these attacks but in general, they can be categorized as requirements to harden facilities against attacks from the capabilities listed on slide #11. It is clear that there are technology solutions to accomplish this. Secondly, countermeasure to attacks, such as decoys, counter-fire methods and operational unpredictability contribute to success when defending a fixed installation.



Requirements: Protect Fixed Installations (V)



Defend *(Continued)*

- Detect and deny contaminants
 - Fuel
 - Water
 - Food
 - Medical supplies
 - Mail and commercial delivery services
 - Airborne CB agents
- Keep threats beyond their effective range
 - Direct-fire weapons (0-2 km)
 - Indirect-fire weapons
 - Ballistic and precision fire depending on environment and range of weapons available in a scenario
 - Sea, land, and air vehicular delivery means

Force Protection Study

Threat – Operations Panel

39

Continuing on slide # 40 are other methods of potential attack on fixed installations. Requirements exist to detect and defend against contaminants to such essential commodities as water and fuel, even the food, medical supplies and incoming mail. We believe technology can greatly assist in these tasks. Also the ability to keep potential attackers or means of attack at stand-off ranges is very desirable.



Requirements: Protect Fixed Installations (VI)



Defend *(Continued)*

- **Negate or minimize effectiveness of attack**
 - **Recognize the attack and its nature**
 - **Track the attack**
 - **Divert/deflect/neutralize the attack**
 - **Reduce the resources available for the attack**
 - **Cause weapons to fail or detonate prematurely**

Force Protection Study

Threat – Operations Panel

40

Finally, in the area of defending a fixed installation, it is important that even if denial and detection fail, commanders must have means to negate and minimize the effectiveness of the attack. Early recognition and tracking can assist in diverting and deflecting the main thrust of the attack and reduce the effectiveness of the attack. Among the potential technology enhancements could be methods of causing weapons to fail or detonate prematurely.



Requirements: Protect Fixed Installations (VII)



Respond, Restore and Retaliate

- Determine and disseminate lessons learned rapidly
- Rapidly implement corrective counter-measures at the installation
- Rapidly detect, track, and retaliate against source of attacks
- Preclude future attacks using all appropriate means
- Disrupt threat plans and ops

Force Protection Study

Threat – Operations Panel

41

When an attack on a fixed installation occurs, the effectiveness can be reduced if a solid response to the attack has been planned and rehearsed. Key to this is the ability to determine the point of the attack and the extent of the attack and then rapidly implement corrective counter-measures. Detection, tracking and rapid retaliation and response are imperative. A goal would be to not only disrupt the attack but to preclude future attacks.



CONUS Base Operations Goals and Priority Requirements



Goals

Maintain maximum operational capability of base with minimum casualties

Priority Requirements

- Forecast attack in a timely manner: what, when, and where
- Cue, localize, verify, and interdict attacks with community law enforcement
- Secure the perimeter and control access
- Harden facilities and protect personnel
- Employ decoys and countermeasures
- Prevent contamination of supplies
- Keep threats beyond their effective range with community law enforcement
- Preclude future attacks using all appropriate means

Force Protection Study

Threat – Operations Panel

42

We will turn now to a brief discussion of the Force Protection requirements for Base Operations on installations at different locations. The first is a large CONUS installation with a relative large base ops footprint. The goal is to maintain an effective level of base ops with minimum disruption to the mission of the installation or the personnel residing and living there. Priority requirements for this kind of installation are listed on slides #35-41. These include many of the elements we have seen on the previous slides but are collected here as a review of the kinds of technology that may assist in achieving this goal.



OCONUS Fixed Installation Goals and Priority Requirements



Goals

Maintain maximum operational capability of base with minimum casualties

Priority Requirements

- Forecast attack in a timely manner: what, when, and where
- Cue, localize, verify, and interdict attacks
- Create multiple dynamic perimeters to control access
- Harden facilities and protect personnel
- Employ decoys and countermeasures
- Introduce unpredictability into routine operations
- Prevent contamination of supplies
- Keep threats beyond their effective range
- Preclude future attacks using all appropriate means

Force Protection Study

43Threat – Operations Panel

DRAFT - Not for Distribution without Permission from The Army Science Board (ASB) Executive Secretary

Shown here are the technology requirements for an OCONUS Main Operating Base. As can be seen, they are essentially the same requirements as that of a CONUS installation. Local conditions and environments vary within installations in CONUS and OCONUS but the fundamental requirements for Force Protection are the same.



Forward Operating Base Goals and Priority Requirements



Goals

- Maintain maximum operational capabilities of base with minimum casualties and friendly force commitments during deployments
- Maintain security of base between deployments

Priority Requirements

- Forecast attack in a timely manner: what, when, and where
- Cue, localize, verify, and interdict attacks
- Create multiple dynamic perimeters to control access
- Harden facilities and protect personnel
- Employ decoys and countermeasures
- Introduce unpredictability into routine operations
- Prevent contamination of supplies
- Keep threats beyond their effective range
- Preclude future attacks using all appropriate means

Force Protection Study

Threat – Operations Panel

44

Included in this slide are priority requirements for protection of a Forward Operating Base. Note that they are virtually identical to those in the previous categories of installations.



OCONUS Small Installation Goals and Priority Requirements



Goals

Maintain maximum operational capability of small installation with minimum casualties and friendly-force commitment

Priority Requirements

- Forecast attack in a timely manner: what, when, and where
- Cue, localize, verify, and interdict attacks
- Integrate in local community to gain intelligence
- Create multiple dynamic perimeters to control access
- Maintain assured secure communication
- Harden small installation and protect personnel
- Employ decoys and countermeasures
- Introduce unpredictability into routine operations
- Prevent contamination of supplies
- Keep threats beyond their effective range

Force Protection Study

Threat – Operations Panel

45

Finally, this slide includes the goal and priority requirements for protection of an OCONUS Small Installation.



Vignette - Threat Attack on Convoy -



- See daily newspapers for vignettes on attacks by fire
- Vulnerabilities

Ammunition and fuel are dangerous, heavy commodities normally transported by surface means, can contaminate fuel by bio agents delivered by hand

- The Plan

Terrorist agents covertly contaminate fuel supplies passing from Kuwait to Iraq by truck

No notes necessary. See charts 46 and 47.



Vignette - Threat Attack on Convoy - (Continued)



- Execution

- Tanker trucks move through Kuwait to the border of Iraq singly or in pairs by infiltration to dump fuel into the bladders at a forward POL supply point just inside Iraq
- Contracted Kuwaiti drivers make the 500-mile roundtrip with a rest stop at the ½ point of each leg
- A balky camel diverts two drivers at the rest stop while an unseen threat agent puts contaminant agents into the fuel truck hatch
- The fuel is delivered and the entire fuel supply must be assumed contaminated when the threat agent is discovered

- Impact

Covert operation costing virtually nothing results in major delay in delivering fuel



Requirements: Protect Convoys (I)



Predict and Monitor

- Establish baselines to determine status of environment of routes and trans-shipment points
 - Collect and store data
 - Establish local-national linkages locally
- Predict routes with the least threat
- Monitor and verify changes in status of environment of routes and trans-shipment points
 - Analyze patterns
 - Integrate with community along routes to establish local trust
 - Infiltrate the local community along routes with intelligence assets
- Forecast threat attack in a timely manner: what, where, and when



Force Protection Study

Threat – Operations Panel



48

Protecting resources in transit requires tailored force protection measures that maintain a posture that precludes a threat attack. Accomplishing this requires as full an operational picture as possible. Situational understanding gained from good, analytic intelligence, and operational risk management standards evaluation will enable commanders to forecast threat attacks in a timely manner.



Requirements: Protect Convoys (II)



Deter

- Monitor changes along, in proximity to and/or under routes
- Integrate in the local community along routes
 - Establish local trust
 - Maximize goodwill
- Cue, verify, localize, and interdict local attacks
- Provide rapid and effective self-protection capability at low manpower cost

Force Protection Study

Threat – Operations Panel

49

Deterring attacks requires that commanders continually monitor changes that occur along the transit route. Commanders must have tailored, focused intelligence to support their missions.

Deterrence provides a level of rapid, effective self-protection at a low manpower cost.

Employing rapid combat identification of possible threats and denying access to those threats identified will secure routes and trans-shipment points, especially choke points, tunnels, bridges, canals, and locks.



Requirements: Protect Convoys (IV)



Defend

- Harden resources in transit and the trans-ship points against
 - Cyber attacks
 - NBC weapons
 - IEDs/bombs
 - Other HE/KE weapons
 - EW
 - Airborne CB agents
 - Incendiary weapons
 - DE weapons
 - Mines
 - Small arms and snipers
 - RPGs and mortars
- Employ decoys and deception techniques
- Employ counter-measures

Force Protection Study

Threat – Operations Panel

51

Hardening resources and trans-shipment points against the range of weapons decreases vulnerability and defeats the threat's intent. Other defensive measures include employing decoys and deception as well as proactive counter measures such as a demonstrated preparedness to deter attacks.



Requirements: Protect Convoys (V)



Defend *(Continued)*

- Detect and deny contaminants in
 - Fuel
 - Water
 - Food
 - Medical supplies
 - Mail and other logistic supplies
- Keep threats beyond their effective range
 - Direct-fire weapons (0-2 km)
 - Indirect-fire weapons
 - Ballistic and precision fire depending on environment and range of weapons available in a scenario
 - Sea, land, and air vehicular delivery means

Force Protection Study

Threat – Operations Panel

52

Detecting and denying the introduction of contaminants in fuel, water, food, medical supplies, mail and other logistic supplies has a two-fold benefit. Not only does it protect the resources in

transit, but also the destination point upon the convoy's arrival. Commanders must evaluate local providers in ways that enhance the force protection posture of the mission.

Strategies that keep threats and weapon delivery beyond their effective range will also provide an effective defense.



Requirements: Protect Convoys (VI)



Defend *(Continued)*

- **Negate or minimize effectiveness of attack**
 - Recognize the attack and its nature
 - Track the attack
 - Divert/deflect/neutralize the attack
 - Reduce the resources available for the attack
 - Cause weapons to fail or detonate prematurely
 - Protect valuable resources in transit during the attack
 - Ensure adversary cannot get these valuable resources

Force Protection Study

Threat – Operations Panel

53

Negating or minimizing the effectiveness of an attack requires that commanders exploit a range of strategies including ensuring that a threat cannot get at the valuable resources in the convoy while it is under attack.



Requirements: Protect Convoys (VII)



Respond, Restore and Retaliate

- Determine and disseminate lessons learned rapidly
- Rapidly implement corrective counter-measures
- Rapidly detect, track, and retaliate against source of attacks
- Preclude future attacks using all appropriate means
- Disrupt threat plans and ops

Force Protection Study

Threat – Operations Panel

54

When an attack is not preventable, commanders must respond, restore, and retaliate as appropriate as soon as practical. The procedures they follow include those that will restore normal operations as soon as possible. Further, actions that will preclude future attacks will also disrupt threat plans and operations.



Convoy Operations Goals and Priority Requirements



Goal

Complete deliveries successfully with minimum losses and casualties

Priority Requirements

- Forecast attack in a timely manner: what, where and when
- Select routes with the least threat and vary the routes
- Provide rapid and effective self-protection at low manpower cost
- Secure the resources in transit and trans-shipment points
- Secure critical choke points such as bridges and tunnels
- Provide rapid combat identification (CID) of possible threats
- Employ decoys and countermeasures
- Keep threats beyond their effective range

Force Protection Study

Threat – Operations Panel

55

This slide summarizes the goals and requirements for convoys.



C⁴ISR Vignette



Vulnerabilities- Computer terminals, transmission lines and fiber cable, antennas, jamming, interruption of GPS signals

The Plan-

- North Korean forces plan to disrupt US C2 networks during critical period of operational maneuver
- Network hacking specialists will introduce viruses and other disruptions on the NIPRNET
- Corrupted data bases will interfere with activities on the SIPERNET
- Powerful jammers near the DMZ will cause some GPS and wireless communications failures
- Attacks by fire will be employed against known comms centers
- Years of quiet intelligence collection near the DMZ enables this ambitious plan

Negating Combat Operations- Attack of Command and Control Centers

Vulnerabilities of C2 Centers - Computer terminals, transmission lines and fiber cable, antennas, jamming, and interruption of GPS signals

The Plan – North Korean forces plan to disrupt US C2 networks during critical period of operational maneuver.



C⁴ISR Vignette



Execution-

- Hackers begin concerted attacks over a 24 hour period and are successful in penetrating the tactical network and delivering hundreds of virus and data base corruption agents
- Many computers must be taken off line, and the operation of the tactical internet is slowed significantly
- Hit and run mortar and artillery attacks on obvious antenna locations impact wireless comms adversely
- GPS jamming disrupts signal and takes many radios and position locators off the air for several hours

Impact- Frequent disruptions of the tactical C2 network reduces confidence of the leaders in the integrity and security of the command network and slows operations significantly

Execution - North Korean network internet hacking specialists operate clandestinely in the DMZ area to target the US JTF headquarters that sets up there after the NKA forces withdraw to the north. Using data collected over many years from listening posts near the DMZ, they conduct repeated hacker attacks on the tactical internet established by US Forces for C2 of its forces. They are successful in entering, corrupting, and destroying several data bases on the NIPERNET and causing many computer shutdowns on the tactical SIPERNET. Frequent hit and run mortar, artillery, and rocket attacks on the obvious antenna farms in the vicinity of the US headquarters by small elements hiding in the mountains cause frequent interruption of communications by damaging antennas, shallowly buried cables and sandbagged generators. Jammers disrupt the local GPS signals and cause many temporary losses of radio signals and position location devices.

Impact - Frequent nuisance disruptions of the command network reduce the confidence of the leaders in the integrity and security of information in the command net and slow operations.



Requirements: Protect C⁴ISR (I)



Predict and Monitor

- Establish baselines to determine status of the C⁴I networks and sensors
 - Collect and store data
 - Establish local-national linkages locally
- Monitor and verify changes in status of C⁴I networks and sensors
 - Analyze patterns
- Forecast threat attack in a timely manner: what, where, how and when

Force Protection Study

Threat - Operations Panel

58

The panel broke out C4ISR for separate examination because it was embedded in each of the cases, scenarios, and vignettes. We did not want to have it buried in the analysis of the details and remain unexamined. The Future Combat System has traded ballistic protection of the FCS elements for an increased and robust situational awareness condition. Therefore, the defeat or denial of C4ISR networks would negate the inherent advantages of the future Objective Force.



Requirements: Protect C⁴ISR (II)



Deter

- Monitor changes in C⁴I networks and sensors
 - Detect intrusions in networks and/or corruption of data
 - Detect physical destruction of sensors and network nodes
- Create completely independent, secure C⁴I networks and sensors
- If this is not possible, then monitor and protect the local community's communications capabilities upon which we are dependent
 - Establish local trust
 - Ensure security of critical data using these networks
- Cue, verify, localize, and interdict attacks

Force Protection Study

Threat – Operations Panel

59

Continuous monitoring is required to verify status, analyze patterns and forecast impending or ongoing attacks.

Independent and secure networks are desirable as they are easier to protect.

If reliance on local networks is required then security measures must be provided.



Requirements: Protect C⁴ISR (III)



Deny and Prevent

- Control access to networks
 - Permit easy friendly access
 - Deny enemy access, perhaps with firewalls that will not reduce timeliness
- Employ intelligent agent software to detect, preclude, and identify intrusions into networks
- Create decoy networks
- Ensure assured secure communications
- Minimize communications latency
- Ensure sufficient bandwidth
- Ensure fault tolerance and quality of service (e.g., self-forming and self-healing networks)

Force Protection Study

Threat – Operations Panel

60

Keys to denial and prevention are access control, intrusion detection, and fault tolerance. It may be necessary to create decoy networks to learn threat attack CONOPS. As always, bandwidth and data latency are issues to be overcome.



Requirements: Protect C⁴ISR (IV)



Deny and Prevent *(Continued)*

- Prevent jamming and distortion of networks and the sensors that support them or provide rapid mitigation if jamming occurs
- Secure the perimeter around key command and communications nodes
 - Establish multiple dynamic perimeters
 - Create “protective bubble” around nodes
 - Minimize troop requirements
 - Use stealth techniques to enhance the perimeter

Force Protection Study

Threat – Operations Panel 61

Network interruption or jamming must be expected and mitigated. Securing key nodes to reduce likelihood or frequency of intrusion or disruption is a necessary step.



Requirements: Protect C⁴ISR (V)



Defend

- Harden networks, sensors, antennas and the physical sites that support them against
 - Cyber attacks: hacking, viruses and enemy corruption of data
 - NBC weapons and anti-material, corrosive agents
 - IEDs/bombs
 - Other HE/KE weapons
 - EW
 - Incendiary weapons
 - DE weapons
 - Small arms and snipers
- Employ decoys of C² nodes and deception techniques
- Employ counter-measures

Force Protection Study

Threat – Operations Panel 62

Hardening, deception, and countermeasures are believed to be the most productive defensive measures for networks.



Requirements: Protect C⁴ISR (VI)



Defend *(Continued)*

- **Assure continuous, uninterrupted power**
- **Keep threats beyond their effective range**
 - Direct-fire weapons (0-2 km)
 - Indirect-fire weapons
 - Ballistic and precision fire depending on environment and range of weapons available in a scenario
 - Sea, land, space and air vehicular delivery means
- **Negate or minimize effectiveness of attack**
 - Recognize the attack and its nature
 - Track the attack
 - Divert/deflect/neutralize the attack
 - Ensure self-healing network

Force Protection Study

Threat – Operations Panel

63

Keeping potential threats outside of their effective attack range is the most effective defense.



Requirements: Protect C⁴ISR (VII)



Respond, Restore and Retaliate

- **Determine and disseminate lessons learned rapidly**
- **Rapidly implement counter-measures (including ECM)**
- **Rapidly detect, track, and counter source of attacks**
- **Preclude future attacks using all appropriate means**

Force Protection Study

Threat – Operations Panel

64

Rapid dissemination of information about IO attacks to other nodes in the networks is a useful step in countering future attacks.



C⁴ISR



Goals and Priority Requirements

Goal

Maintain maximum operational capability of networks and connectivity with minimum intrusion, disruption and distortion

Priority Requirements

- Forecast IO attack in a timely manner: what, when, and where
- Cue, localize, verify, and interdict IO attacks with intelligent agent software
- Secure the networks and control access with firewalls and security systems
- Harden facilities and protect communications nodes
- Create decoy networks and countermeasures
- Prevent corruption of data with self-forming, self-healing networks
- Keep threats beyond their effective range
- Preclude future attacks using all appropriate means

Force Protection Study

Threat - Operations Panel

65



Vignette



- Threat Attack on Small Team in Colombia -

Vulnerabilities

Usually soft targets, concentration of personnel in relaxed state of readiness, off-duty personnel not on alert

The Plan

- Threat platoon of paramilitary troops, funded by the drug lord, hide in and operate out of the populated area
- Conduct night attack using RPGs and small arms to kill the sentries at the doors of hotel in city used by CA team living near places of work
- Conduct hit and run attack employing small arms, hand grenades and satchel charges to kill as many people as possible working from the ground floor upward

Force Protection Study

Threat - Operations Panel

66

Vulnerabilities- Usually soft targets, billeted personnel are normally in relaxed state of readiness, off-duty personnel not on alert.

Plan- Several temporary billets are established in small hotels to house Civil Affairs teams that operate in a medium-size town wrested from control of the drug cartel by combined force operations. These hotels employ contract guards at all entrances. Drug cartel paramilitary elements observe the billets over several days and devise a plan to attack the hotel guard force by

fire of RPGs and small arms, enter the building in a quick assault and kill as many Americans as possible with hand grenades, satchel charges and automatic weapons fire before a reaction force can be employed.



Vignette

- Threat Attack on Small Team in Colombia – *(Continued)*



Execution

- At midnight, paramilitary elements suddenly appear and destroy guard posts with simultaneous RPG fire
- Paramilitary assault teams enter the building and run room-to-room killing the occupants
- Within 3 minutes, they reach the third floor before being seriously opposed
- Raiders withdraw after 5 minutes leaving 7 dead and wounded behind but many more U.S. personnel casualties

Impact - Attack disrupts the rebuilding of civil institutions, causes redirection of resources and raises the anxiety level of all forces operating in the area

Force Protection Study

Threat – Operations Panel

67

Execution- On a dark and stormy night, a paramilitary force that had been hiding in the local area stages a raid on the billet that houses the CA teams. Using RPG's to blast three of the guard posts at a range of 50 to 100 meters, the paramilitary force rushes the hotel with AK-47s, hand grenades, and satchel charges. In less than 5 minutes, they are able to penetrate to the third floor and kill many of the soldiers who were sleeping and were caught unaware at the first blast. While leaving seven of their own behind either dead or too seriously wounded to move, the raiders quickly withdraw.

Impact- The attack causes redirection of resources and raises the anxiety level of all forces operating in the area.



Requirements: Protect Individuals and Detached Small Units (I)



Predict and monitor

- Establish baselines to determine status of local environment
 - Collect and store data
 - Establish local-national linkages locally
- Monitor and verify changes in status of local environment
 - Analyze patterns
 - Integrate with community to establish local trust
 - Infiltrate the local community with intelligence assets
- Forecast threat attack in timely manner: what, where, and when

Force Protection Study

Threat – Operations Panel

68

This next series of slides (#68-#74) outline the requirements for protecting individuals and detached small units. Our analysis, derived from reviewing and cross-walking from scenarios to vignettes, has resulted in a number of areas in which FP gaps exist for these kinds of potential threat targets.

The first requirement is to establish an ability to predict and monitor the environment in which these individuals and small units operate. This includes collecting and storing data and doing the basic HUMINT to establish and develop linkages into the local community. Once the baseline is established, the requirement is changed to monitoring and verifying changes in the local environment to be able to predict and forecast the likelihood of an attack, or as an objective, the time and place of the attack.



Requirements: Protect Individuals and Detached Small Units (II)



Deter

- Integrate in the local community
 - Establish local trust
 - Maximize goodwill
- Monitor and protect the local community's communications capabilities upon which we are dependent
 - Establish local trust
 - Ensure security of critical data using these networks
- Provide rapid and effective self-protection capability at low manpower cost

Force Protection Study

Threat – Operations Panel

69

It is vital to have the ability to deter attacks. Deterrence is achieved through effective integration with the local community, monitoring and protecting the lines of communications on which individuals, small units, and the community depends, and in having an assured rapid and effective self-protection capability.



Requirements: Protect Individuals and Detached Small Units (III)



Deny and Prevent

- Secure the perimeter around the small unit
 - Establish multiple dynamic perimeters
 - Minimize troop requirements
 - Use stealth techniques where practical
- Keep threats beyond their effective range
 - Direct-fire weapons (0-2 km)
 - Indirect-fire weapons
 - IEDs and sea, land, & air vehicular-delivered weapons
- Disrupt threat plans and operations

Force Protection Study

Threat – Operations Panel

70

These next two slides outline the requirements for denying a threat to individuals and small detachments. These are fundamental, time proven methods of force protection. They include

securing a perimeter; keeping threats away from effective engagement ranges; disrupting threat plans and operations; having an ability to identify quickly both threats and non-combatants; control access to the area; the use of misinformation and decoys; and maintaining assured, secure communication. Each of these areas has specific requirements, reflected on charts #71 and #72, which could be aided via technology.



Requirements: Protect Individuals and Detached Small Units (IV)



Deny and Prevent *(Continued)*

- **Provide rapid combat identification (CID) to distinguish threats and friendlies**
- **Control access to small-unit AOR**
 - Permit easy friendly access
 - Deny access of adversaries
- **Create decoys & misinformation and employ random patterns**
- **Maintain assured secure communication**

Force Protection Study

Threat – Operations Panel

71



Requirements: Protect Individuals and Detached Small Units (V)



Defend *(Continued)*

- **Harden personnel, facilities, and resources against:**
 - Mines
 - Small arms and snipers
 - CB weapons
 - IEDs/bombs
 - RPGs and mortars
 - Thermobaric weapons
 - Incendiary weapons
 - DE weapons
 - RPGs and mortars
 - Contaminants
- **Maximize passive protection with multi-faceted armor and clothing**

Force Protection Study

Threat – Operations Panel

72

If the ability to predict and deny fail, individuals and small detachments will have to defend themselves from threat attack. Slides #66 - #67 outline the possible methods of an attack against these kinds of friendly targets, and the requirements soldiers need to defend themselves when attacked.



Requirements: Protect Individuals and Detached Small Units (VI)



Defend *(Continued)*

- **Provide survivability through personnel monitoring (e.g., location, IFF, health, and rescue aids)**
 - Minimize the effectiveness of an attack
 - Recognize the attack and its nature
 - Track the attack
 - Divert/deflect/neutralize the attack
 - Reduce the resources available to the adversary
 - Cause weapons to fail or detonate prematurely
 - Employ decoys and deception techniques
 - Employ counter-measures and unpredictability

Force Protection Study

Threat – Operations Panel 73



Requirements: Protect Individuals and Detached Small Units (VII)



Respond, Restore and Retaliate

- Rapidly detect, track, and militarily negate source of attacks
- Determine and disseminate lessons learned
- Rapidly implement corrective counter-measures

Force Protection Study

Threat – Operations Panel 74



Small Team Operations

Goals and Priority Requirements



Goal

Maintain maximum operational capability of individuals and small teams with minimum casualties

Priority Requirements

- Forecast attack in a timely manner: what, when, and where
- Cue, localize, verify, and interdict attacks
- Integrate in local community to gain intelligence
- Maintain assured secure communication
- Provide rapid combat identification (CID) of possible threat
- Harden transit means and protect personnel
- Introduce unpredictability into routine activities

Force Protection Study

75 Threat – Operations Panel--11/4/2003 3:32 PM

DRAFT - Not for Distribution without Permission from The Army Science Board (ASB) Executive Secretary

Following an attack or an attempted attack, individual soldiers and small detached units must have the ability to quickly respond, restore, and retaliate against the source of the attack.



Scale for

Requirements Prioritization

Related to accomplishing U.S. Mission and Denying Threat from Achieving Objectives



5 Extremely important

4 Very important

3 Important

2 Somewhat important

1 Less important

a Fixed installation (CONUS)

b Fixed installation (OCONUS)

c Resources in transit

d C⁴ISR

e Individuals and detached small units

Force Protection Study

Threat – Operations Panel

76



Combined Requirements



Predict and monitor

- Establish baselines to determine status of local environment, of routes & transfer points, & C⁴I networks & sensors {5}
 - Collect and store data [a,b,c,d,e]
 - Establish local-national linkages locally [a,b,c,d,e]
- Monitor and verify changes in status of local environment, of routes and trans-shipment points, and C⁴I networks & sensors [a,b,c,d,e] {5}
 - Analyze patterns [a,b,c,d,e]
 - Integrate with community to establish local trust [a,b,c,e]
 - Infiltrate the local community with intelligence assets [a,b,c,e]
- Forecast threat attack in timely manner: what, where, and when? [a,b,c,d,e] {5}

Force Protection Study

Threat – Operations Panel

77



Combined Requirements



Deter

- Provide rapid and effective self-protection capability at low manpower cost [c,e] {4}
- Cue, verify, localize, and interdict attacks [a,b,c,d] {4}
- Monitor changes in C⁴I networks and sensors [c,d] {5}
 - Detect intrusions in networks and/or corruption of data [d]
 - Detect physical destruction of sensors and network nodes [d]
- Integrate in the local community and monitor changes along routes [c,d] {4}
 - Establish local trust [a,b,c,d,e]
 - Maximize goodwill [a,b,c,e]

Force Protection Study

Threat – Operations Panel

78

After predict and monitor to assesses possible threat actions, force protection efforts must now provide an effective self protection capability at low manpower cost to deter the attack. This requires seeking a cue to a hostile action, localizing it, and verifying it to allow the interdiction of the attacks. Helpful in this regard is the monitoring of C4I networks and all applicable sensors. HUMINT data can be achieved by integrating personnel into the local community, and by monitoring changes along key routes. An additional benefit of such effort is that they will also develop goodwill.



Combined Requirements



Deter *(Continued)*

- Create completely independent, secure C⁴I networks and sensors {3}
- Monitor and protect the local community's communications capabilities upon which we are dependent {2}
 - Establish local trust [e]
 - Ensure security of critical data using these networks [e]

Force Protection Study

Threat – Operations Panel

79

To ensure rapid and timely action once a threat attack has been detected, it is important to create completely independent, secure C4I networks and sensors. Since there will be some dependence on the local communities' communications, it will be important to protect and monitor their viability. This is vital to ensure the security of critical data. Establishing local trust will facilitate this.



Combined Requirements



Deny and Prevent

- Secure the perimeter, resources in transit along routes and trans-shipment points, and around key installations and command and communications nodes [a,b,c,d,e] {5}
 - Establish multiple dynamic perimeters [a,b,d,e]
 - Minimize troop requirements [a,b,c,d,e]
 - Use stealth techniques where practical [a,b,c,d,e]
 - Provide “protective bubble” around the resources in transit and nodes [c,d]
- Secure the routes and/or trans-shipment points, especially choke points and non-redundant places along routes such as tunnels, bridges, canals, locks [c] {4}
- Provide rapid combat identification (CID) of possible threats along the routes and/or trans-shipment points [c,e] {5}

Force Protection Study

Threat – Operations Panel

80

After deterring threats, denying and preventing hostile threat actions is a key capability requirement in force protection. Some specific requirements include; securing the operational perimeter with multiple dynamic perimeters and the use of stealth techniques as appropriate. Similar actions are required to protect resources along transit routes, trans-shipment points, key installations and command and communications nodes. This requirement can be thought of as providing a “protective bubble”. In addition protection must be provided for choke points and non-redundant places along routes such as tunnels, bridges, canals, locks and similar constructs. It is also important to provide rapid combat identification(CID) of possible threats at all perimeters, transit routes and trans-shipment points. These actions can also lead to a minimization of troop requirements.



Combined Requirements



Deny and Prevent *(Continued)*

- **Control access [a,b,e], to networks [d] {5}**
 - Permit easy friendly access [a,b,d,e]
 - Provide rapid IFF for people, vehicles, boats, aircraft, and electrons [a,b]
 - Deny access of possible threats [a,b,e]
 - Military and civilian people, vehicles, boats, aircraft, electrons [a,b]
 - Deny access of adversaries that have been identified through CID [c]
 - Military and civilian people, vehicles, boats, aircraft, electrons [c]
 - Deny enemy access, perhaps with firewalls that will not reduce timeliness [d]

Force Protection Study

Threat – Operations Panel

81

Protection of our communications is a vital component of force protection. This requires controlling access to our networks while permitting easy, friendly access and rapid identification of friend or foe(IFF) for people, vehicles, and electrons. Further it requires denial of access of possible threats both military and civilians. This may require the employment of firewalls that will protect our networks but will not reduce timeliness. The use of intelligent agents to detect, preclude, and identify network intrusions may be a useful.



Combined Requirements



Deny and Prevent *(Continued)*

- Employ intelligent agents software to detect, preclude, and identify intrusions into networks [d] {4}
- Ensure assured secure communications [d,e] {3}
- Minimize communications latency [d] {3}
- Ensure sufficient bandwidth [d] {2}
- Ensure fault tolerance and quality of service (e.g., self-forming and self-healing networks) [d] {3}
- Prevent jamming and distortion of networks and the sensors that support them or provide rapid mitigation if jamming occurs [d] {4}

Force Protection Study

Threat – Operations Panel

82

Security of communication networks can be further assured by minimizing communications latency and ensuring sufficient bandwidth. The utilization of self-forming and self-healing networks can ensure fault-tolerant and quality of service. Force protection also requires the prevention of jamming and distortion of networks and the sensors that support them, and/or provide rapid mitigation, if jamming occurs.



Combined Requirements



Deny and Prevent *(Continued)*

- Create decoys & misinformation; employ random patterns [a,b,c,d,e] {4}
- Keep threats beyond their effective range [a,b,c,d,e] {3}
 - Direct-fire weapons (0-2 km) [a,b,c,d,e]
 - Indirect-fire weapons [a,b,c,e]
 - Ballistic and precision fire depending on environment and range of weapons available in a scenario [a,b,c,d]
 - Sea, land, space [c] and air vehicular delivery means [a,b,c,d]
 - IEDs and sea, land, and air vehicular-delivered weapons [e]
- Disrupt threat plans and operations [a,b,c,d,e] {4}

Force Protection Study

Threat – Operations Panel

83

Force protection can be further enhanced by the utilization of decoys and disinformation along with employing random patterns of movement and deployment. Another key force protection enabler is to keep threats beyond their effective range of engagement for direct and indirect fire weapons. In any hostile threat scenario ballistic and precision fire depends on the environment and range of weapons utilized. It also depends on the launch location and platform including water, land and air vehicle delivery of weapons. Improvised explosive devices(IEDs) must also be protected against whether delivered from land, sea or air.

A major force protection strategy is to disrupt the threats plans and operations by whatever means possible.



Combined Requirements



Defend

- Harden facilities, personnel, resources [e] in transit and the trans-ship points, and networks, sensors, antennas and the physical sites that support them against: [a,b,c,d] {4}
 - Cyber attacks [a,b,c,d]: hacking, viruses and enemy corruption of data [d]
 - NBC weapons [a,b,c,d,e], anti-materiel agents [c], contaminants [e]
 - IEDs/bombs [a,b,c,d,e]
 - Other HE/KE weapons [a,b,c,d]
 - EW [a,b,c,d]
 - Thermobaric weapons [a,b,e]
 - Incendiary weapons [a,b,c,d,e]
 - DE weapons [a,b,c,d,e]
 - Mines [d,e]
 - Small arms and snipers [c,d,e]
 - RPGs and mortars [b,c,e]
 - Maximize passive protection with multi-faceted armor and clothing [c,e]

Force Protection Study

Threat – Operations Panel
84

If prediction, monitoring, denying, preventing, and deterring fail to thwart a hostile attack, then we must defend our high value targets. This requires the hardening of facilities, personnel, resources in transit, trans-shipment points, networks, sensors, antennas and the physical sites that support them. Hardening must defend against cyber attacks such as hacking, viruses, and enemy corruption of data. It must also defend against Nuclear, Biological and Chemical(NBC) weapons; Radiological Dispersive Devices(RDD); anti-materiel agents and contaminants; IEDs and conventional explosive bombs: other explosives weapons such as thermobaric, incendiary weapons and mines; kinetic energy weapons; electronic warfare, directed energy weapons and other non-kinetic attack means. Hardening must also prevent casualties from small arms, snipers, RPGs, and mortars utilizing passive protection and multi-faceted armor.



Combined Requirements



Defend *(Continued)*

- Detect and deny contaminants [a,b,c] {5}
 - Fuel [a,b,c]
 - Water [a,b,c]
 - Food [a,b,c]
 - Medical supplies [a,b,c]
 - Mail, logistic supplies, and commercial delivery services [a,b,c]
 - Airborne CB agents [a, b, c]
- Employ decoys [a,b,c,d,e]; of C² nodes [d]; and deception techniques [c,d,e] {4}
- Employ counter-measures [a,b,c,d,e] {3}

Force Protection Study

Threat – Operations Panel

85

A key force protection requirement is to protect our forces by denying and detecting any insertion of contaminants into: fuel, water, food, medical supplies, mail; logistic supplies, and commercial delivered services, and airborne CB agents.

Again it will be useful to employ counter-measures such as decoys and deception techniques especially at C2 nodes



Combined Requirements



Defend *(Continued)*

- Minimize the effectiveness of an attack [a,b,c,d,e] {3}
 - Recognize the attack and its nature [a,b,c,d,e]
 - Track the attack [a,b,c,d,e]
 - Divert/deflect/neutralize the attack [a,b,c,d,e]
 - Reduce the resources available for the attack [a,b,c,e]
 - Cause weapons to fail or detonate prematurely [a,b,c,e]
 - Protect valuable resources in transit during the attack [c]
 - Ensure adversary cannot get these valuable resources [c]
 - Ensure self-healing network [d]
- Assure continuous, uninterrupted power [d] {2}

Force Protection Study

Threat – Operations Panel

86

An important element of defending against an attack is to mitigate and minimize the effectiveness of an attack by taking the following actions: recognize promptly that an attack is underway and assess the nature of the attack; track the attack for possible retaliation; divert, deflect, and neutralize the attack; reduce the threats resources available for the attack; cause the weapons to miss, fail or detonate prematurely. Protect valuable resources in transit during an attack. For all high value targets assure the integrity of their umbilicals such as continuous uninterrupted power, water, and communication networks.



Combined Requirements



Respond, Restore and Retaliate

- Rapidly detect, track, retaliate against, [a,b,c,e] and counter [d] source of attacks {4}
- Preclude future attacks using all (military, political, financial, ...) appropriate means [a,b,c,d,e]
- Rapidly determine and disseminate lessons learned [a,b,c,d,e] {4}
- Rapidly implement corrective counter-measures [e] at the installation [a,b,c] including ECM [d] {4}

Force Protection Study

Threat – Operations Panel

87

To prevent further enemy attacks, we must rapidly detect and track weapons so that we can rapidly retaliate and counter the source of the attack. We must preclude any future attacks by using any and all appropriate means whether, military, political, financial. It is imperative that we rapidly determine and disseminate lessons learned to upper level command, and local war fighters and civilians. All corrective counter-measures must be rapidly implemented include electronic counter measures(ECM)



High Priority Technology Requirements



- **Ensure assured communication capabilities to all individual soldiers and units**
- **Explore technologies that can provide more effective self-protection for individuals**
- **Establish multiple dynamic perimeters around installations and create moving protective bubbles around resources in-transit**
- **Explore appropriate technologies to harden facilities from both physical attack and contamination**
- **Provide early warning of impending attacks**

Force Protection Study

Threat – Operations Panel

88

Good communications need no justification. Without them, the warfighter can neither operate effectively nor survive. Similarly, Combat Support and Combat Service Support Soldiers cannot support the warfighters effectively and survive themselves without good communications. The panel recommends that communications assurance at all levels remain a critical priority.

Self protection for individual soldiers is an evolutionary process. However, body armor advancements in the ten-years between Operation Desert Storm and Operation Iraqi Freedom represent a quantum leap. More work remains, however, and the panel strongly recommends that The Army continue to explore self protection technologies for individual Soldiers.

Dynamic perimeters around installations and mobile protective bubbles around resources in transit represent two effective force protection strategies. The panel recommends that The Army explore technologies in these areas that will create disruptive environments for threats.

Finally, appropriate technologies to hard facilities from physical attack and contamination would provide protection for assets that other methods cannot protect.



High Priority Technology Requirements

(continued)



- Create completely independent, secure, self-healing C⁴I network and sensors that will:
 - Establish baselines to determine status of local environment
 - Monitor and verify changes in status of local environment
 - Provide rapid combat identification
- Create decoys and misinformation
- Assure continuous uninterrupted power to facilities, platforms, and soldiers

***Again, there is no affordable or effective force protection
without accurate prediction***

Force Protection Study

Threat – Operations Panel

89

The Objective Force and the FCS system of systems will dependent totally upon C4I networks and sensors. As part of the Joint Force, The Army will utilize advanced information technologies and C4ISR decision tools and assets will enhance the Common Relevant Operating Picture (CROP). The Objective Force will identify, locate, and engage critical targets with lethal or non-lethal affects and assess battle damage on those targets. The joint C4ISR linkages will enable the attack of targets with whatever joint or Army assets are available for immediate employment, whether the force is in contact or out of contact. Similarly, enhanced situational awareness will facilitate multi-layered active and passive defense measures – including both offensive and defensive counter air against air and non-air breathing, manned and unmanned aerial vehicles. Inadequate protection for C4I networks and sensors will cripple the Objective Force. For this reason, the panel members strongly recommend that The Army creates completely independent, secure, self-healing C4I networks and sensors.

Similarly, rapid combat identification will provide not only a force protection asset but also a force multiplier.

Decoys and misinformation technology would enhance force protection across all operations.

Power remains the single most critical issue. By assuring continuous uninterrupted power to facilities, platforms, and Soldiers, we assure the protection of the force.

The panel members realize that no perfect solution exists for Force Protection. Force Protection is both art and science—something that neither technology nor training alone can attain. Instead, it is the combination of advanced technological advances with appropriate training, techniques, and procedures that will give Army Soldiers the fighting edge to win the Nation's wars and survive in the day to day operations both in-theater and at home.



Observations - FP Impacts on Military Operations -



- **Casualties due to inadequate FP degrade mission effectiveness**
- **FP efforts often at the expense of mission accomplishment**
 - Forces commander into a more defensive posture
 - Changes nature of interaction with local community
 - Diverts troops from other essential missions
- **Continued small-scale attacks (on small detachments and individual soldiers) can have greater strategic than tactical impact in terms of shaping or diminishing national commitment**
- **Inadequate FP decreases soldier confidence and increases anxiety and stress in everyday operations**
- **Current fielded solutions to FP are manpower intensive**
- **Use of soldiers for FP as an additional duty obscures the full manpower cost**

Force Protection Study

Threat – Operations Panel

90

This slide is the first of four slides that presents observations that our panel learned through the analysis of requirements that we have just finished presenting.

Our review of current force protection measures shows that they are generally very manpower intensive, low-tech and inadequate.

Because they are so manpower intensive, force protection efforts have often been at the expense of mission accomplishment. For example, during the IFOR deployment in Bosnia, force protection SOPS required that each convoy have four vehicles, eight soldiers and a crew-served weapon. This meant that anytime one person needed to make a delivery or sign a form on another base, seven other soldiers were required to go with them, taking those other soldiers away from their other duties. In the most extreme, counter-intelligence and civil affairs agents were often forced to operate in the same convoy, because the unit did not have enough personnel to man the convoys and guard the small bases. Obviously, having CI and CA operating simultaneously in the local environment was completely counterproductive. In this way, force protection impeded the mission of engaging with the local population and implementing the terms of the Dayton Accord.

Finally, the full manpower cost of force protection is often hidden, because many soldiers participate in force protection actions (such as guard duty) as an additional duty. These soldiers are rarely counted in the totals of personnel performing force protection, but the time spent performing this function is significant.



Observations - Doctrine/TTP -



- Major emphasis is currently on physical protection of assets rather than precluding threat attacks
- Deterrence and prevention, as well as retaliation and response, are important components of the force protection continuum
- Unlike safety, FP is often viewed as a separate activity rather than being integral to all operations. The approach to achieving FP should be an integral part of Army operational doctrine.
- The importance of high value targets can be reduced through redundancy, deception, operational changes, and other means
- Structured, predictable methods of operation create vulnerabilities
- Countering opportunistic attacks requires real-time knowledge versus long lead-time for prediction against planned attacks

Force Protection Study

Threat – Operations Panel

91

This slide deals with observations related to doctrine and TTP. Currently, most force protection efforts focus on the physical protection of assets, rather than on preventing threat attacks. As we suggested with the force protection continuum, there are a variety of actions that commanders can take to protect the force beyond simply defense during an attack. There are a variety of actions during the pre-attack and post-attack phase that can improve force protection as well. Overall, the most important take-away is that force protection efforts taken during the pre-attack phase can have the largest pay-off. Prediction is the single most important component of the force protection continuum. A prediction capability is crucial for force protection to be the most effective, affordable and efficient.

The importance of high value targets can be reduced through a variety of operational measures, like redundancy, deception and varied routines. For both kinds of threats – deliberate or opportunistic – the more that US forces rely on routines or SOPs, the easier it is for the threat to attack and thus accomplish their objectives. Therefore, varying routines will minimize the risk of attack.



Observations - Intelligence -



- **Intelligence leading to prediction is required to achieve highly effective FP**
- **The terrorist adversary may be susceptible to intelligence collection and discovery in the extended pre-attack phase**
- **Improved intelligence can make FP more proactive**
- **Threat analysis must include both friendly and threat perspectives about high value targets**
- **Integration into the indigenous community can provide intelligence and resources to improve FP**
- **Knowledge of a potential attack is necessary but not sufficient until acted upon by the appropriate commander**

Force Protection Study

Threat – Operations Panel

92

This slide presents our conclusions about intelligence.

As our analysis has demonstrated, the most effective way to provide force protection is during the pre-attack phase, through prediction. The threat, especially terrorists and organized military and paramilitary units, is very vulnerable to detection and deterrence during its pre-attack planning and surveillance process. US forces can capitalize on this vulnerability with enhanced intelligence capability. Intelligence will make force protection more effective by making it more proactive.

As we have suggested throughout this briefing, the threat is not monolithic. Rather, the threat is actually a wide variety of different threats, ranging from organized regular military units to terrorists to criminals to diffuse and disorganized non-combatant mobs. Each of these different groups has a different modus operandi, different objectives and different US targets they attack. One way to classify different threats is to look at their planning and execution cycle. Deliberate planners have a long planning and surveillance process, which makes them vulnerable to US detection and deterrence. Opportunistic threats are less organized and less predictable, but their attacks are smaller scale.

It is important to remember that both deliberate planners and opportunistic threats value US high value targets differently than we do. From a US perspective, a high value target has value because it is critical for mission accomplishment. From the threat's perspective, however, a target is only valuable if it helps the threat accomplish its objectives, and as we said earlier, those objectives are usually political in nature. The US target is frequently only a means for the threat to reach its objective, not an objective or end in itself.

Therefore, threat analysis must include both friendly and threat perspectives on high value target valuation.

Finally, knowledge of a potential attack can only help to prevent that attack if the commander acts on that knowledge in a timely manner. Intelligence is a necessary but not sufficient means of achieving force protection.



Observations - Training -



- Countering FP threats will only become integrated into soldier and units' performance when integral to all tactical training
- FP competencies would be greatly enhanced if explicitly included in training simulations
- FP awareness and proficiency are enhanced by their inclusion into all training exercises
- FP training qualification and certification procedures are needed for all units, individuals, and civilians prior to deployment into the AOR
- Every soldiers can be a better intelligence source with appropriate observation and reporting training— “every soldier is a sensor”

Force Protection Study

Threat – Operations Panel

93

This is the final slide listing the observations we learned during our analysis. As this slide suggests, training is an important component of protecting the force. To conduct adequate force protection during a mission, soldiers and leaders must train for force protection during simulations and exercises as well. Such training will increase awareness among leaders and soldiers about the importance of force protection measures during their other missions. Ultimately, soldiers trained in force protection will be able to serve as intelligence sources, helping to predict threat attacks. In this way, “every soldiers is a sensor.” The best way to capitalize on these many sensors is to train them to observe and report threat behavior more accurately and more quickly.



Recommendations - Doctrine/TTP -



- TRADOC should develop doctrine/TTP that:
 - Focuses on the pre-attack phase as leverage for more efficient and effective force protection capability
 - Includes response and retaliation measures as part of FP planning
 - Introduces unpredictability into routine Army operations, including the use of decoys, deception, and misinformation
 - Tailors the CONOPS/TTP to reflect the specific FP threat environment
 - Provides for the development of multiple sets of rules of engagement, to adapt to changing FP situations

Force Protection Study

Threat – Operations Panel

94

Studies of threat execution cycles show that any change in a targets behavioral pattern disrupts the threat planning process. By introducing unpredictability into routine operations, U.S. Forces disrupt the threat execution cycle. Other ways to thwart attacks against high value targets include minimizing their value or eliminating them altogether. Both the Downing Report and the U.S.S Cole Commission set out recommendations that this current study re-emphasizes. In short, if the threat cannot see a target, he cannot attack it.

Because Force Protection is not an exact science of technological solutions, attacks will still occur. Therefore, appropriate response and retaliation measures must form part of contingency Force Protection planning efforts.

However, a recommendation diametrically opposed to previous studies recommends the establishment and approval of multiple rules of engagement based on the situation. Previous studies judged the standing rules of engagement for U. S. forces adequate against the terrorist threat and recommended no changes. We believe the situation has changed since the commission report and this issue needs to be readdressed.



Recommendations - Intelligence -



- Establish TTP for proactive intelligence activities during threat pre-attack phase *(TRADOC, 60 days)*
- Focus intelligence assets (HUMINT) on prediction capability
 - Establish baselines and monitor changes in status of local environment *(G2, now)*
 - Re-prioritize HUMINT and SIGINT resourcing *(CSA, now)*
- Develop policy and procedures to more closely integrate in the indigenous communities in the AOR
 - Understand the local culture, objectives, motivations
 - Improve language and culture training, invest in translation capacity
 - Understand and be prepared to address local sources of discontent
 - Deploy more CA, SOF, MP, and FAO personnel *(FORSCOM-TRADOC, 60 days)*
- Provide local commanders direct access to a dedicated intelligence capability which provides timely threat attack indicators *(G2, now)*

Force Protection Study

Threat – Operations Panel

95

Force Protection must become more proactive with improved intelligence especially during the threat's pre-attack phase. Many of the recommendations contained in this briefing reiterate those contained in the Downing Report, the U.S.S. Cole Commission Report, and other national security level studies. However, due to the escalating situation and the fact that Force Protection measures require more than technology solutions, we feel that it is imperative to reiterate these recommendations.

The Army must focus intelligence assets (especially tactical HUMINT) on prediction capability. Our operational posture must remain engaged with the local community through people to people exchanges and engagement in community activities that will allow us to monitor the local environment. Once we establish a baseline, we can monitor changes that will allow us to forecast threat attacks in a timely manner.

Becoming engaged in the OCONUS community gives us the intelligence required to address sources of discontent that can lead to attacks. Additionally, through human engagement, U.S. forces begin to understand the threat's culture, objectives, and motivations. This in turn provides the knowledge that allows them to exploit threat vulnerabilities creating disruption of plans and operations before an attack begins.



Recommendations Training



- **Develop FP awareness training packages and performance standards for use in TRADOC institutional training programs; provide FP training package to be sent to deployed units** *(TRADOC, 60 days)*
- **Incorporate FP simulation capability in simulation-supported training** *(DUSA(OR)/TRAC/TRADOC, 60 days)*
- **Provide individual soldiers with training on observation and intelligence collection and reporting necessary to contribute to the FP mission** *(TRADOC, 90 days)*
- **Incorporate appropriate FP events into field exercises** *(FORSCOM, 90 days)*
- **Develop appropriate metrics to evaluate individual and unit success in FP** *(TRADOC, 60 days)*

Force Protection Study

Threat – Operations Panel

96

The panel recommends that The Army develop contingency operations and rigorous tactics, techniques, and procedures with measurable Force Protection training standards. Training regimens should integrate Force Protection into unit-level training plans and pre-deployment exercises. We cannot emphasize previous recommendations strongly enough that Force Protection training should be the equivalent of a primary mission area and provide the same emphasis as combat tasks. This will inculcate a force protection awareness across The Army.

***Army Science Board
2003 Summer Study on
Force Protection***

***“Force Protection Technologies
for the 2010-2020 Timeframe”***

Technology Solutions Panel Report



October 2003

Technology Solutions Panel Report

Table of Contents

Executive Summary

1.0 Introduction

- 1.1 Force Protection Challenge
- 1.2 Principal Themes
- 1.3 Visits

2.0 General Technology Recommendations

- 2.1 Force Protection Umbrella
- 2.2 Network Technology
- 2.3 Decision Aids Technology
- 2.4 Sensor Technology
- 2.5 Automation and Robotics Technology
- 2.6 Weapons and Survivability Technology

3.0 Specific Recommendations

- 3.1 Technology Investment
- 3.2 Army Implementation of FP Integrated System
- 3.3 Force Protection Architect
- 3.4 Force Protection Organization
- 3.5 Integrated Network Centric FP ATD

4.0 What Can We Do Immediately?

5.0 Summary: Conclusions and Recommendations for FP Technologies

- 5.1 Networks
- 5.2 Decision Aids
- 5.3 Sensors
- 5.4 Automation and Robotics
- 5.5 Weapons and Survivability

Appendix:

- I. Panel Members
- II. Briefing Charts (4 charts per page)

Executive Summary

The Force Protection Summer Study Technology Solutions Panel was chartered to simultaneously address two potentially conflicting requirements: first, to identify technology solutions that could have a high impact on the immediate force protection needs of our deployed troops; and second, to identify long term technology-based solutions to the overall force protection problem. Through our deliberations, site visits, and study, we found that there is no dearth of technical tools available in the marketplace. There is a large and vibrant community of suppliers of technologies ranging from perimeter security to design tools that can be procured and deployed today (it is only a cost-benefit issue). However, we also discovered that the availability of the large number of tools is a dual-edged sword. The value that each tool provides the commanders who chose to deploy them is incremental to the tools deployed before. ***There is virtually no leveraging effect in which the tools work together to provide significant combined benefits.***

Further, the large number of available material solutions confuse the selection process for the commanders who have to make the deployment decisions. ***There are virtually no tools that allow commanders to determine best practices in selecting and deploying protection solutions; nor are there tools that provide assessment of appropriate responses to the output of the tools.*** Decision-making today is driven by human intuition and human-centric analysis processes. In particular, we could not find any analytic or computational tools that would allow commanders to reason about extreme low probability events, and long timelines as are encountered in most force protection scenarios.

We also found that the force-protection technology community (alluded to earlier) is focused on the dominant, low-tech threats. High impact asymmetric future threats such as biological weapons are not being, and indeed, cannot be adequately addressed by the existing vendor community for various commercial and technical reasons. ***Consequently, there is inadequate support for the development of desirable portable broad-spectrum biological sensing tools to augment the more traditional sensors that exist.***

Force Protection (FP) is a global multi-scenario problem. For tractability during this study, we decomposed the problem into four canonical scenarios: CONUS Base, OCONUS Base, Convoy, and Small Detachment team. Within each canonical scenario we identified numerous different situations. It was neither practical nor feasible to develop stovepipe-like FP solutions for every scenario. By recognizing that every FP system has common technology components (networks, decision aids, sensors, automation & robotics, and weapons & survivability) we identified the building blocks for FP system solutions that can be tuned to any given scenario.

Our recommendations address our key conclusions. We recommend the adoption of a ***Network-Centric Integrated Systems Approach (NCISA)*** to the optimization of all force protection tools. This should be backed by a strong focal point for the associated systems

engineering effort, an articulated vision reinforcing NCISA, and a permanent testbed for demonstrating and analyzing force protection technology solutions. We recommend the creation of a well funded program for the development of an integrated **Decision Support System** that would provide commanders with cradle-to-grave analytical capability in the selection, deployment, and employment of force protection tools. We also recommend a renewed commitment by the Army to funding the development of a capable, lightweight, **handheld biological pathogen detection system**. Finally, we recommend an increased focus on integrated **human-robotic-team** solutions to reduce the manpower currently deployed on routine patrol missions.

The consolidated panel recommendations are:

Recommendation 1: Technology Investments should be encouraged and funded in the following areas: Decision Aids Technology, Unmanned Vehicle Technology, Sensor Technology, and Weapons and Survivability.

Recommendation 2: CSA create vision of Force Protection as a Network Centric Integrated System (Force Protection Umbrella).

Recommendation 3: A Force Protection Architect must be identified.

Recommendation 4: CSA task the G3 to develop an Organizational Solution for Army Force Protection

Recommendation 5: Army sponsor an integrated network centric Force Protection ATD (FY 2004)

***A new vision of Force Protection is required.... A
Network Centric Integrated System!***

1.0 Introduction

1.1 Force Protection Challenge

The Force Protection Summer Study started with the expectation that a set of tools could be found to assist the deployed Army. In reality, there is a large industry supporting the physical security requirements around the world spending large quantities of money developing products to improve safety and security. Parts of the Army's Force Protection needs can be met today by just buying components and installing them at Army posts and deployed locations. This would address near term problems; however, it does not address the complete needs of the Army. There is more to the solution than just buying parts and installing them. The key is networking today's systems to enable the Army to make a large leap forward and provide dynamic and responsive Force Protection systems to our troops. Thus, the basic challenge for this study team was:

Challenge for the Technology Solutions Panel:
Assess and recommend current and future technologies for Army Force Protection

After the six months of study and travel to various locations, the Technology Solutions panel found that:

1. A wealth of proven technologies are available TODAY; however, the technologies are individual islands without a systems approach.
2. A Network Centric Integrated Systems Approach (NCISA) needs active and immediate high-level recognition and support.
3. This network centric architecture could help alleviate the lack of data exploitation and sensor fusion technology

1.2 Principal Themes

Throughout this study, many ideas surfaced that looked attractive to pursue. It turns out that there are many paths to follow and many advocates of different approaches. However, this study group found that there were five principal themes that cut across the study.

The principal themes are:

1. “Network Centric Integrated Systems Approach”¹ – network centric, standards based, self healing, graceful degradation, plug-and-play
2. Overlap with current Army programs allows leverage of equipment, funding, and processes
3. Some requirements/issues are specific to “force protection”
4. Techniques to deal with extremely low probability events over extremely long time periods
5. Commanders need a decision support system to help them optimize their Force Protection strategy and tactics.
6. Force Protection Technology can significantly enhance U.S. Army unit survivability.

1.3 Visits

The visits that were conducted during nearly a year long activity were varied and covered the total scope of Force Protection technologies. The list of locations is given below, while details are expanded upon in Appendix II, Briefing Charts. Each location provided a very valuable insight into many aspects of the problem and provided some potential solutions to the current Force Protection threats.

CECOM	ERDC	JPEOCBD	TWSG	ICT
ARL	ARKL	PEO IEW&S	USA NVL	ECBC
PEO / PM-PSE	JCS JAT	INSCOM	Sandia	
JPO		Quantico	DTRA	
JCS J-3	DARPA	USAF / BDSS	USAF TAS	Information Op’s Center

One very informative visit was the DoD Force Protection Demonstration at Quantico. A great deal of insight was gained into the availability of technology, both now and in the near future. Many suppliers displayed their equipment and showed the effectiveness of each piece. The superb show of equipment and modestly configured systems was an “eye opener” to the panel on the availability of equipment. There were approximately 400 exhibitors of hardware with significant international representation. One observation was that most of the exhibitors were displaying components, rather than systems. There were companies of all sizes, with some small ones that were literally

¹ During this study, the term “**System of Systems**” surfaced many times and led to multiple definitions. Our study team tried to understand the term and what it meant for this effort. When used in this report, the term reflects a rigorous engineering approach resulting in a balanced system with an architecture that integrates all elements of Force Protection (e.g. weapons, sensors, decision aids, automation/robotic, networks and survivability). The study group ended up with the term **Network Centric Integrated Systems Approach** rather than Systems of Systems to make it clear that at all levels the global perspective should be applied.

operating on a shoestring. There were many interesting items for exhibit, to include, night vision devices, 360-degree observation devices, area lighting, commercial armored vehicles, non-lethal technologies, and x-ray back scatter machines for container examinations. Most of the industry was working toward parts and components. There were lots of COTS and GOTS, but very few systems. And, no major integrated systems approach to Force Protection was presented by any company. The Air Force base defense set-up was as close to a NCISA as exists today. A CD is available showing the COTS and GOTS.

2.0 Technology Solutions Panel Overview

2.1 Force Protection Umbrella

The basic conclusion from this Force Protection Technology Solutions Panel is:

Current (COTS/GOTS) and future technologies should be leveraged into a Network Centric Integrated System for optimum protection of our soldiers in the Force Protection arena.

Study members represented the proposed integrated system as an umbrella for Force Protection. This system would consist of four integrated functional elements. (1) The foundation is a network centric environment with a decision support system (DSS) encompasses applications to aid the FP commander in maintaining a full understanding of his/her environment (as part of total Common Operating Picture). This DSS should efficiently establish FP security, allow for flexibility of system emplacement, and enable rapid decisions for force response. The three enabling pillars that provide data collection and defensive responses are: (2) sensors; (3) robotics and automation; and, (4) lethal and non-lethal weapons. This NCISA provides a Force Protection umbrella reacting to the diversity of threats. This integrated approach will provide the commander with a system that is dynamic, flexible, modular, and with capable of providing timely situational awareness, and appropriate response.

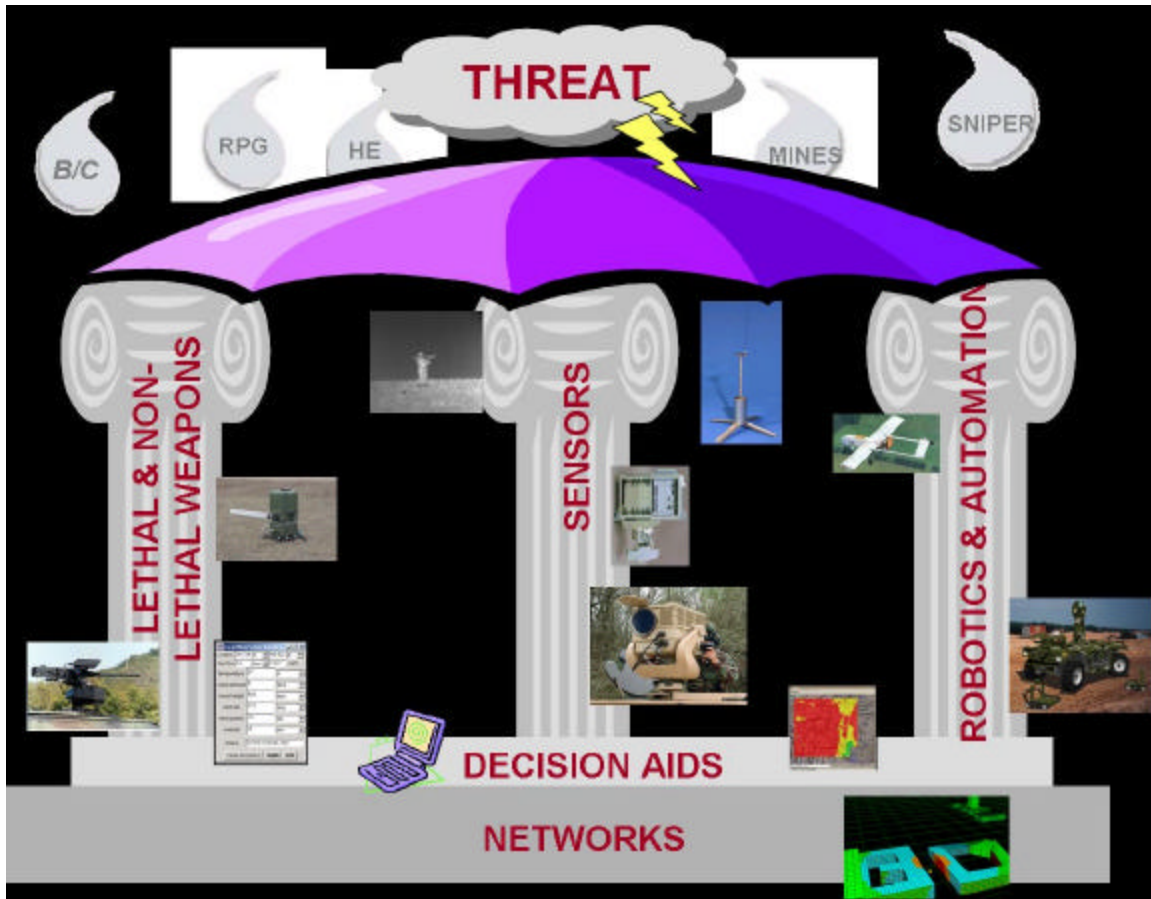


Figure 1, Force Protection Umbrella

To accomplish this Integrated Systems approach, future technology investments, augmentation of GOTS and COTS, should include:

2.1.1 Network Technology

The network sub-panel team identified three major conclusions. First, an integrated approach to network assurance is needed. Second, the Army should focus their development efforts on the totality of information management, data flow, network, and radios to support network-centric operations. Third, an approach needs to be developed for providing soldiers with the additional IT skills necessary for the future Army.

A recommendation is that the Director of Army's CERDEC (RDECOM) direct the System Engineering Office (CERDEC ASE0) to be the responsible office for integrating and maintaining an Army-wide policy and network for force protection. In addition, this office should be given the responsibility for determining how and what level of IT support will be needed through the various spiral development

phases of network development for FCS. This should include the IT expertise required of the individual soldier, and how the Army will interface to host-nation IT infrastructures.

2.1.2 Decision Aids Technology

The application of Decision Aids Technology, information, and knowledge management can provide leverage to successful Force Protection way beyond the cost of the implementation of this technology. Decision Aids Technology includes the essential information collection and fusion, required for information and knowledge management for the commanders Force Protection C2. These technologies are a powerful adjunct today to the development of knowledge management and will become exponentially more capable over the next 10 years. The ability to use knowledge to make improved and more timely decisions based upon the knowledge provided by these technologies is discussed in this report. The commander's decision cycle needs to be supported by FP Decision Aids throughout the FP process, starting with planning and ending with mission accomplishment. This process can repeat and extend for days, weeks, months or years. The Pre-Attack, Trans-Attack and Post-Attack phases can all be supported by decision aids. **A recommendation is that technological leverage for the near and far term should be focused as an integrated and tailored Force Protection System centered about a Commander's Decision Support System (DSS).**

2.1.3 Sensor Technology

A tremendous variety of sensor systems are being developed in the DoD community, sometimes responding to specific Army needs. Emphasis during the study was placed upon biological agent detectors and identifiers because such detectors are absent from most military platforms as well as on the dismounted soldier. Multi-array sensor technologies have become a reality for Biological agents. These have the capability to detect and identify threat agents as point detectors but not stand-off detectors. The ability to produce agent detectors and identifiers that can regenerate functional surfaces and therefore sustain operation for extended periods of time in an autonomous/robotic mode is yet to be realized. Stand-off detectors for chemical agents are available using spectral analysis in the visible and infra red range. Point detectors utilize gas chromatographic and mass spectroscopic devices. Radiological detectors for portal analysis are available using technology developed in the Second Line of Defense (Sandia).

Recent events have increased the need to detect sealed and encased high explosives. HX, high explosive, can be detected from unsealed sources by analysis of emitted volatiles. Sealed or encased sources can not be detected today using field ready equipment. Some plastic coatings of land mines can be detected by analysis of volatile compounds from the casing. Radar and infra red systems can be used to detect vehicles and persons. **A major recommendation is that this variety of sensors be refined, developed and deployed in a more consistent manner within a Network Centric Integrated FP System.**

An intriguing discovery was that vision systems capable of sensing and automatically processing video imagery to determine patterns of activity are being developed by several groups, including ARL and DARPA. These technologies can have significant impacts in reducing the manpower required to observe and monitor large areas, especially in crowded urban environments. The Army should make significant investments in the development and maturation of this technology and deploy systems that embody this technology as rapidly as possible.

2.1.4 Automation and Robotics Technology

General findings and conclusions were that robotics technology is maturing rapidly, and is now capable of insertion into the field in restricted environments. For example, the MDARS (E) program for the development of a perimeter patrol robots could be deployed now. With continued funding from programs such as the Future Combat System (FCS), autonomous robots could be operable in less restricted environments within a few years. Further, the investments being made by DARPA on refining the video processing technology through the “Combat Zones that See” program, have significant benefits in the Force Protection realm. These technologies should be rapidly matured and accelerated into the field through Army investments in ATDs and supported through ACTDs. Force Protection technologies are applied more often in fixed locations versus combat environments. In these environments, current levels of semi-autonomous and autonomous robotics technology can be readily deployed. **Two recommendations are: (1) the Army should accelerate the deployment of semi-autonomous and autonomous robots for tasks such as perimeter protection and convoy operations, and (2) the Army should invest in furthering the technologies for the collaborative use of unmanned ground and air vehicles in such surveillance applications, and in rapidly maturing the existing programs for robotic followers.**

Another finding was the lack of a suitable integrated test beds for integrating and evaluating FP technologies in a systems context. All three services have indicated a desire to have test beds for evaluating FP technologies in controlled environments. However, these test bed concepts need to be expanded to include the development of architectures, CONOPS, and integrated tactics. Without such a broad test bed, the appropriate utility of the FP technologies will not be realized.

2.1.5 Weapons and Survivability

Major fixed bases, whether Army bases, airfields, or depots, tend to have assets spread over large areas. Also, they are vulnerable to attack by indirect fire originating in even larger potential areas. The combination of these two factors plus the short flight time attacking weapon makes active area protection difficult. The situation makes an indirect fire weapon such as a mortar a likely weapon of choice. A representative older design is the French Hotchkiss-Brandt 120 mm design. This mortar weighs slightly less than 100kg and can be carried by a three-man team. Each round weighs 14 kg and can be fired at 8-15 rounds per minute. Presumably the rounds could be terminally guided using GPS or a forward observer equipped with a laser designator.

Active point defense of high value targets is probably achievable. The mortar round can be tracked by radar and its ballistic trajectory computed. As it is a threat to a high value target, a short-range defensive missile can be fired to detonate either by proximity fuse or at a predicted time and place, deflecting the mortar round's trajectory more than the guidance can correct. Typical high value targets are troop concentrations (e.g. barracks, mess halls, parked aircraft, ships in port). Active defenses should be mobile so that their locations vary with the presence of people or assets. To be effective, counter-battery fire may need to be direct fire from an UAV or UGV. Depending on the rules of engagement, responses may be lethal or less-than-lethal. Convoys could be attacked on the move or at a stop if the place and time of a stop is known and reported in real time.

Table 1, Threat Responses

	Highest Potential	Useful Potential
Indirect Fire	Multiple sensor integration Illumination control Armed UAV's	Bomb shelter Personnel areas ballistic protection Preventive point defense Counter fire
Direct Fire	Non-lethal Weapons Mine detection and neutralization Illumination control Armed UAV's	Commercial armored vehicles Personnel areas hardening
Vehicle	Remote explosive detection and neutralization	Inspection areas Air defense
Suicide Bomber	Stand off explosive detection and neutralization Human behavior screening	Isolation area for suspects

Whether protecting a fixed base or convoy, the key elements are vulnerability reduction, prevention, and quick reaction. Defense problems are magnified by possible wide variations in threat level, weapons, objectives and tactics. Effective perimeter surveillance and prevention of entry are key factors for fixed bases. Earlier studies [ASB 2001] calculated that deployment of armed UGV's reduced losses significantly. Table 1, Threat Responses, compares the four threat categories and expands on appropriate protection technologies and methodologies.

2.2 General Findings

The panel distilled the information gathered from site visits, briefings, and discussions with Government and industry personnel into four general findings that reach across the Force Protection arena. They are:

1. There are many successful programs working in various aspects of Force Protection; however, no single proponent or system architect for Force Protection was identified.
2. After viewing many R&D and S&T programs around the Army, concern was raised in a familiar area: Much of the successful Force Protection S&T does not transition to the field.
3. Components that do transition, are left to the field commander to identify and integrate. Once again, individual pieces vs. an Integrated Systems approach.
4. A Network Centric Integrated Systems Approach is essential to ensure adequate Force Protection for our soldiers.

2.3 Major Conclusion:

Based upon these findings, the major conclusion that the Technology Solutions Panel reached was:

**Fielded Force Protection capabilities are
fragmented and often ineffective**

3.0 Specific Recommendations

Solid recommendations surfaced during this investigation and were categorized in five areas. An intriguing aspect across the Force Protection arena is that many people know what to do and how to do it, but, they are not in an organizational location empowered to bring an integrated system to the field. The following is a quick summary of the major Recommendations that surfaced, with further discussions in the next few sections of this report:

1. Technology Investment
2. Army implement FP integrated system
3. Identify a Force Protection Architect
4. G3 develop an Organizational Focus
5. Sponsor an integrated network centric FP ATD

3.1 Technology Investments

There are many excellent S&T and R&D Force Protection programs in the Army's development plan. The panel recognizes that in addition to the availability of GOTS and COTS there are investment programs that must go forward. Here are some of those that should be **encouraged and funded**:

Decision Aids Technology

- Tools for Intelligence Preparation of Areas of Interest (Staging Areas, Convoy Routes)
- Army RDECOM (SOSI/ARL) develop an Integrated Force Protection Decision Support System (DSS) for the Commander. This would include many decision support technologies with support to the Commander in all phases of Force Protection (defend, preempt, deceive, etc.). The purpose of the tool would be to provide recommended actions and implementation plans for the Commander in a timely manner. However, it is currently difficult to accomplish cost benefit tradeoffs to improve the Decision Support System across the individual decision aids, with no plan to solve this issue in the future.

Unmanned Vehicle Technology

- Joint UAV/UGV Collaborative Surveillance Capabilities
- Semi-Automated robotics for convoy operations

Sensor Technology

- Army develop a small, lightweight, power efficient, biological sensor, able to detect all DOD identified biological agents with minimal false positive/negative outcomes [ARL/ECBC lead effort in partnership with other agencies and services]
- Remote Detection of Encased/Sealed Explosives (Countermines, VIEDs, IEDs)
- Video, Visual/IR, Lidar and Radar Continual Surveillance
- Sub-terrain Sensor (Acoustic/Seismic/RF Monitoring)

Weapons and Survivability

- Dynamic Large Area Illumination Control
- Non-lethal Weapons
- Reliable mine / IED detection on the move

3.2 Army Implementation of FP Integrated System

The recommendation in this arena is oriented toward organizational and leadership issues. The Integrated Systems Approach recommendation is:

CSA create vision of Force Protection as a Network Centric Integrated System (Force Protection Umbrella).

This vision should be focused around the network centric concept with strengths such as; plug-and-play equipment; alternatives which could be tailored to the commander's needs; extensive use of COTS and GOTS; and, grounded in good systems architecture and systems engineering processes, procedures and standards. One key would be the Decision Support System using field commander's inputs to ensure that

his/her view is accounted for during the refinement of requirements. This vision would require some centralized management, a continuous refinement of a Force Protection Architecture, and a process to ensure future life cycle development and maintenance activities.

3.3 Force Protection Architect

The reality of the development world in today's DoD is that without a single point of focus to pull together the diverse organization, developmental, operational and mission needs, Force Protection for our troops will not improve. The current practice is to develop three separate architectures; operational, systems and technical. Each has a place in the development cycle and deals with various parts of the program. The need is real to have just one person in charge of developing the DoD required trio of architectures.

A Force Protection Architect must be identified.

3.4 Force Protection Organization

There are multiple aspects to this action.

CSA task the G3 to develop an Organizational Solution for Army Force Protection.

The first is that TRADOC should develop a "school" for the Force Protection activity. In addition, AMC should identify a single focus for the Systems of Systems Force Protection R&D. To ensure that the development cycle does not get derailed, a PEO should be identified as the acquisition "Czar." This PEO would then address the risk management role, be responsible for the systems development and the life-cycle support systems and tools, and provide technical and operational support to the various entities deploying the Integrated FP System. These would include tactical and installation entities (Installation Management Agency & Installation and Tactical Commanders). The PEO would also be responsible for the R&D and COTS community integration while providing focus for other services and government agencies (notably Homeland Security).

3.5 Integrated Network Centric FP ATD

Army sponsor an integrated network centric FP ATD (FY 2004).

This ATD would illustrate the integration of many classes of sensors, decision aids and networks. As a minimum, it would contain soldier portable 2 lb bio sensor (small, lightweight, power efficient, biological sensor, with minimal false positive/negatives); soldier portable 2 lb chemical sensors; mobile sniper response sensor; mobile mortar response sensor set, UAV/UGS combine mine team, suicide bomber identification; and, block zero Decision Support System (DSS); additionally, the Army

(AMC) should conduct urgent study of means, tactics, and payoff for novel illumination control over threat based and defended areas or corridors.

3.6 Closing words:

In today's world of Army global deployments, Force Protection takes on an importance beyond the historic look at boundaries and sentries. An integrated systems approach is critical to the "enabling" of the Army's mission when personnel are sent in harms way. A new way of thinking, intense training, centralization of doctrine, and flexible hardware availability are key elements to mission success.

***A new vision of Force Protection is required
A Network Centric Integrated System!***

4.0 What Can We Do Immediately?

The Technology Solutions Panel was asked to “brainstorm” about the equipment that could be shipped to our troops in IRAQ today (within 90 days). Without trying to prioritize, the team spent a short amount of time developing this list. The list was then pared down by the rest of the study participants to determine the highest priority and the most likely to succeed.

The following table reflects the creative aspects of delivering equipment to help our troops in harm’s way. Some ideas have merit and some have potential. Someone needs to be given responsibility to execute, and good things could happen.

Table 2, List of Ideas for IRAQ

Send more of	New concepts to IRAQ
Shortstop (jams radio controlled explosives)	Lifeguard Sniper Detection
Spider (Area Surveillance)/ JLENS	PILAR (French) Sniper Detection
Sniper Detection	UAVs
Other “jam-proof” weapons	UGVs (eg MDARS)
Commercial GPS	Technical Advisors (Government and Industry)
Commercial Armored Cars	DROZD/ARENA with paintballs instead of ball bearings
JLENS Comm’s Relay (Aerostat Relay for Military Comms)	Elevated IR mortar locator
Non-Lethal Capability sets (move from other Army units)	Truck Tracking Satellite
Commercial Non-lethal weapons (TASERS)	LOJAC
Selected Decision Aids	Downed pilot location network for individual soldiers
Perimeter Illumination	Commercial Emergency Locator (Individual Tags)
More Iridium/INMARSAT phones	NVGs for support soldiers (commercial version)
Commercial perimeter and detection systems	Weapon Detection (magnetic wand, portals)
Prison perimeter security equipment	Magnetic balance loops detecting metal movement
Wichmann’s Ground Penetrating Radar for Mine Detection	Nitrate trace detector (signature of handling explosives)
Tunnel Detecting Technology	Cell/TETRA commercial infrastructure (with hand held unit)
	Current commercial imagery from space
	Commercial broadcast audio and video propaganda
	Commercial Bulldozer
	Funding to purchase weapons from Iraqis

5.0 Summary: Conclusions and Recommendations for FP Technologies

The Technology Solutions Panel within the Force Protection Summer Study was further divided into the following sub-panels: sensors, networks, robotics and automation, weapons, and decision aids. Each subpanel worked independently, but achieved cross fertilization through members that worked across several subpanels. A cross listing of the members and their subpanel assignments is shown in Table below.

Table 3: Subpanel Membership

	Networking	Robotics & Automation	Decision Aids	Sensors	Lethality
G Glaser			x	x	
M Hofmann		x	x		
D Kelly	x				
I Kohlberg					x
S Korngluth				x	
G Lew	x				
R Montgomery				x	x
P Mulgaonkar	x	x	x		
J Reese			x	x	
P Tilson			x	x	
R Mosher				x	
M Toscano		x			x
J Wade				x	
R Woodson				x	
J Wisniewski	x	x	x	x	x

The sections that follow summarize the individual subpanel findings, conclusions and recommendations. These recommendations provide a finer granularity on the overall panel findings, conclusions, and recommendations already presented.

5.1 Networks

The networks sub-panel goal was to examine how the Army might improve networks used for Force Protection. The timeframe considered was short term (through 2006) and long term (2010-2015). Mr. Pete Van Syckle provided a series of informative briefings at CECOM. These briefings were particularly focused on information and network assurance, in addition to other topics such as FCS communications.

Table 4, CECOM Briefings

JTRS Squad Level Comms	Dynamic Re-Addressing and Management (DRAMA)
FCS Comms	Free Space Optical Communications System (FOCUS)
MARCON-I	Adaptive Joint C4ISR Node (AJCN)
MOSAIC	Networked Sensors for the Objective Force ATD
On the Move SATCOM	Tactical Wireless Network Assurance
Advanced Antennas	

5.1.1 Network Findings: There are many aspects to networks and network protection. This presents a major challenge, in that many of these areas are treated in a disjoint manner. This sub panel` found three key themes in its research. First, much of the technologies needed for force protection are also needed for other military operations, both combat and non-combat. Thus, while we identified a few force protection related technologies, most are general technologies needed for the protection of any network. Second, our belief is that, in many instances, low tech solutions may be just as important and effective as high tech solutions. Third, it appears that there is inadequate funding available to develop the needed network assurance technologies.

5.1.2 Network Conclusions: There is a definite need to trade the low and high tech solutions to Force Protection. The low tech needs are: each soldier must be trained to basic IT levers, there must be physical security of all components of the network, IT procedures must follow good COMSEC guidelines, and there is a definite need for contractor and in-country support. The high tech needs are also understandable and executable with items like quick purge of data, over the air re-keying, remote disable of users and nodes, re-routing of traffic to exclude persons or nodes, and network intrusion detection.

In addition, important areas lack sufficient commercial R&D funding. Many should be funded by the DoD and Army. Some technologies that should be funded are: network intrusion detection; COMSEC and multi-level security, protocols and data formats for Force Protection and information assurance; “Guard” – transfer info from one level to another, protection from unauthorized access at all levels; Interoperability with other and legacy systems, conforming to standards; Role-Based Access Control – Tie the network access of each soldier to his/her role rather than visibility; Group Key Management – Dynamic, flexible, rapid re-keying in battlefield, secure multicast (no commercial standard); Ad Hoc, Mobile, Self Organizing Networks; Small, Easily Erectable Masts; Low Profile OTM Antennas; Smart antennas; Spectrum - Restricted Frequency Assignments; Geographically Impacted; and LPI, LPD, anti-jam communications. The Army should also focus development efforts on information processing, data flow, networks and radio to support network centric operations.

In addition, the Network sub-panel identified three top-level conclusions. First, an integrated approach to network assurance is needed. Second, the Army should focus their development efforts on the totality of information management, data flow, network, and radios to support network-centric operations. Third, an approach needs to be developed for providing soldiers with the additional IT skills necessary for the future Army.

5.1.3 Network Recommendations: This study recommends that the Director of Army's CERDEC (CECOM) direct the System Engineering Office (CERDEC ASEO) to be the responsible office for integrating and maintaining an Army-wide network force protection and policy. In addition, this office should be given the responsibility for determining how and what level of IT support will be needed through the various spiral development phases of network development for FCS. This should include the IT expertise required of the individual soldier, and how we will tie-in to any host-nation IT infrastructure.

5.2 Decision Aids

The sub-panel of the Force Protection Technology Panel for Decision Aids was established in January of 2003 and met several times to receive briefings, and discuss the relevance of Decision Aid technology to the Force Protection issue. The sub-panel attempted to address the technologies and applications needs of commanders for current and future Force Protection decision support. This report covers the meetings, briefings, background, findings, conclusions and recommendations that the sub-panel members thought were the most important results of their 6 month effort.

As always, a short intense effort with a small group of experts is constrained to providing an overview and impression of the issue not a comprehensive analysis. Therefore, it is important that this report be recognized as a starting point for developing a good understanding of the decision aid technology and its importance to the US Army Force Protection objectives and not a final determination

The sub-panel on Decision Aids had an extremely broad view or scope of the Decision Aid boundary. It was assumed that the Decision Aids area covered all information processing for the commander's force protection C2, the development and organization of the data bases supporting C2 allocation of the FP processes and the information and C2 interaction with Peers and other Echelons. Key components of the Force Protection Decision Aids set are:

Threat Behavior Prediction (Indications and Warnings)

Technology is producing better capabilities to provide commanders with forecasts of adversary intent. These predictive capabilities derive from analytical decision and behaviorally based models. These models can be invaluable when used by commanders as decision support tools for shaping and adjusting their force protection postures prior,

during and after deployment. Development, demonstration and testing is ongoing among a number of organizations including DoD, National Guard, Federal, State and Local agencies as well as commercial entities. For example, under DARPA's War gaming the Asymmetric Environment (WAE) program models are being developed based on behavioral prediction theory and computer-based reasoning techniques. WAE relates arrays of behaviors exhibited by all parties involved to include the adversaries to arrays of responses. Therefore, when certain arrays of behaviors are detected under certain conditions, in certain locations, etc., certain adversarial responses of certain types can be predicted. Such predictive technologies, when combined with automated information extraction technology, will support a continuous indication and warning capability that will aid analysts in providing earlier, more specific warnings of threats. In addition, when combined with a decision aid such as that envisioned in DARPA's Rapid Analytical War gaming (RAW), various intervention strategies can be evaluated very quickly.

Perimeter Security

Perimeter Security is a very rich area of technology. The Services have extensive development programs under way (e.g. Smart Gate, IBDSS, Electronic Fence, etc.). In addition, there is a very mature set of perimeter security system available to the Army for deployment, barriers, fences, sensors, deterrent and delay systems). This is coupled with the extensive commercial development (as noted at the recent TSWG sponsored FPED at Quantico – see the 2003 “FPED IV” CD). However we have not identified an integrating decision support system to assist the commander in implementing, monitoring and respond to changes such a threat, weather, attacks and Intelligence and Mission changes. It is essential that a DSS tool be available to support the effective deployment, monitoring and reaction to the perimeter security systems, which need to be deployed in depth with complimentary effects. The DSS tool needs to be developed in conjunction with the sensors, barriers, identification, and reaction technologies and be able to predict the effectiveness, shortfalls and changes to the deployed systems to provide the Commander an understanding of the perimeter security risks against a broad range of threats and alert conditions.

Intelligence Fusion

The intelligence community (IC) is implementing various software tools to provide both the analysts and intelligence user with the ability to efficiently utilize derived information. The Army FP activity can benefit from these efforts. As an example, the Joint Intelligence Virtual Architecture (JIVA) program is an in-place evolving system currently within the IC, research centers (e.g., NAIC, MISIC, NGIC) and Joint Intelligence Centers (JIC's). JIVA provides users with a system to provide direct access

to necessary data bases, information retrieval tools, and collaborative means to communicate and support interactive analysis and data exploitation. JIVA is not currently interfaced with lower echelon forces, but nothing precludes its use.

Multi-Sensor Fusion

Currently exists the capability to correlate different type sensors' data outputs to enhance interpretation of collection. For example, microwave and infrared collection of a given field of view can be overlaid to provide complementary information for higher probability of detection and identification. Automatic Target Recognition (ATR) is primarily in the research and development stage and will likely not be available in the 2010 time frame. Combining target recognition techniques with human in the loop is available and improving. Decision Aids which are supportive of the Force Protection mission span a broad range of maturity (or TRL level).

Weather Support to Force Protection

A wealth of worldwide weather information from a number of sensors and reporting stations is available to support force protection. Terrestrial meteorological reporting stations throughout the United States and cooperating foreign nations provide regular weather observations to the National Oceanographic and Atmospheric Administration's (NOAA) National Weather Service, where it is combined with sensor data from several meteorological satellites to support worldwide weather forecasts. In addition to the civilian weather sources, the Department of Defense (DoD) operates a constellation of Defense Meteorological Satellite Program (DMSP) satellites that provide high resolution information in the millimeter wave, visible, and infrared bands of cloud coverage and temperatures, atmospheric water vapor content, sea surface temperatures and winds, land surface temperature, snow cover, precipitation, and soil moisture content. Furthermore, the U.S. Navy Fleet Numerical Meteorology and Oceanography Center uses all-source data from DMSP, NOAA, and maritime reports, to provide weather reporting and data services to all DoD users worldwide. Global weather information from NOAA, DMSP, and the Fleet Numerical Meteorology and Oceanography Center is archived for future use in prediction and forecasting.

Weather information plays a vital role in force protection. Archival weather information can be used to determine the trafficability of planned convoy routes. Weather archives can also be helpful in planning permanent or deployed bases by providing information of historic rainfalls, snowfalls and accumulations, periodic flooding, soil moisture content, and availability or lack of water sources. Current and forecast weather information are important planning and decision tools in support of current operations, while predictive weather models can provide valuable insights for long range planning. Predictive weather models are also important tools for intelligence preparation of the battlefield (IPB), helping to highlight vulnerabilities and improving survivability.

Images and sensor data from weather satellites can provide synoptic information on current weather and cloud patterns, precipitation, atmospheric water content, and fog which are necessary when planning aircraft, airdrop, or UAV operations and can have a direct affect on force protection.

National Systems Tasking and Dissemination

National Systems can provide a broad spectrum of products to support Force Protection when these systems are properly tasked. These products are generally requested through the G2 and are delivered through various means and timelines. National products can be made available on demand as regular periodic, regular-as-available, and *ad hoc*, with times of delivery ranging from minutes to days, depending on the collection tasking and production cycle of the particular system, method of delivery, and relative priority of the tasking. Delivery of products can be through G2 channels or, in some cases, directly to the user. In the future, National products can be expected to be delivered through the Global Information Grid (GIG), perhaps improving the speed of delivery.

Decision Aids and the Decision Related Structures Program

The purpose of the Decision Related Structures (DRS) program is to create an agent modeling simulation environment for the purpose of *assessing vulnerabilities* to the leader centric, network enabled, digitized battlefield. The simulation model parameterizes the decision-making processes (DMPs) on the battlefield. Execution of the model generates time series state data that is used to compute metrics and performance measures. It is the relationship between parameters, DMP logic, metrics and performance data that forms the basis for vulnerability assessment. DRS is based on the integration of discrete-time, agent-modeling simulation of the battlefield, with a suite of analytic technologies to provide a ***predictive*** decision aid for the battlefield command. The battlefield domain model is centered on the decision-making processes (DMP) of the battle commanders. The supporting communications infrastructure for the DMPs is modeled to provide the necessary information related to maneuver, engagement, and sensing. An important aspect of the suite of DRS decision aids is the reference time frame. Decision aids designed to address tactics on the battlefield have decision cycles in the order of minutes and to a few hours. Decision aids that address doctrinal issues may span the course of days to months. DRS, through multiple levels of abstraction address a spectrum of decision time frames.

There are several sub-disciplines critical to better understanding the phenomenon of rare events, some of these already share space in terms of methodologies and world view. Funding would encourage a more targeted joint endeavor. Such areas as logic analysis (e.g., King and Zeng, 2001) and cognitive engineering (e.g., Hancock, 2002, Parasuraman, 2002) need to refine some of their methodologies and metrics to better consider a new appreciation for the need to explain rare events. Addressing this problem and developing the proper tools will also help in addressing low probability, moderate consequence events--- that characterize the CONUS force protection problem.

A large number of developments are on-going in the DoD which support future US Army force Protection options. Typical of these would be the deployable sensors (UGS) associated with these two programs. Developments of sensors capable of large area surveillance for vehicle or personnel movement are valuable for all the cases under consideration in this study. Effective integration into an Army Force Protection system would require the use of decision aids to manage deployment and utilize these types of sensor resources.

A broad range of individual effective decision tools exist or are under development which support a variety of applications, well beyond just force protection. Many that are applicable to Force Protection can be observed in the box shown in the charts above. It is important to recognize that these are independent decision aids that have significant synergy with each other in many cases. In addition these decision aids have significantly different importance not only to different Force Protection cases, but also to different phases of the same case. This “Box” of decision aids if correctly applied as an integrated set of tools can provide a significant improvement in the decision support to a commander as critical force protection decisions and COAs are developed.

5.2.1 Decision Aids Findings: There is a definite need for an integrated Force Protection Decision Support System (DSS) for the Commander because many individual decision aids exist and are not tied together for user friendly operations during times of crisis. Individual Technologies can provide significant capability to support Commander in all phases of FP (defend, preempt, deceive, etc.). A Decision Support System (DSS) that integrates individual aids that will support commanders, at all levels, to determine the best FP courses of action does not exist (design-ops). In addition, this development is software intensive and will require a “center of excellence” to maintain, evolve and insert to aids. The rationale for the development of this Integrated DSS is that:

DSS will be the key enabler for a Force Protection system

5.2.2 Decision Aids Conclusions: There are two basic conclusions from this sub-panel. The first is that there is a need for the development of an FP integrated data bases for creating a common operating picture (COP). This would include facilities, FP packages, estimated weapons effects, threat characteristics, current threat assessments and real-time intel. The second conclusion is that the set of algorithms for FP assessments need to be adaptable for changing COP. This would especially be true for mobile as well as fixed facilities, complex environments such as weather or terrain, key intelligence analysis and collection management activities, and for current operations analysis and assessment tools (including survivability and lethality analyses, likelihood of threat attack/locations ad type, and probabilities traded against consequences). This set of Decision Aid tools would definitely support all command levels (squad to corps).

5.2.3 Decision Aids Recommendations: The commander’s decision cycle needs to be supported by FP Decision Aids throughout the FP process, starting with planning and ending with mission accomplishment. This process can repeat and extend for days, weeks, months or years. The Pre-Attack, Trans-Attack and Post-Attack phases can all be supported by decision aids. **A recommendation is that technological leverage for the**

near and far term should be focused as an integrated and tailored Force Protection System centered about a Commander's Decision Support System (DSS).

5.3 Sensors

Sensor systems are comprised of an environment sampling component, a material that interacts with substances or conditions in the environment that are of interest, an opto-electronic transduction component, a data fusion component and an archival data set to recognize significant changes in the steady state environment. The data acquired by the sensor must be presented in a coherent manner to the customer, usually involving iconographic display. For applications involving network-centric systems, such as the FCS, the sensor platform must be autonomous and self-regenerating over extended periods of time. The sensors of interest are those that detect CBRN and high explosives in the form of mines.

Multi-array sensor technologies have become a reality for B agents. These have the capability to detect and identify threat agents as point detectors but not stand-off detectors. The ability to produce agent detectors and identifiers that can regenerate functional surfaces and therefore sustain operation for extended periods of time in an autonomous/robotic mode is yet to be realized. The great advance in biotechnology accompanying the sequence of the human genome in 2002 has yielded extensive knowledge regarding the genome of almost all BW threat agents and has offered some understanding of elements of the human genome that predispose to infection. An emphasis has been placed upon biological agent detectors and identifiers by this study panel because of the absence of such detectors on almost all military platforms as well as on the dismounted soldier.

Standoff detectors for chemical agents are available using spectral analysis in the visible and infra red range. Point detectors utilize gas chromatographic/mass spectroscopic devices. Radiological detectors for portal analysis are available using technology developed in the Second Line of Defense (Sandia). HX can be detected from unsealed sources by analysis of emitted volatiles. Sealed or encased sources cannot be detected today using field ready equipment. The recent events have increased the need to detect sealed and encased high explosives. Some plastic coatings of land mines can be detected by analysis of volatile compounds from the casing. Radar and infrared systems can be used to detect vehicles and persons. This study looked at a multitude of sensor systems, as shown by Table 5.

Table 5, Multitude of Sensor Systems

Biological agents(100 agents, MCTL)	Vehicles (tanks, APC, cars, ambulances)
Chemical agents (60 agents)	Perimeter breach
Industrial chemicals	Booby traps, mines, and UHX and HE storage
Radiological/Nuclear materials (threats, hospital sources, facilities, civil source)	Aircraft [including unmanned aerial vehicles (UAV), civilian]
HX (unexploded ordnance)	Mortars, RPGs, MANPADS
Dismounted threats (snipers, IED, troops, non-combatants, friend/foe)	

The PILAR (French), SADS (Israeli), the VIPER (USNRL) and the BBN (US) are all available for detection of snipers after the event (they detect the muzzle flash, the bang of a weapon discharge, or the crack of a high velocity round passing the sensor array). Perimeter surveillance consists of visual, IR, seismic and acoustic detection. GPR and seismic approaches have utilities for underground surveillance. GPR can be used to scan large surface areas but moisture in the soil reduces effectiveness. Seismic analysis can be used to scan underground cavities but the acoustic detectors must be spaced at intervals of approximately 30 meters limiting the area that can be scanned. Radar can be used to detect patterned mine arrays. Individual mines or IED are not readily detected by current technology. IED's that emit volatiles can be detected by stand off technologies. Sealed or encased HX is not readily detected by field ready devices. Emerging radar based technologies can be used to screen persons for concealed HX by changes in morphology of the person.

5.3.1 Sensor Findings: The Army already has relatively large, bulky pieces of equipment that detect and identify B and C agents. The equipment works but is not easily portable and falls short of meeting all of the soldier's needs. The Army's capabilities also include: (a) An abundance of individual CBNRE detecting and identifying elements but these are not multiplexed or integrated, and (b) Detection and identification of nuclear sources. The Army has extensive existing and under development Radar, IR, EO and microwave detection of persons and ground platforms from a distance – these developments are essential to Force Protection needs and are complimented by a broad range of COTS. Investments in smaller, lighter, less expensive sensors are essential to the Force Protection needs. The Army has a development program with IR, microwave and broadband detection of both high- and low-velocity projectiles which can provide significant future FP capabilities with defense and retaliation options. However, these systems are stovepiped and not integrated; once again, our main theme of the study.

5.3.2 Sensor Conclusions: There are several unmet needs:

There are two Army Critical Unmet Needs. They are: (1) A portable, energy-efficient system to detect and identify B agents. [The development of a small, lightweight, power efficient biological sensor that is based on currently available technology is estimated to cost approximately 60-100 million dollars. The funding will

support development of an optical based or a redox system.], and, (2) Field capable sensors for detecting high explosives encased or sealed (solution set not defined).

There are also five important Army Unmet Needs that need to be funded. They are (1) Detection and location of direct and NLOS fire (e.g. Sniper detection), (2) Perimeter and area surveillance (e.g. Beyond the fence line, (3) Below the fence line, and/or Video activity monitoring), (4) Mines and IED detection, Detection of Surveillance of Army facilities and units (counter Surveillance), and (5) Positive ID of individuals.

5.3.3 Sensor Recommendations: Emphasis during the study was placed upon biological agent detectors and identifiers because such detectors are absent from most military platforms as well as on the dismounted soldier. Stand-off detectors for chemical agents are available using spectral analysis in the visible and infra red range. Point detectors utilize gas chromatographic and mass spectroscopic devices. Radiological detectors for portal analysis are available using technology developed in the Second Line of Defense (Sandia). Recent events have increased the need to detect sealed and encased high explosives. HX, high explosive, can be detected from unsealed sources by analysis of emitted volatiles. Radar and infra red systems can be used to detect vehicles and persons. **A major recommendation is that this variety of sensors be refined, developed and deployed in a more consistent manner within a Network Centric Integrated FP System.**

5.4 Automation and Robotics

The panel visited and reviewed multiple Army and DARPA programs connected with automated ground and air vehicles, including the ARL Demo III, Collaborative Alliance on Robotics Technology, and the Robotic Follower programs. We also reviewed real-time video processing technologies being developed as an offshoot of the robotics video work to analyze video streams to extract activity information.

5.4.1 Automation and Robotics Findings: The robotics research community has been making steady progress in the key technologies for unmanned systems, in particular, perception, control systems, mobility platforms, and sensor payloads. Despite this progress, inserting robotics, especially semiautonomous robots, into the force has been challenging because of the high level of complexity of the combat environments in which the Army operates. However, Force Protection presents environments which are more controlled, and therefore likely to be amenable to robotic deployment. We recommend that the Army should consider exploiting this opportunity to deploy the current generation of autonomous and semiautonomous robots in order to gain sufficient realistic operational experience. The robotics research community has also developed perception technology that exploits real-time computer processing of video streams to automatically determine patterns of human activity. This technology is being furthered by DARPA in a new program called “Combat Zones that See.” We believe that this technology has the potential to significantly reduce soldier workload, especially in monitoring large urban areas.

Some technologies being developed that should be closely tracked by the Army Force Protection community are:

1. Unmanned vehicles (ground and air), including platforms for
 - a. Carrying sensor packages
 - b. Fixed site protection
 - c. Routine patrol of secured areas
2. Automatic visual sensor processing for
 - a. Improved surveillance without overload
 - b. Sensor net to cover urban areas
 - c. Connectivity into existing civilian camera systems
3. DARPA/ARL research in video surveillance technology mature enough to transition to the FP community
 - a. Significant progress in: Object tracking, Video motion detection, Multi camera coordination, Activity understanding and monitoring
4. No fully integrated testbed exists where technologies can be evaluated in a systems context, and leaders trained in their use
 - a. All three services have identified the need for integrated testbeds.
 - b. Needs to broaden scope to include: Architectures, CONOPS and TTPs, Training on users and commanders in the use of the technologies, and Inter-service commonality and reuse of knowledge/tools/etc.

5.4.2 Automation and Robotics Conclusions: Our findings support our conclusions that the robotics technology is maturing rapidly, and in fact, is capable of insertion into the field in many restricted environments. For example, the MDARS (E) program for the development of a perimeter patrol robot, could be deployed now. Investments being made by DARPA on furthering the video processing technology through the Combat Zones that See program, have significant benefits in the Force Protection realm, and should be rapidly matured and accelerated into the field through Army investments in ATDs and supported through ACTDs. Another conclusion was that the lack of a suitable integrated testbed where FP technologies could be integrated and evaluated in a systems context is hampering the conceptualization and deployment of semi-autonomous and autonomous robotics and vision technology into the field. All three services have indicated a desire to have testbeds where FP technologies could be evaluated in controlled environments. However, these testbed concepts need to be expanded to include the development of suitable architectures, CONOPS, and integrated tactics. Without such a broad testbed, the appropriate utility of the FP technologies will not be realized.

The Army is not investing sufficient resources in the development of technologies for manned and unmanned systems to operate as a coherent system. Maximizing the

effectiveness of the small number of troops in long-term, high alert postures (the most stressing environment for FP), requires a tightly interconnected system of humans and air and ground robots operating together. A key aspect of such manned unmanned teams is the Human Robot Interface issues. The ASB has found in prior studies (Summer Study 1999, Special Study on Human Robot Interface Issues 2002) that unless this critical issue is addressed, the introduction of robotics into the force will be challenging. Further, there is insufficient experimentation with integrated air and ground robotics teams to adequately develop technologies that will provide sufficiently responsive surveillance coverage around our forces. Such responsive coverage, especially well before any incident occurs, is critical to our ability to deter or deny our opponents the ability to attack our forces.

Programs such as the MDARS (E) being developed by the PM for Physical Security (PM-PSE) are transitioning Army technology for semiautonomous ground robotics into materiel solutions. However, we believe that in today's environment, such programs need to be expanded and the technology deployed on a timescale much faster than that currently envisaged by the MDARS program.

In the discussion of robotics (especially autonomous robots) it is useful to have a set of working definitions of various levels of autonomy. While fully autonomous (goal directed, unsupervised) robotic operations in unconstrained terrain, is still many years away, the panel believes that supervised autonomy (also called semi autonomous operations) at levels 5 or 6, can be reached within five years. This is particularly true in constrained or semi-constrained environments such as convoy operations on hard surface roads, perimeter protection in CONUS or OCONUS prepared bases, etc.

Unmanned vehicles both ground and air represent ideal carriers for sensor packages for use in detection of adversaries in force protection efforts. Application of these technologies will not only reduce manpower requirements but also reduce the requirements to place soldiers in harms way. For fixed site applications unmanned ground platforms and sensors packages are available. The Army should increase investments in this area to accelerate development of both sensors and platforms

Vision systems capable of sensing and automatically processing video imagery to determine patterns of activity are being developed by several groups, including ARL and DARPA. These technologies can have significant impacts in reducing the manpower required to observe and monitor large areas, especially in crowded urban environments. Some of these systems are ready for transition. The Army should make significant investments in the further development and maturation of this technology and deploy systems that embody this technology as rapidly as possible.

Though many individual FP systems exist there is no system of systems architecture for achieving comprehensive structured site protection. In addition, no methodology currently exists for getting to this state, i.e., few interface standards to ensure all allow plug and play for various systems offering different capabilities. No

suitable integrated testbed has been established where FP technologies can be integrated and evaluated in a systems context.

5.4.3 Automation and Robotics Recommendations: The subpanel recommends that the Army should create a new ATD and support joint ACTDs aimed at combining UAVs and UGVs with soldier teams; and accelerate transition of video analysis technology from DARPA into Army applications. The panel believes that one valuable robotics ACTD would be to couple the MDARS(E) platform with small UAVs emerging from R&D programs within the Army or others in the S&T community (e.g., ONR). A critical set of demonstrations would include having a dismount squad patrol an area, with the UGV on point in the front, and the UAV flying an automatically generated pattern overhead. The ACTD would demonstrate the autonomy of this team to use surveillance data from either the UGV or the UAV to have the squad dynamically change its patrol route, and have the autonomous systems track these changes in real time. Successful demonstration of this technology would have immediate application to fixed and hasty CONUS and OCONUS site perimeter protection.

The panel also believes that the video image interpretation technology for human activity monitoring is mature enough for rapid experimentation and insertion into use. Based on our assessment of the maturity of the technology, we expect DARPA to have realistically useful technology within a year (by 2004). The subpanel recommends that the Army should create a technology group (at ARL or at one of the RDECs) ready to accept the technology and transition it into 6.3 demonstrations. Unless this is done in parallel with the DARPA funded S&T programs, the technology will not transition and have the requisite impact on Army needs.

5.5 Weapons and Survivability

This section of the panel had two areas of concern at the beginning of the tasking; lethal and non-lethal weapons with the associated survivability. While studying those issues, a surprising technology surfaced. This old mission – illumination—could almost be called a “breakout” technology because of its new capabilities (low cost, low power, high illumination, long life). Therefore, this section deals with Illumination, Weapons and Survivability, and non-Lethal issues.

5.5.1 Illumination Control Summary: Friendly control of illumination is a basic enabling factor in all or nearly all Force Protection defense constructs. Control is exerted before, during, and post-attack. Broad area low intensity illumination can minimize potential night-time threat advantages. Medium intensity lighting can be focused, in conjunction with other sensors on likely concealment areas. High intensity narrow area illumination potentially can disrupt operations. Factors affecting the illumination control plan include: Topography, Threat intel, Weather, Illuminator platforms available, Sensors available, Weapons available, and Defense plans.

Enabling Illumination Technologies: Light Emitting Diodes(LED’) are being used commercially in both interior and exterior lighting applications. The industry is already

are more than a billion dollar business annually. In particular the gallium nitride LED, invented in Japan about seven years ago, provides white, or other color light, with amazing efficiency. Devices currently providing 25 lumens per watt are predicted to improve to 50 l/w by 2005 and 150 l/w by 2012. In addition the wattage per device should double by 2005. The devices in the near future will be 10 times as efficient as incandescent lamps and last 100 times as long. (IEEE SPECTRUM Sept, 2002). For arrays of LED's, both the intensity and the color emitted can be dialed instantaneously. Any "gas and glass" device will be less efficient and less durable or long-lasting. Avoiding predictability of defense posture and reaction is important. Daily variation in defensive procedures and deployment of assets would impact the attack planning. Rising the ambient light level over the whole, or selected portions of, the threat keep out area compound the problems of the attacker in reaching this desired threat operations point undetected Low light level visual sensors complement radar and other sensors. A capability to instantaneously spot-light or flash light up smaller areas would be very useful both in disrupting the threat and /or confirming and identifying the threat.

Table 6, Illumination Levels

Darkness	<.05 lumens/ft ²
Bright Moonlight	.25 lumens/ft ²
Cloudy Day	1000 lumens/ft ²
Bright Sunlight	10,000 lumens/ft ²
Range of Variation	10 ⁵ – 10 ⁶

5.5.2 Findings for Illumination Control: The usage of the new LED technology for the Army can be a "Breakout" opportunity because of its many uses at a very low cost, as the commercial world is exploding in this arena. The uses include: Dynamics usage – Dependent on threat, weather, tactics, and level of hostilities, Extends utilization of all visual sensors including human and UAV's, Detect penetration of restricted areas/complements other sensors, Disrupt threat operation, Aids perimeter surveillance, and Reflection from clouds option. In addition, because of its mobility, elevated high intensity light sources can be applied for wide-area or selected zone illumination. The major features of this new LED technology include: High efficiency light weight LED light source (e.g., gallium nitride), Tunable (color, intensity), Flash or continuous, and Fixed wing (FW) or lighter than air (LTA) unmanned.

5.5.3 Weapons and Survivability Summary: The following section is organized by threat category and protection measures. We include information relative to identifying the technology capabilities and gaps in current and planned program

There is a strong analogy between force protection for land forces and the anti-submarine warfare of the past century, and indeed continues today. The threat, in both cases, is difficult to detect or track. Fixed bases and supply lines are primary targets. Both platform mounted active and passive sensors and distributed small sensors [sonobuoys] have been the tools of the trade, Midget submarines, suicide missions, were

predecessors to special forces. Well guarded convoys may be needed for land supply lines as for shipping lanes. Special hunter-killer groups of war-ships {search and destroy} plus air cover turned the tide in WWII. Torpedoes are stand-off weapons like mortars. The past submarine threat was asymmetric as is the special operation or terrorist threats to land based forces. That is, the cost of protection may be an order of magnitude greater than the threat cost but still significantly smaller than the value [human or material] of the protected assets. As for a war-ship force protection of any Army unit must be inherent in the equipment and training of the crews. Major fixed bases, whether Army bases airfields, depots, or other tend to have assets spread over large areas. Also they are vulnerable to attack by indirect fire originating in even larger potential areas. The combination of these two factors plus the short flight time attacking weapon makes active area probably impractical.

The likely indirect fire weapon is the mortar. A representative older design is the French Hotchkiss-Brandt 120 mm design. This mortar weighs slightly less than 100kg and can be carried by a three-man team. Each round weighs 14 kg and 8-15 rounds per minute can be fired. Presumably the rounds could be terminally guided using GPS or a forward observer equipped with a laser designator. Active point defense of high value targets is probably doable. The mortar round can be tracked by radar and its ballistic trajectory computed. It is a threat to a high value target a short-range missile or can be fired to detonate either by proximity fuse or at a predicted time and place, deflecting the mortar round's trajectory more than the guidance can correct. Typical high value targets are troop concentrations, such as, barracks, mess halls, parked aircraft, ships in port. Active defenses should be mobile so that their locations vary with the presence of people or assets. To be effective counter-battery fire may need to be direct fire from an UAV or UGV. Depending on the rules of engagement the response may be lethal or less-than-lethal. Convoys could be attacked on the move or at a stop if the time of a stop is known and reported by the threat in real time.

Whether protecting a fixed base or convoy, the key elements are vulnerability reduction, prevention, and quick reaction. Defense's problems are magnified by possible wide variations in threat level, weapons, objectives and tactics. Effective perimeter surveillance and prevention of entry are key factors for fixed bases. Earlier studies [ASB 2001] calculated that deployment of armed UGV's reduced losses significantly. The detection and neutralization of side attack and buried mines is a of the highest priority. Applications of ground penetrating radars are being explored both in the USA and in Europe. Both Ford and BMW are offering four wheel drive vehicles with ballistic protection and other features. In addition, specialty firms customize other vehicles, such as the commercial HUMMER or Suburban. Such ballistic protection combines synergistically with reduced soldier loads, and lightweight body armor and weapons. The threat from small aircraft does not seem to be fully considered relative to resulting consequences. Small aircraft (manned or unmanned) may come as a suicide bomber or a crop duster spraying C/B. For car or truck bombs, access control, standoff and passive protection are the primary defense for installations. Standoff detection is the most important technology development area for preventing or preempting suicide bombers. The potential suicide bomber needs to be identified as a potential threat by a standoff

detection device and isolated from other individuals entering a location. The isolation facilitates needs to contain the blasts from 100 pounds of high explosives.

Simulations have shown that armed UAVs have significant potential for defending convoys in rural and urban areas. Point active defense systems will easier to develop than wide area active defense systems. Currently the Army is developing solid-state high temperature lasers for interception of incoming munitions. S&T is underway to develop a hit avoidance capability for regional protection.

5.5.4 Findings and Conclusions: To prioritize our Force Protection capabilities in the five major countermeasures categories, we graded the potential for significant improvement in three levels (1, 2, 3). From the Delphic process prediction, prevention and presumption counter measures were judged to have the highest potential pay off. Previous studies (DSB) arrived at similar conclusions.

Table 7, Technology Payoff

<i>Threats</i>	<i>Vulnerability Reduction</i>	<i>Prediction Prevention Preemption</i>	<i>Active Defense</i>	<i>Damage Control</i>	<i>Response (counter fire, etc.)</i>
<i>Indirect Fire</i>	2	1	2	3	2
<i>Direct Fire</i>	2	1	3	3	2
<i>Vehicle Delivery</i>	2	1	2	3	3
<i>Suicide Bomber</i>	2	1	3	3	3

1. Highest potential payoff 2. Useful potential payoff 3. Unlikely payoff

Building on the needs prioritization analysis, we identified the necessary technology based capabilities to satisfy these needs, as shown in Table 8, Technological Capabilities.

Table 8, Technological Capabilities

	Highest Potential	Useful Potential
Indirect Fire	Multiple sensor integration Illumination control Armed UAV's	Bomb shelter Personnel areas ballistic protection Preventive point defense Counter fire
Direct Fire	Non-lethal Weapons Mine detection and neutralization Illumination control Armed UAV's	Commercial armored vehicles Personnel areas hardening
Vehicle	Remote explosive detection and neutralization	Inspection areas Air defense
Suicide Bomber	Stand off explosive detection and neutralization Human behavior screening	Isolation area for suspects

5.5.6 Non-Lethal Weapons Summary: The non-lethal weapons area is one of potential payoff to the DoD. There are many organizations working this area; however, a concerted legal and operational environment must be better understood to leverage these tools.

DoD NLW Definition Weapons that are explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesirable damage to property and the environment.

The core capabilities for Non-lethal weapons are: Counter personnel (deny access, clear facilities, crowd control, and incapacitate), and Counter material (aerial denial-air, land, sea, and disable/neutralize equipment and facilities).

Non-Lethal Recommendations:

1. The Army should define its capability needs and operational plans for the use of non-lethal weapons.
2. The Army should identify the policies, legal, or treaty restrictions and make the necessary changes to ensure that non-lethal weapons can be effectively used.
3. The Army should establish it own requirements for Non-lethal Weapons.

5.6 Technology Panel Basic Recommendation: When the study group gathered in Newport Beach to assess the results of the study, it was soon recognized there was an immediate need for a systems approach to the problem of Force Protection. The parts are

available; however, the integration of the parts in a network centric manner is missing. The basic recommendation is:

**Current (COTS/GOTS) and future technologies should
be leveraged as a Network Centric Integrated System to
help our soldiers
in the Force Protection arena**

Appendix I

Member Affiliation

The panel consisted of Army Science Board members and consultants while being ably assisted by many government advisors. In addition, during the two week summer study, there were two cadets who assisted in the development of the report. The table shows the names of the members of the Technology Solutions Panel while the next section gives organizational details.

Table 9 - Technology Solutions Panel Members

Panel Chairs	ASB Members/Consultants	Government Advisors
Dr. Peter Swan	Mr. Gary Glaser	Dr. Reed Mosher
Dr. Edward Brady	Dr. Mark Hofmann	Mr. Paul Tilson
	Dr. Donald Kelly	Mr. Mike Toscano
	Dr. Ira Kohlberg	Dr. Jack Wade
	Dr. Steven Kornguth	Mr. James Wisniewski
	Ms. Ginger Lew	Mr. Randy Woodson
	Dr. Richard Montgomery	CDT Heather Ritchey
	Dr. Prasanna Mulgaonkar	CDT Adam Tritsch
	Mr. John Reese	

Co-Chairs

Dr. Edward C. Brady
Strategic Perspectives, Inc.
1488 Evans Farm Drive
McLean VA 22101-

Dr. Peter A. Swan
Vice President and Chief Engineer
SouthWest Analytic Network, Inc.
5865 East Sanna Street
Paradise Valley, Az 85253

Panel Members

Mr. Gary Glaser
Independent Consultant
11609 Twining Lane
Potomac, MD 20854-

Dr. Mark A. Hofmann
President, Colmar-L.L.C.
3200 Summit Court
Newburgh, IN 47630-8422

Dr. Don Kelly
AdvanTECH Partners
5316 Anaconda Lane
Austin, Texas 78730

Dr. Ira Kohlberg
Science and Technology Division
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

Dr. Steven E. Kornguth
Director, IAT Chemical Defense and Biological
Defense
Professor of Neurobiology
Institute for Advanced Technology
University of Texas at Austin
3925 W. Braker Lane
Suite 400
Austin, TX 78759-5329

Ms. Ginger E. Lew
CEO and Managing Director
Telecommunications Development Fund
2020 K. St. NW, Suite 375
Washington, DC 20006-1806

Dr. Richard Montgomery
1398 Avenida Da Cortez
Pacific Palisades, CA 90272-

Dr. Reed L. Mosher
Technical Director for Survivability and
Protective Structures
Geotechnical and Structures Laboratory
US Army Engineer Research and Development Center
3909 Halls Ferry Road
Vicksburg, MS 39180-6199

Dr. Prasanna Mulgaonkar
Research Sector Director, Intel Research
Intel Corporation, 2200 Mission College Blvd (MS
RNB6-37)
Santa Clara, Ca 95052

Mr. John H. Reese
13869 Lynde Avenue
Saratoga, CA 95070-5310

Mr. Paul E. Tilson, Jr.
National Reconnaissance Office
WF-1, AS&T/CTG, 14A00J
14675 Lee Road
Chantilly, VA 20151-1715

Dr. Jack Wade
Director, Army Research Lab
White Sands Missile Range, NM 88002

Mr. James Wisniewski
Science Advisor to the Director for Research &
Laboratory Management
US Army (SAAL-TR)
2511 Jefferson Davis Hwy
Arlington, VA 22202

Mr. Randy Woodson
Senior Program Manager / Dep Division Chief
US Army Research Laboratory
Computational & Info Sciences Dir
2800 Powder Mill Road
AMSRL-CI
Bldg. 205
Adelphi, Md. 20783-5424

Mike Toscano
Staff Specialist for OUSD(AT&L),
Pentagon, Room 3D1063,
Washington, DC 20301

CDT Heather Ritchey
U.S. Military Academy

CDT Adam Tritsch
University of Kansas

Appendix II
Technology Solutions Panel Briefing




Force Protection Study

Army Science Board

Summer 2003

Technology Solutions Panel

Force Protection Study

1




Technology Solutions Panel

Challenge:

- Assess and recommend current and future technologies for Army Force Protection

Basic recommendation:

- Current (COTS/GOTS) and future technologies should be leveraged as an integrated system to help our soldiers in the Force Protection arena

Force Protection Study

2




Technology Solutions Panel

Co- Chairs

Dr. Edward Brady Dr. Peter Swan

ASB Members & Consultants Government Advisors

Mr. Gary Glaser	Dr. Reed Mosher
Dr. Mark Hofmann	Mr. Mike Toscano
Dr. Donald Kelly	Dr. Jack Wade
Dr. Ira Kohlberg	Mr. James Wisniewski
Dr. Steven Kornguth	Mr. Randy Woodson
Ms. Ginger Lew	CDT Heather Ritchey
Dr. Richard Montgomery	CDT Adam Tritsch
Dr. Prasanna Mulgaonkar	
Mr. John Reese	
Mr. Paul Tilson	

Force Protection Study

3




Technology Solutions Outline

- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

4




Technology Panel Site Visits (partial list)

• CECOM	• PEO IEW&S
• ARL	• INSCOM
• PEO / PM-PSE	• Quantico
• JPO	• USAF / BDSS
• JCS J-3	• TWSG
• ERDC	• USA NVL
• ARKL	• Sandia
• JCS JAT	• DTRA
• Information Operations Center	• USAF TAS
• DARPA	• ICT
• JPCEOCBD	• ECBC

Force Protection Study

5




Force Protection Demo (6 May – Quantico)

- Force Protection Demo
 - Approximately 400 exhibits of hardware
 - Significant International Content
 - Components – not systems
 - Small Businesses (shoestrings)
 - Particular Interest (night vision 360 degrees, Area lightening, commercial armored vehicles)
 - Non-lethal most interest
 - Navy xray back scatter for containers, excellent program
- Conclusions
 - Supports need for systems approach
 - Wealth of proven technologies
 - Need better balance between attention on resources for tactical combat and force protection
 - Lack of data exploitation and sensor fusion technology

Many components – No system!

*GOTS – GOTS – GOTS – GOTS
A Plethora of parts!*

Two lessons learned

Force Protection Study

6




Technology Solutions Outline

- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

7




Principal Themes

- Integrated Systems Concept – network centric, standards based, self healing, graceful degradation, plug-and-play
- Some requirements/issues are specific to “force protection”
- Overlap with current Army programs allows leverage of equipment, funding, and processes
- Need to consider techniques to deal with extremely low probability events over extremely long time periods

System of Systems reflects a rigorous engineering approach resulting in a balanced system with an architecture that integrates all elements of force protection (e.g. weapons, sensors, decision aids, automation/robotics, networks and survivability).

Force Protection Study

8



Technology Investment (1)



- Technological leverage for the near and far term should be focused as an integrated and tailored Force Protection System centered about a Commander's Decision Support System (DSS)
 - CSA set a vision of FP as an Integrated Systems
 - CSA assign a Force Protection Architect
 - G3 to develop an FP Organizational Focus
 - RDECOM Sponsor an integrated network centric FP ATD
 - RDECOM Develop an Integrated Force Protection Decision Support System

Force Protection Study

9



Technology Investment (2)



Future Technology investments, augmentation of GOTS and COTS, should include:

Decision Aids Technology

- Tools for Intelligence Preparation of Areas of Interest (Staging Areas, Convoy Routes)
- Commander's Force Protection Decision Support System

Unmanned Vehicle Technology

- Joint UAV/UGV Collaborative Surveillance Capabilities
- Semi-Automated robotic followers for convoy operations

Sensor Technology

- Small, Light Weight, Low Power Biological Agent Detection
- Remote Detection of Encased/Sealed Explosives (Countermine, VIEDs, IEDs)
- Video, Visual/IR, Lidar and Radar Continual Surveillance
- Sub-terrain Sensor (Acoustic/Seismic Monitoring)
- Dynamic Large Area Illumination Control

Weapons and Survivability

- Non-lethal Weapons
- Reliable mine / IED detection on the move

Force Protection Study

10



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

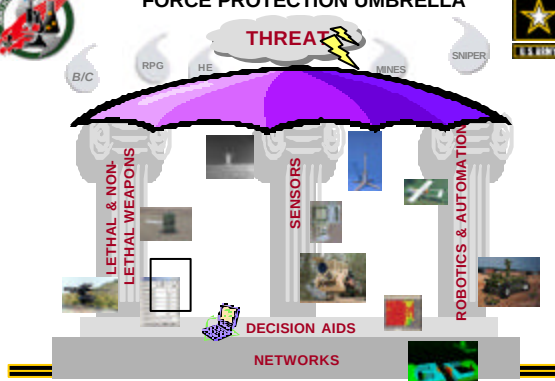
Force Protection Study

11



FORCE PROTECTION UMBRELLA





Force Protection Study

12



Elements of a Sensor System



- Environment sampler
- Agent binding
- Opto-electronic transduction (buried fiber cable, laser designator)
- Data fusion
- Archival data set to recognize significant changes in the steady state environment
- Iconographic display for alerting military decision makers to a threat state.

Force Protection Study

13



Sensor Systems



- Sensor systems to detect:
 - Biological agents(100 agents, MCTL)
 - Chemical agents (60 agents)
 - Industrial chemicals
 - Radiological/Nuclear materials (threats, hospital sources, facilities, civil source)
 - HX (unexploded ordnance)
 - Dismounted threats (snipers, IED, troops, non-combatants, friend/foe)
 - Vehicles (tanks, APC, cars, ambulances)
 - Aircraft [including unmanned aerial vehicles (UAV), civilian]
 - Booby traps, mines, and UHX and HE storage
 - Perimeter breach
 - Mortars, RPGs, MANPADS

Force Protection Study

14



Sensors Findings



- Current Sensor situation
 - The Army already has relatively large, bulky pieces of equipment that detect and identify B and C agents. The equipment works but is not easily portable and falls short of meeting all of the soldier's needs. The Army's capabilities also include:
 - An abundance of individual CBNRE detecting and identifying elements but these are not multiplexed or integrated
 - Detection and identification of nuclear sources
 - The Army has extensive existing and under development Radar, IR, EO and microwave detection of persons and ground platforms from a distance – these developments are essential to Force Protection needs and are complemented by a broad range of COTS. Smaller, lighter, less expensive sensors are essential to the Force Protection needs
 - The Army has a development program with IR, microwave and broad band detection of both high- and low-velocity projectiles which can provide significant future FP capabilities with defense and retaliation options. Smaller, lighter, less expensive sensors are essential to the Force Protection needs
 - These systems are stovepiped and not integrated

Force Protection Study

15



Sensors Conclusions



Army Critical Unmet Needs

- A portable, energy-efficient system to detect and identify B agents. The development of a small, lightweight, power efficient biological sensor, that is based on currently available technology is estimated to cost approximately 60-100 million dollars. The funding will support development of an optical based or a redox system
- Field capable sensors for detecting high explosives encased or sealed (solution set not defined)

Force Protection Study

16




Other Unmet Sensor Needs

- Detection and location of direct and NLOS fire
 - Sniper detection
- Perimeter and area surveillance
 - Beyond the fence line
 - Below the fence line
 - Video activity monitoring
- Mines and IED detection
- Detection of Surveillance of Army facilities and units (counter Surveillance)
- Positive ID of individuals

These are being developed and/or evaluated by Army and other programs but must be monitored

Force Protection Study

17




Technology Solutions Outline

- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

18




Findings Illuminating Control Concept

- Mobile elevated high intensity light source for wide-area or selected zone illumination
- Features
 - High efficiency light weight LED light source (e.g., gallium nitride)
 - Tunable (color, intensity)
 - Flash or continuous
 - Fixed wing (FW) or lighter than air (LTA) unmanned
- Uses
 - Dynamics usage – Dependent on threat, weather, tactics, and level of hostilities
 - Extends utilization of all visual sensors including human and UAV's
 - Detect penetration of restricted areas/complements other sensors
 - Disrupt threat operation
 - Aids perimeter surveillance
 - Reflection from clouds option

Force Protection Study

19




Findings – Needs Prioritization

Weapons and Survivability

	Protective Measures				
	Vulnerability Reduction	Prediction/Prevention/Preemption	Active Defense	Damage Control	Response (Counter Fire, etc.)
Indirect Fire	2	1	2	3	2
Direct Fire	2	1	3	3	2
Vehicle Delivery	2	1	2	3	3
Suicide Bomber	2	1	3	3	3

1. Highest potential payoff 2. Good potential payoff 3. Unlikely payoff

Force Protection Study

20



Technology Applications Prioritization



	Highest Potential	Useful Potential
Indirect Fire	Multiple sensor integration Illumination control Armed UAV's	Bomb shelter Personnel areas ballistic protection Preventive point defense Counter fire
Direct Fire	Non-lethal Weapons Mine detection and neutralization Illumination control Armed UAV's	Commercial armored vehicles Personnel areas hardening
Vehicle	Remote explosive detection and neutralization	Inspection areas Air defense
Suicide Bomber	Stand off explosive detection and neutralization Human behavior screening	Isolation area for suspects

Force Protection Study

21



Weapons and Survivability Conclusions



- The Army should define its capability needs and operational plans for the use of non-lethal weapons.
- The Army should identify the policies, legal, or treaty restrictions and make the necessary changes to ensure that non-lethal weapons can be effectively used.
- The Army should establish its own requirements for Non-lethal Weapons.
- The Army should invest in future technology for preemption and defense of direct and indirect fire:
 - Dynamic large area illumination
 - More mine detection and neutralization
 - Point defense of ballistic fragment protected troop concentrations
 - Non-lethal weapons and sensors
 - Armed UAV's
- The Army should continue to invest in technology development to reduce vulnerability

Force Protection Study

22



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids



Force Protection Study

23



Automation and Robotics Findings/Conclusions



- Unmanned vehicles (ground and air), including platforms for
 - Carrying sensor packages
 - Fixed site protection
 - Routine patrol of secured areas
- Automatic visual sensor processing for
 - Improved surveillance without overload
 - Sensor net to cover urban areas
 - Connectivity into existing civilian camera systems
- DARPA/ARL research in video surveillance technology mature enough to transition to the FP community
 - Significant progress in: Object tracking, Video motion detection, Multi camera coordination, Activity understanding and monitoring
- No fully integrated testbed exists where technologies can be evaluated in a systems context, and leaders trained in their use
 - All three services have identified the need for integrated testbeds
 - Needs to broaden scope to include: Architectures, CONOPS and TTPs, Training on users and commanders in the use of the technologies, and Interservice

Force Protection Study

24



Automation and Robotics Findings/Conclusions



- Manned/Unmanned teaming
 - Human-Robot interfaces is a continuing issue
 - Minimal combined-UAV-UGV systems being transitioned or operationally experimented with at this time
- Structured (fixed or planned) site protection application appears to be amenable to automation and robotics
 - PM-PSE making significant strides in technology for physical security
- Programs (e.g., MDARS) underway to transition ARL and TARDEC UGV technology into user programs
 - MDARS-E program is on track to move unmanned ground systems into operational use

Force Protection Study

25



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

26



Network Findings



- Most of the network technologies needed for force protection are also needed for combat and non-combat networks
- Low tech solutions, such as adhering to COMSEC practices, are still extremely importance in network force protection
- Inadequate funding to develop the technologies needed by DoD that will not be developed commercially

Force Protection Study

27



Network Conclusion: Must Consider Both Low and High Tech Needs



Low Tech Force Protection Needs

- Each soldier trained to certain level on IT basics
- Physical security of all components of network
- COMSEC procedures
- Contractor and In-Country support

Higher Tech Network Force Protection Needs

- Quick purge of data
- Over-the-air re-keying
- Remote disable of users and nodes
- Re-routing of traffic to exclude persons or nodes
- Network intrusion detection

Force Protection Study

28



Network Conclusions



- Important Areas That Lack Sufficient Commercial R&D Funding
 - Network intrusion detection
 - COMSEC and multi-level security
 - Protocols and data formats for force protection and information assurance (C2 and SA messages)
 - “Guard” – Transfer info from one level to another, protection from unauthorized access at all levels
 - Interoperability with other and legacy systems, conforming to standards
 - Role-Based Access Control – Tie the network access of each soldier to his/her role rather than visibility
 - Group Key Management – Dynamic, flexible, rapid re-keying in battlefield, secure multicast (no commercial standard)
 - Ad Hoc, Mobile, Self Organizing Networks
 - Small, Easily Erectable Masts; Low Profile OTM Antennas; Smart antennas
 - Spectrum - Restricted Frequency Assignments; Geographically Impacted
 - LPI, LPD, anti-jam communications
- Army should focus development efforts on information processing, data flow, networks and radio to support network centric operations

Force Protection Study

29



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids



Force Protection Study

30



Decision Aids Findings



- A Need for an Integrated Force Protection Decision Support System (DSS) for the Commander
 - Many individual decision aids exist
 - Individual Technologies provide significant capability to support t Commander in all phases of FP (defend, preempt, deceive, etc.)
 - A Decision Support System (DSS) that integrates individual aids that will support commanders, at all levels, to determine the best FP courses of action does not exist (design-ops)
 - This development is software intensive and will require a “center of excellence” to maintain, evolve and insert to aids

DSS is a key enabler for a force protection system

Force Protection Study

31



Decision Aids Conclusion



- Development of FP integrated data bases for common operating picture (COP)
 - Facilities, FP Packages, Weapon Effects
 - Threat characteristics
 - Current threat assessments (wide range in effect, technique and duration)
 - Current Intel
- Allocation algorithms for FP assessments of changing COP
 - Facilities (fixed and mobile)
 - Complex environments (Weather, Terrain, Political,.....)
 - Intelligence analysis and collection management
 - Operations analysis and assessment tools
 - Survivability and lethality options developments
 - Analysis of likely threat attack locations (and ambush possibilities)
 - Probabilities vs. consequences (low probability, long time frames, devastating effects)
- Supports all command levels (squad to corps)

Force Protection Study

32



Decision Aids Conclusion



- DSS requires Interaction / collaboration with other echelons concerning FP options, threats and courses of action
 - Peer group
 - Down Echelon / Up Echelon
 - Experts and Centers of Excellence
 - Standards and common relevant operating picture
- Development of DSS requires a systems center which continually supports
 - Integration of the best decision aids
 - The system when deployed
 - Mentoring and training

Force Protection Study


33



Decision Aid Roadmap



Develop DA Inventory

- Current
- In Development 6.3+
- Research 6.1, 6.2, 6.3

Develop DSS Architecture

- Consistent with Obj. Force & GIG
- Service based
- Support to all Cmdr. Levels

FP DSS Red Team

Add new DA tools as they are available

IOC FP-DSS
Center of
Excellence

FP ATD for Cmdr/DSS
CONUS Base Ops
OCONUS Base Ops
Convoy Ops LIC
Small Unit Ops

ACTD for Cmdr. DSS
Bloc 1 IOC

IOC Bloc 2

2004
2005
2006
2007

Force Protection Study


34



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study


35



FORCE PROTECTION TECHNOLOGIES BY OPERATIONAL CASE



THREAT

B/C RPG HE MINES SNIPER

FP Cases

CONUS Base
OCONUS Base
Convoy
Small Teams

LETHAL & NON-LETHAL WEAPONS

SENSORS

ROBOTICS & AUTOMATION

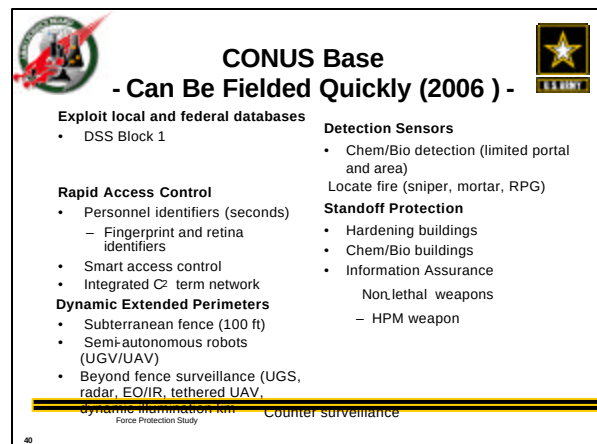
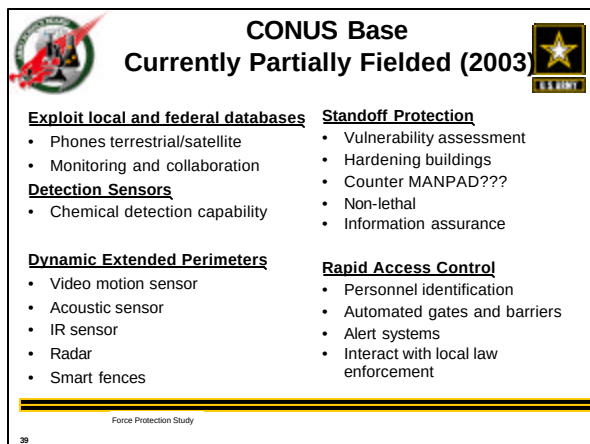
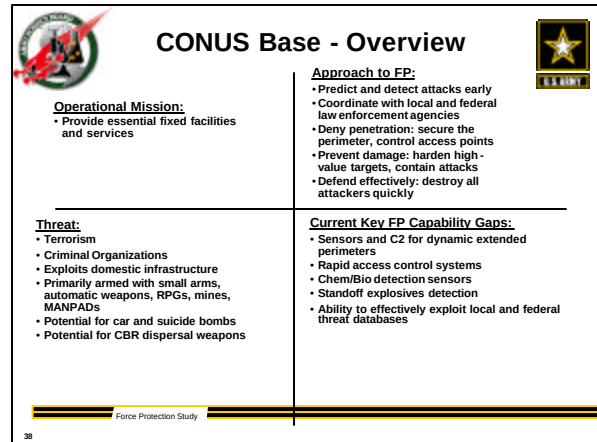
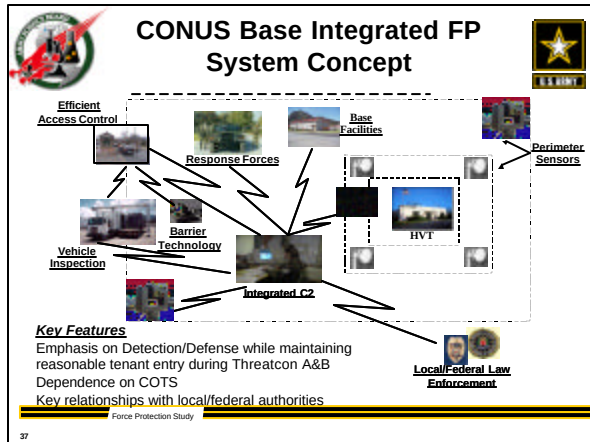
DECISION AIDS

NETWORKS

Force Protection Umbrella

Force Protection Study


36






CONUS Base - Needs S&T (2010) -

Exploit local and federal databases

- Advanced DSS
 - Information Management
 - HUMINT Database
- Threat behavior
- Rapid Translation
- Autonomous UAV/UGV Teams
- Integrated Secure local wireless, SATCOM and wired reach-back

Rapid Access Control

- Network Area Sensors
- Contagious Disease monitoring
- IFF

Dynamic Extended Perimeters

- Tunnel detection (100ft)
- Intelligent Networked Video Sensors for activity monitoring
- UGV/UAV
- UAV/UAV (rehearsed-aerostat)

Detection Sensors

- Food, water, fuel monitoring
- Chem/Bio networked sensors (large area, small sensors, timely)

Standoff Protection

- Buildings (immune)
- Enhanced counter MANPADS
- Portal and Internal CBRNE sensors
- Active Point Defense (Mobile)
 - Sensors (IR and radar)
 - Weapons
- Information Assurance

41

Force Protection Study




Prioritized GapFilling Technologies for CONUS Base

Can be fielded quickly

- Beyond fence enhanced surveillance
 - UAV/OAV/UGV
 - UGS
 - Radar
 - EO/IR
 - Counter Surveillance
 - Decision Support System- Block 1
- Smart access control
- Chem-Bio detection
- Locate Fire
- Sniper Detection
- Non-Lethal Options

Can be fielded by 2010

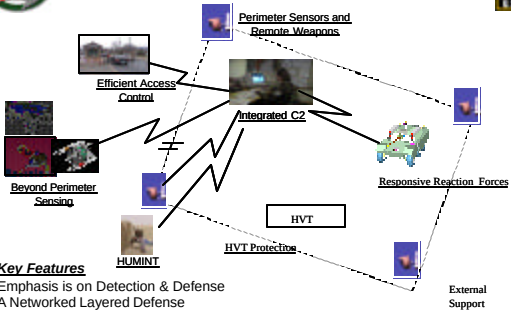
- Enhanced beyond-fence surveillance
- Advanced DSS
 - Threat behavior monitor
- Information assurance
- Enhanced access control
- Portal and Area CBRNE sensors
- Food, water, fuel contaminants and contagious disease monitoring
- Enhanced counter MANPADS capability

42

Force Protection Study




OCONUS Base: Integrated FP System Concept



Key Features

- Emphasis is on Detection & Defense
- A Networked Layered Defense
- High Degree of Autonomy with Personnel in the Loop

43

Force Protection Study




OCONUS Base - Overview -

Operational Mission:

- Provide and protect essential fixed facilities and services for deployed forces
 - Minimize casualties
 - Minimize damage to base

Approach:

- Predict
 - Establish baseline
 - Monitor changes
- Secure the perimeter
- Control access

Threat:

- Modern conventional forces and guerrilla/terrorist elements
- Primarily armed with small arms, machine guns, RPGs, mines, mortars, light artillery, MANPADs
- High potential for suicide bombers
- Potential for CBR dispersal weapons

Current Key FP Capability Gaps:

- Intel to monitor local environment trends and forecast attack
- Rapid access control measures (Seconds)
- Dynamic perimeters (Distance, Area)
- Contaminant detection (Portal and Interior)
- Ability to protect facilities and personnel
- Rapid detection and retaliation (Seconds)

44

Force Protection Study



OCONUS Base

Currently Partially Fielded (2003)



<u>Intelligence</u> • Phones terrestrial/satellite • Monitoring and collaboration <u>Access Control</u> • Personnel identification • Automated gates and barriers <u>Perimeters</u> • Video motion sensor • Acoustic sensor • IR sensor • Radar • Smart fences	<u>Contaminants</u> • Chemical detection capability <u>Protection</u> • Vulnerability assessment • Hardening buildings • Cyber security/Network assurance • Counter MANPAD ??? <u>Response and Retaliation</u> • Response forces • Alert system • Non-lethal • Automated targeting MG

Force Protection Study
45



OCONUS Base

- Can Be Fielded Quickly (2006) -



<u>Intelligence</u> • DSS Block 1 • Counter surveillance • JTRS <u>Access Control</u> • Personnel identifiers (seconds) – Fingerprint and retina identifiers • Smart access control • Integrated C² term network <u>Perimeters</u> • Subterranean fence (100 ft) • Semi-autonomous robots (UGV/UAV) • Beyond fence surveillance (UGS, radar, EO/IR, tethered UAV, dynamic illumination km)	<u>Contaminants</u> • Chem/Bio detection (limited portal and area) <u>Protection</u> • Hardening buildings • Chem/Bio buildings • IA <u>Response and Retaliation</u> • Non-lethal weapons – HPM weapon • Counter fire (sniper, motor, RPG)

Force Protection Study
46



OCONUS Base

- Needs S&T (2010) -



<u>Intelligence</u> • Advanced DSS – Information Management – HUMINT Database • Threat behavior • Rapid Translation • Autonomous UAV/UGV Teams • Integrated Secure local wireless, SATCOM and wired reach-back <u>Access Control</u> • Network Area Sensors • Contagious Disease monitoring • IFF • Physiological/ Taggents Based Identifiers <u>Perimeters</u> • Tunnel detection (100ft) • Intelligent Networked Video Sensors for activity monitoring • UGV	<u>Contaminants</u> • Food, water, fuel monitoring • Chem/Bio networked sensors (large area, small sensors, timely) <u>Protection</u> • Buildings (immune) • Enhanced counter MANPADS • Portal and Internal CBRNE sensors • Active Point Defense (Mobile) – Sensors (IR and radar) – Weapons • Network Assurance <u>Response and Retaliation</u> • Combat UAV/UGV

Force Protection Study
47

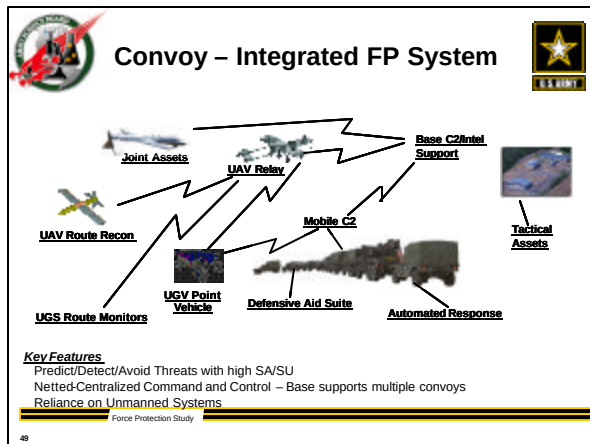


Prioritized Gap-Filling Technologies for OCONUS Base



<u>Can be fielded quickly</u> • Beyond fence enhanced surveillance – UAV/OAV/UGV – UGS – Radar – EOIR – Counter Surveillance – Decision Support System - Block 1 • FBCB2 • Smart access control • Chem-Bio detection • Counter Fire/Sniper Detection • Non-Lethal Options	<u>Can be fielded by 2010</u> • Enhanced beyond-fence surveillance • Advanced DSS – Threat behavior monitor • Network assurance • Enhanced access control • Portal and Area CBRNE sensors • Food, water, fuel contaminants and contagious disease monitoring • Enhanced counter MANPADS capability

Force Protection Study
48



Convoy - Overview

Operational Mission: • Move people & materiel successfully from Point A to Point B by surface vehicle • Minimize casualties • Minimize cargo/vehicle loss	Approach: • Preclude attack • Avoid attack • Counter the attack • Disengage with minimal losses • Accomplish the mission
Threat: • Ranges from small number of individuals (including non-combatants and combatants integrated within non-combatants) to paramilitary and small military forces • Small arms, MGs, RPGs, mines, barriers, mortars	Current Key FP Capability Gaps: • Intel to predict and avoid attacks in a timely manner • Intel to locate and destroy/neutralize direct-fire/ambush attackers pre- and trans-attack • Countermeasures to direct fire/ambush attackers • Continuous assessment of convoy status to execute an attack response • Enhanced vehicle defense

Force Protection Study

Convoy Protection - Partially Fielded (Current) -

Predict and avoid • UAV • Weather • EO/IR/Radar/Acoustic/SIGINT • National products	Continuous assessment • Cell phones/Mobile Netted • NVGs Night Vision Goggles • GPS and Integrated Maps
Intel to locate and neutralize • Limited mine/IED detection • Limited people detection	Vehicle defense • Obscurants • "Run-Flat" tires • Ballistic Protection Appliqué • Non-lethal Capability Set
Countermeasures • Camouflage	

Force Protection Study

Convoy Protection -Can Be Fielded Quickly (2006)-

Predict and avoid • Semi-autonomous UAV/UGV leading the convoy • Surface mine detection – Coherent Change Detection • Chem Detection (all, immediate) • Limited Bio Collection/Detection • Robotic Followers	Countermeasure • Tele-operated Combat UAV
Locate and neutralize • Digital maps • DSS Block 1 • Tele-operated armed lead UGV for hard surface roads • Surveillance detection • Sniper detection	Continuous assessment • JTRS • SATCOM • SLICE (TBD) • UAV relays • Dynamic RF tags
	Vehicle defense • Non-lethal small area denial (e.g., obscurant, sticky foam) • Ballistic appliques

Force Protection Study




Convoy Protection - Needs S&T (2010) -

Predict and avoid

- Advanced DSS
- Use Gint detection/Multi-Spectral for RPG, mortar, sniper detection
- Soldier-portable Chem/Bio detector
- Integrated secure LP/ILPD wireless SATCOM or UAV relay
- Network assurance

Continuous Assessment

- Disposable UGS
- Hovering UAVs
- Decoy UGVs
- Global video coverage
- Micro UAV sampling of volatiles from HE
- Various sensors (EO/IR, Radar)
- National/Joint INTEL
- JLENS relay

Locate and destroy

- UAV/UGV/UGS
 - Sensors
 - Weapons
- Dynamic Illumination (Large Area, Multi-spectral, Intensity)

Vehicle defense

- Ballistic vehicle protection, lethal and non-lethal weapon options

Countermeasures

- Counter fire against small arms and crew-served weapons
- Mine neutralization (buried and SA)
- Obscurants, modular appliqué

Force Protection Study




Prioritized Gap-Filling Technologies for Convoy Protection

Can be fielded quickly

- Provide Blue SA to individual deployed vehicle level
 - Radio and GPS
 - Digital maps
 - Enhanced DSS Block 1
 - Dynamic RF Tags
- UAV proliferation to support convoy operations.
- Ballistic appliqué blankets to hang on vehicle doors, sides, etc.
- Sniper Detection
- Obscurants

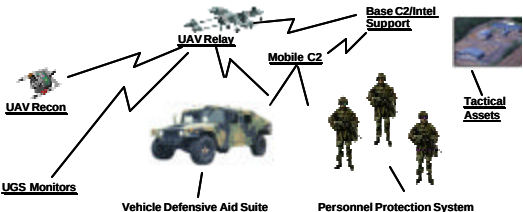
Can be fielded by 2010

- Enhanced surveillance with ubiquitous UAV/UGS/UGV
 - Various EO/IR/radar Sensors
 - Enhanced LED illuminations
 - Bio/Chem sensors, small, power efficient with low false
- Assured communications and Blue SA
- Combat UGV
- Mine detection and neutralization capability on the move
 - Micro UAV sampling of volatiles from HE
- Advanced Decision Support System
- Enhanced Ballistic Vehicle Protection against RPG, Mortar, Sniper;
- Small gas chromatographic/ mass spectroscopy
- Advanced non-lethal options
 - HPM, Laser Dazzler

Force Protection Study




Small Team – Integrated FP System



Key Features

- Predict/Detect/Avoid Threats with high SA/SU
- Netted-Centralized Command and Control – Base supports multiple teams

Force Protection Study




Small Team Operations - Overview -

Operational Mission:

- Conduct necessary activities among the civilian population in the operational environment to build/restore the infrastructure and institutions of the society
- Minimize casualties and collateral damage

Threat:

- Modern conventional forces and guerrilla/terrorist elements
- Criminal organizations
- Primarily armed with small arms, machine guns, RPGs, mines, mortars, light artillery, MANPADs
- High potential for suicide bombers
- Potential for CBR dispersal weapons

Approach:

- Predict
 - Establish baseline
 - Monitor changes
- Integrate in the local community
- Ensure communications
- Accomplish mission

Current Key FP Capability Gaps:

- Intel to establish and monitor local environmental baselines
- Ability to monitor and protect necessary communications
- Combat ID capability in a non-combatant environment
- Ability to secure and protect perimeters
- Individual soldier protection
- Continuous soldier monitoring

Force Protection Study



Small Teams Protection Currently Partially Fielded (2003)



<u>Intelligence</u> GPS Maps & Terrain Model Decision Aids FBCB2 <u>CID</u> Uniform <u>Perimeters</u> NVGs Binoculars	<u>Protection</u> Lethal/Non-Lethal Weapons Body Armor <u>Soldier Monitoring</u> Radio

Force Protection Study

57



Small Teams Protection Could Be Fielded Quickly (2006)



<u>Intelligence</u> PDA class situational awareness device DSS Block I <u>CID</u> Selected vehicle and personnel tags <u>Perimeters</u> Non-Lethal Kit Video for immediate environment	<u>Protection</u> IED Detector Enhanced Body Armor Chemical Detector (small & portable) Armor Appliques Individual Dipsticks (bio detection) <u>Soldier Monitoring</u> Radio cell phone RF Tag (hostage locator) Vehicle locator monitoring system

Force Protection Study

58



Small Teams Protection - Needs S&T (2010) -



<u>Intelligence</u> Portable DSS Surveillance Augmentation MAV Low light visual detection <u>CID</u> • Suicide bomb detectors <u>Perimeters</u> • Non-lethal crowd dispersion • Multi spectral monitoring for immediate environment	<u>Protection</u> Robust Secure Communication • Armored vehicles • Enhanced effective small arms • Locator for small arms fire • Micro Chem/Bio detector HE detector <u>Soldier Monitoring</u> Comprehensive Body Armor • Continuous monitoring – ID tagging – Physiology – Location

Force Protection Study

59



Prioritized Gap-Filling Technologies for Small Team Operations



<i>Can be fielded quickly</i> • Ubiquitous radio/cell phone with GPS for individual soldiers • Enhanced body armor • RF ID tag (hostage location)	<i>Can be fielded by 2010</i> • IED detector – Suicide bomb detector • Non-lethal crowd dispersion • Surveillance Augmentation – MAV – Low light visual detection – Video for immediate environment – Micro B/C detector • Continuous monitoring – ID tagging – Physiology – Location • Locator for small arms fire • Portable DSS

Force Protection Study

60



Summary of Prioritized Gap-Filling Technologies



<i>Can be fielded quickly</i>	<i>Can be fielded by 2010</i>
• Provide Blue SA to individual deployed vehicle level – Radio and GPS – Digital maps – DSS Block 1 – Dynamic RF Tags • Beyond fence enhanced surveillance – UAV/OAV/UGV – UGS – Radar – EO/IR – Surveillance Detection • UAV proliferation to support convoy operations • Ubiquitous radio/cell phone with GPS for individual soldiers • Smart access control	• Enhanced surveillance with ubiquitous UAV/OAV – Various EO/IR Sensors – Enhanced LED illuminations • Bio/Chem sensors, small, power efficient with low false response • IED High Explosive detector – Suicide bomb detector • Assured communications and Blue SA • Mine detection and neutralization capability on the move – Micro UAV sampling of HE • Surveillance Augmentation – MAV – Low light visual detection – Video for immediate environment – Micro B/C detector

Force Protection Study
Advanced BSG

61



Integrated System Findings and Conclusions



- Many are successfully working in various aspects of Force Protection, however no single proponent or system architect for Force Protection could be identified.
- Much of the Force Protection successful S&T does not transition to the field.
- Components that do, are left to the field commander to identify and integrate.

Fielded force protection capabilities are fragmented and often ineffective

Force Protection Study

62



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

63



Panel Recommendations



Total Systems Solution:

- Technology investments
- Army implement FP integrated system
- Identify a Force Protection Architect
- G3 develop an Organizational Focus
- Sponsor an integrated network centric FP ATD
- Develop an Integrated Force Protection Decision Support System

Force Protection Study

64



Technology Investment Recommendations



Future Technology investments, augmentation of GOTS and COTS, should include:

Decision Aids Technology

- Tools for Intelligence Preparation of Areas of Interest (Staging Areas, Convoy Routes)
- Commander's Force Protection Decision Support System

Unmanned Vehicle Technology

- Joint UAV/UGV Collaborative Surveillance Capabilities
- Semi-Automated robotic followers for convoy operations

Sensor Technology

- Small, Light Weight, Low Power Biological Agent Detection
- Remote Detection of Encased/Sealed Explosives (Countermines, VIEDs, IEDs)
- Video, Visual/IR, Lidar and Radar Continual Surveillance
- Sub-terrain Sensor (Acoustic/Seismic Monitoring)
- Dynamic Large Area Illumination Control

Weapons and Survivability

- Non-lethal Weapons
- Reliable mine / IED detection on the move

Force Protection Study

65



Integrated Systems Recommendations



- CSA create vision of Force Protection as an integrated system (Force Protection Umbrella), which has:
 - Network Centric baseline that includes
 - Plug-and-play alternatives tailored to commander's needs
 - Extensive use of COTS and GOTS
 - System Architecture & Standards
 - Decision Support System developed for Commander's view
 - Force protection organization
 - Centralized management
 - FP system architecture
 - Life cycle development/maintenance

Force Protection Study

66



Force Protection "Organization"



- CSA task the G3 to develop an Organizational Solution for Army Force Protection
 - Requires a "School" - TRADOC
 - Requires a Systems of Systems R&D Focus - AMC
 - Requires an Acquisition "Czar" PEO - FP
 - Owns the Risk Management role (a most important and difficult task to allocate limited FP resources)
 - Responsible for the systems development and life-cycle support of FP systems and tools
 - Provides Technical and Operational support to
 - Tactical and Installation entities
 - The Installation Management Agency
 - Installation and Tactical Commanders
 - The R&D and COTS community for FP applications
 - Focus for other Services, Homeland Security, and other Govt. Agencies

Force Protection Study

67



Integrated, Network-centric Force Protection ATD



- Army sponsor an integrated network centric ATD (FY 2004), integrating the following classes of sensors, decision aids and networks:
 - Soldier portable 2 lb bio sensor; small, lightweight, power efficient, biological sensor, with minimal false positive/negatives
 - Soldier portable 2 lb chemical sensors
 - Mobile sniper response sensor
 - Mobile mortar response sensor set
 - UAV/UGS combine mine team
 - Suicide Bomber identification
 - Block Zero Decision Support System (DSS)
 - Army (AMC) conduct urgent study of means, tactics, and payoff for novel illumination control over threat based and defended areas or corridors

Force Protection Study

68



Critical Biological Sensor Recommendation



- Army develop a small, lightweight, power efficient, biological sensor, able to detect all DOD identified biological agents with minimal false positive/negative outcomes
 - ARL/ECBC lead effort
 - Partnership with other agencies and services

Force Protection Study

69



Decision Aids Recommendation



- Army RDECOM (SOSI/ARL) develop an Integrated Force Protection Decision Support System (DSS) for the Commander
 - Many individual Decision Support Technologies
 - Individual Technologies provide significant capability to support Commander in all phases of FP (defend, preempt, deceive, etc.)
 - However, it is currently difficult to accomplish cost benefit tradeoffs (to improve the DSS) across the individual decision aids and with no plan to solve this in the future
 - A decision support system which integrates the individual decision support systems is required to support the Commander with the capability to determine the best FP course of action and implementations

Force Protection Study

70



Closing Words



In today's world of Army global deployments, Force Protection takes on an importance beyond the historic look at boundaries and sentries. An integrated systems approach is critical to the "enabling" of our mission when our personnel are sent in harms way. A new way of thinking, intense training, centralization of doctrine and flexible hardware availability are key elements to mission success.

A new vision of force protection is required

Force Protection Study

71



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately? 
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

72

 What can we do immediately? (within 90 days) 			
Technology/Ops	Application	Function	Source/Implementation
Sniper detection Pillar--NRL--Lifeguard	Detect and return fire	Acoustic, Acoustic + Flash detection, IR night signature tracking to origin	- Pilar-France via NVL - NRL-Flash & Acoustic - Lifeguard - LLNL/Marines
Inter-squad radio with long life batteries (Li-Ion, solar recharge) and embedded GPS	Situational Awareness (SA)	Constant wireless communication for small units	Commercial
Enhanced body armor (to cover extremities plus torso)	Soldiers at guard posts and low mobility functions	Protect soldiers from small arms fire and fragmentation weapons	Commercial in concert with Natick Labs
Soldier-launched small UAVs with EO/IR sensors	Overflight views of areas of concern	Surveillance	Commercial
*Combined Technology/Treat/Operations Panels' recommendations			
Force Protection Study			

73

 What can we do immediately? (within 90 days) 			
Technology/Ops	Application	Function	Source/Implementation
Enhanced vehicle applique armor	Prevent penetration by small arms and shrapnel	Use fiber composites/ceramics/cermets to prevent penetration	Commercial/ARL
Non-lethal High Power Microwave (HPM)	- Crowd control - Separate hostiles from innocents	At ranges 1 - 2 Km expose personnel to short-pulse burning sensation	Joint Non-Lethal Weapons Office (Marines, AFRL)
SPIDER (Stabilize Panoramic Intrusion Detection and Recognition)	- Base perimeters	- Perimeter area surveillance	- PM-PSE - Global International Security
*Combined Technology/Treat/Operations Panels' recommendations			
Force Protection Study			

74

 What can we do immediately? (within 90 days)* 			
Technology/Ops	Application	Function	Source/Implementation
*Enhanced IED detection (under development, available approx 1 year)	Detection of suicide bombers/mines/other munitions	- Detects electronic initiation systems of IEDs	- Israel Ministry of Defense/Rafael Industries
*Combined Technology/Treat/Operations Panels' recommendations			
Force Protection Study			

75

 What can we do immediately? (within 90 days) 			
Technology/Ops	Application	Function	Source/Implementation
Joint patrols with indigenous personnel	- Enhances community relations - Suppresses uniqueness of US forces - Provides conduits for intel	- "Cop on beat" benefits - Reduce aversion to "occupation" forces	- Local military and rehabilitated police who are integrated as rapidly as possible
More secure bounties	- Encourage information flow - "Buy-back" of weapons - WMD information	- Locate and neutralize threats	- Establish secure and completely confidential award system - Promptly act on information flow
*Combined Technology/Treat/Operations Panels' recommendations			
Force Protection Study			

76




Brainstorming on What we could provide to Iraq today?

- Shortstop (jams radio controlled explosives)
- Spider (Area Surveillance)/ JLENS
- Sniper Detection
- Other "jam-proof" weapons
- Commercial GPS
- Commercial Armored Cars
- JLENS Communications Relay (Aerostat Relay for Military Comms)
- Non-Lethal Capability sets (move from other Army units)
- Commercial Non-lethal weapons (TASERS)
- Selected Decision Aids
- Perimeter Illumination
- More Iridium/INMARSAT phones
- Commercial perimeter and detection systems
- Prison perimeter security equipment
- Wichmann's Ground Penetrating Radar for Mine Detection

Force Protection Study

77




Send to Iraq?

- Lifeguard Sniper Detection
- PILAR (French) Sniper Detection
- UAVs
- UGVs (eg MDARS)
- Technical Advisors (Government and Industry)
- DROZD/ARENA with paintballs instead of ball bearings
- Elevated IR mortar locator
- Truck Tracking Satellite
- LOJAC
- Downed pilot location network for individual soldiers
- Commercial Emergency Locator (Individual Tags)
- NVGs for support soldiers (commercial version)
- Weapon Detection (magnetic wand, portals)
- Magnetic balance loops detecting metal movement
- Nitrate trace detector (signature of handling explosives)

Force Protection Study

78




Send to Iraq?

- Cell/TETRA commercial infrastructure (with hand held unit)
- Current commercial imagery from space
- Commercial broadcast audio and video propaganda
- Commercial Bulldozer
- Funding to purchase weapons from Iraqis

Force Protection Study

79




Quantico Demo Vendors

- Query them for availability today
- Fixed Price, immediate delivery, undefined number, quick contract

Force Protection Study

80



Technology Solutions Outline



- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately? ←
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

81



Sensor Technology for Force Protection



- Subpanel to Technology panel of the ASB Force Protection Study 2003
- Members:
 - Steven Kornguth - Lead
 - Gary Glaser
 - John Reese
 - Paul Tilson
 - Jack Wade
 - Randy Woodson

Objective: Evaluate existing and emerging sensor technologies that could make a significant contribution to the US Army Force Protection needs

Force Protection Study

82



Background Biological Chemical



- In 1996, the Army Science Board (ASB) addressed and made following recommendations on B/C Defense programs:
- Improve detection and decontamination technologies against biological and chemical agents.
- The study group analyzed seven key areas:
 1. Agent Detection and Identification
 2. Decontamination
 3. Protective Clothing, Equipment, and Shelter
 4. Pharmaceutical Countermeasures
 5. DOTLMP
 6. Post-Engagement Ground Effects Model
 7. Diplomacy as a passive defense

Force Protection Study

83



Biological/Chemical



- Nerve agents included (sarin, GB), vesicants (sulfur mustards), and blood agents (cyanides). Biological agents considered included those causing anthrax, brucellosis, plague, q-fever, tularemia, Venezuelan (Eastern and Western) Equine encephalitis, viral hemorrhagic fevers (yellow fever and Lassa fever), and toxins including ricin, botulinum, enterotoxin B, and T-2 mycotoxin.

Most Critical Needs

- Increased defense capability against biological warfare (BW) because of past emphasis of the defense community on chemical warfare (CW). Expediting implementation of enzymatic, scavenger, supercritical fluid, foam, ozone, and light technology systems for decontamination.
- Critical capability for anthrax and plague vaccine production.
- Better integration between Joint Staff and Services in BW/CW responses.

Force Protection Study

84



Biological/Chemical



- Little progress has been realized in Force Protection from BW agents by 2003
- Multiple systems are currently required to detect all near term BW and CW agents; no single networked or integrated system exists in 2003
- DECON solutions were corrosive to equipment
- Protective mask design and filter composition for BW agents need improvement to enhance shelf life and usable time during deployment

Force Protection Study

85



High Explosives



- The threat to deployed allied forces from non-metallic mines, RPG's, improvised explosive devices(IED) persists at a high level (Iraq, Afghanistan)
- There is a significant difference between stand off detection of open vs. sealed/encased high explosives
- The free standing explosives release volatile signatures that may be detected remotely

Force Protection Study

86



Bio Agent Prophylaxis and Treatment



- Prophylaxis
 - Vaccines (use attenuated live or heat killed agent)
 - Administer pre or immediate post exposure
 - Adjuvants and biological response modifiers to enhance immune response (reduce time from ~10 days to 3 days); enhance innate immune properties
 - Face masks and light body covering
- Treatment and Management
 - antibiotics/ antivirals
 - quarantine

Force Protection Study

87



Findings Chem/Bio



- Significant investments exist in biological, chemical detection. Stand-off technology exists for chemical agents in air including spectral analysis in UV/VIS/IR range. No current stand-off capability for B agents
- Extensive work needed to achieve small (<2 lbs), power efficient B sensors with very low false positive/negative rates.

Force Protection Study

88



Findings–Bio/Chem Threat



- In 2003, multi-array sensor technologies have become a reality for BW agents. These sensors detect and identify threat agents as point detectors but not as standoff detectors. No current capability to produce agent detectors and identifiers that can regenerate functional surfaces and sustain operation for extended periods of time in an autonomous/robotic mode
- The great advance in sequencing the human genome in 2002 has yielded extensive knowledge regarding the genome of almost all BW threat agents and has offered some understanding of elements of the human genome that predispose to infection
- Protective clothing for BW and CW agents that permit full field of vision and comfort needed during operational activities are not available

Force Protection Study

89



Findings Bio/Chem



- In the Biological arena, antibody based sensors are secondary effect systems that react primarily with a threat agent but other non-pathogens also react with antibody. Genetic recognition elements are unambiguous identifiers but processing takes time (>20 min)
- Chemical agents HX and volatile precursors are readily detected/identified by GC-MS or tandem MS
- The sensor platform must be autonomous and self-regenerating over extended periods of time

Force Protection Study

90



Findings - High Explosive



- Detection of non-metallic mines, encased explosives (e.g. car bombs, RPG's, human suicide bombers) requires unusual technology (e.g. neutron activation and analysis). Requires extensive shielding because of adverse effects on persons thereby reducing utility for rapid screening of persons and equipment in populated settings
- Programs include Ancore CA, VEDS and INEEL, R/SEDS

Force Protection Study

91



Findings Radiological/Nuclear



- Portal and rail transport monitoring of radio/nuclear materials are currently available. Rate limiting effects include velocity of vehicle and dosage of nuclear material
- Programs include Sandia Second Line of Defense

Force Protection Study

92



Findings – Detecting Camouflaged/Hidden Threats



- Active Army R&D Programs successfully detect heat emitting and microwave absorbing/reflecting targets (platforms and persons) covered by foliage or solid structures.
- Seismic/acoustic systems and ground penetrating radar has utility in identification of Underground facilities at depths to 100 meters. Seismic/acoustic systems are effective in wet and dry soils but require close spaced receivers (approximately spaced at 200 ft intervals) which complicates mapping large areas. The GPR is very useful for large area scanning in dry sand and rock areas; clay soils are refractory because high humidity/water content reduces effectiveness.

Force Protection Study

92



Findings Prophylaxis and Treatment



- Prophylaxis
 - Vaccines
 - current vaccines for B agent (e.g. b. anthracis-Bioport) utilize traditional methodologies and exhibit undesired side effects
 - All vaccines to date exhibit adverse effects on subjects
 - Recent FDA approval of vaccines shown to have efficacy in animal testing alone will greatly facilitate development of new vaccines for rare infectious disease.
 - Strong Program at Joint Program Executive Office Chemical
 - Biological Defense supports development novel vaccines to select threat agents

Force Protection Study

94



Findings Prophylaxis and Treatment



- Adjuvants
 - Can enhance response to lower dosage immunogen and reduce time for protection
 - Novel adjuvants explored by JPEOCBD
- Biological Response Modifiers
 - Interleukins, cytokines affect immune response
 - May provide protection when administered immediately post exposure
 - Cause adverse side effects (e.g. fever)
- Masks and Face Protection
 - Face covering and light body covering protect exposed persons from contracting illness from B agents

Force Protection Study

95



Findings – Prophylaxis and Treatment



Antibiotics and antivirals

- Introduction of new antibiotics/antivirals into the public sector rapidly results in development of drug resistant strains. Associated with legal and social implications (e.g. lack of release till crisis may result in increased morbidity of population exposed to agent)

Quarantine

- Experience of SARS in Spring of 2003 indicates public acceptance of quarantine policy CONUS and OCONUS

Force Protection Study

96




Conclusions - Bio/Chem

- Large equipment exists for detecting and identifying B and C agents.
 - equipment weighing >100 pounds can be installed at fixed facilities
 - compact sensors (~ 40 pounds), based on genomics, are available for a limited number of B agents
 - Heavy equipment exists for the stand-off detection of C agents.
- The threat from booby trapped caves, large government buildings is not addressed with these capabilities

Force Protection Study

97




Conclusions - Sensors for Threat Persons/Equipment

- Radar and microwave systems detect persons and ground platforms from a distance of hundreds of meters. These systems can penetrate foliage and several building materials.
- IR, microwave and broad band detect both high- and low-velocity projectiles

Force Protection Study

98




Conclusions Prophylaxis and Treatment

Vaccines

- Funding exists through JPEOCBD and HHS for development of a limited number of threat agents; JPEOCBD strives to develop FDA approved vaccines. Need common goals between DoD and HHS funded vaccine activities

Adjuvants and Biological Response Modifiers

- Novel adjuvants and BRM are appearing in commercial market

Antibiotics/ Antivirals

- Develop drugs with restricted distribution

Force Protection Study

99




Recommendations

- Small, lightweight (<2 lbs), energy efficient sensors for all DoD identified biological agents. The sensors must have low false positive/negative responses
- Sensors to detect sealed/encased high explosives at a distance

Force Protection Study

100



Investments to Enhance FP Regarding Biological Agents



- **Sensors- detect and ID**
 - Biological-small, light weight (<2 lbs) multi-array, integrated/networked detect/ID for all identified threat agents-\$120 million dollars
- **Protection pre-exposure**
 - Vaccines (FDA Approval approximates \$500 million per vaccine)
 - Immune Response Enhancers/Modifiers
 - Provide general increased resistance to disease but not comparable to vaccine in specific protection
- **Individual and group protection post release**
 - Antibiotics/antivirals with no antibiotic resistance
 - Preclude distribution prior to threat-social legal issues

Force Protection Study

101



Investment Issues B Agents



- Sensor investments for B agents heavily driven by HHS compared to DoD (99:1)
- B agent vaccines developed by DoD and HHS must be directed toward FDA approval process (new FDA policy on animal in lieu of human testing facilitates this)
- Immune enhancers include adjuvants and immune response modifiers. Both require significant investment by a magnitude less than individual vaccines. Must determine relative protection offered by vaccines vs. IE.
- Social/legal issues in withholding effective antibiotics/antivirals

Force Protection Study

102



Technology Solutions Outline



- **Overview**
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- **What can we do immediately?**
- **Technology Team Reports**
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids



Force Protection Study

103



Force Protection Technology Solutions

Weapons & Survivability Sub-Panel



Scope

- Tasked to survey to depth required for support overall study
- Work supports overall total systems approach
- Few findings and recommendations

Members:

- Dr. Richard Montgomery – ASB Consultant
- Dr. Reed Mosher – Government Advisor – USA
- Mr. Mike Toscano – Government Advisor – OSD

Visits:

- Quantico Army Base – May 6, 2003
- Study plenary sessions

Force Protection Study

104



Technology Solutions Panel

Weapons & Survivability



Cover - Scope - Outline Background - Threat characteristics - Threat characteristics (cont'd) - Threat characteristics (cont'd) - Lethal weapons - Non-lethal weapons - Lethal/non-lethal weapons use	Passive counter measures Dynamic large area Illumination control Major Findings - Illuminating Control Concept - Needs Prioritization - Technology Application - Prioritization Conclusions Recommendations

Force Protection Study

105



Background

Weapons & Survivability



Indirect Fire

- **Threats**
 - Principally mortars and short range rockets
 - Weapons are crude but effective
 - Threat magnified by addition of in-flight guidance
- **Protection**
 - Passive Protection
 - Prediction and Preemption
 - Active Protection
 - Active point defense is the most practical
 - Active defense concepts for high-value targets
 - Deflection
 - Pre-detonation
- **Observations**
 - Preemption preferred tactic and is dependent on multiple sensor integration and assessment

Force Protection Study

106



Background

Weapons & Survivability



Direct Fire

- **Threats**
 - Principally Mines, RPG's, MANPAD'S, Bombs, and Small Arms
 - Light Weight Body Armor increases its use in non-combat scenarios
- **Protection**
 - Passive Protection
 - Body Armor
 - Commercial Produced Ballistic Protected Vehicles Available
 - Barriers and Ballistic and Blast Hardening Facilities
 - Prediction and Preemption
 - Mine detection and neutralization
 - Counter Fire
- **Observations**
 - Standoff Procedures are Important
 - Need Additional Layered Protection for Personnel Concentration and Command and Control
 - Solution Both Procedural and Technology Based
 - Routine Transportation in Smaller Armored Vehicles commercially available
 - Ground penetrating radar for detection of buried mines current hope

Force Protection Study

107



Background

Weapons & Survivability



Vehicle delivery

- **Threats**
 - Car or truck – most lethal to date (HE)
 - Small aircraft (Manned or Unmanned)
 - Difficult to Identify and stop
- **Protection**
 - Prevention and Preemption
 - Perimeter Fences and Barriers
 - Gates and Access Control
 - Ballistic and Blast Hardening Facilities
- **Observations**
 - Preemption preferred tactic
 - Keep out zones essential -- HPM and active defense
 - Preemption is dependent on multiple sensor integration and assessment

Force Protection Study

108



Background Weapons & Survivability



Suicide bomber

- Threat
 - Human Delivery
 - Difficult to Identify and stop
- Protection
 - Prevention and Preemption
 - Access Control
 - Ballistic and Blast Hardening Facilities
- Observations
 - Preemption preferred tactic
 - Standoff detection and isolation identified needs
 - Counter bomb/counter bomber ACTD in place
 - Need improved prediction and warning

Force Protection Study

109



Background Weapons & Survivability



Defensive Lethal weapons

- Primarily standard tactical issue
- Remote control and automated applications including UAV's and UGV's
- Additional specialized needs
 - Point defense of high-value targets/personnel concentrations
 - Gun applications – e.g., BOFOR
 - Vehicle mounted solid state laser
 - Armed UAV/UGV for preemptive opportunities

Force Protection Study

110



Non-Lethal Background



- No formal DoD requirement – DoD may have unique needs
 - Army Operational Concept pamphlet – April 2003
- High priority for research, development, and testing
- Wide range of applications
 - Force protection
 - Supports stability and support operations (SASO)
 - Crisis and contingency response options
 - Separate combatant and non-combatant
 - Complements current, interim and objective forces
- Criteria for use
 - Rules of engagement
 - Treaty constraints
 - Legality (national resolution)
- Near instantaneous effects is needed in most scenarios
- **Need both point and limited area weapons – direct/indirect**

Force Protection Study

111



Background Weapons & Survivability



Current: non-lethal weapons capability sets

- 12 gauge point, area & flash band
- 40mm point & area rounds
- 5.56mm area muzzle launched ordnance
- Stun grenade
- Handheld dye marker
- Modular crowd control munitions

Force Protection Study

112



Background

Weapons & Survivability



Current non-lethal weapons acquisition programs

- Mobility denial system
 - Anti-traction material
- Clear A space
 - Combined acoustic/optical device
- Hand emplaced NL munitions
 - Pre-emplaced
 - Electric stun under consideration

Force Protection Study

113



Background

Weapons & Survivability



Non-lethal weapons technology

- Electrical
 - Direct current
 - Pulsed current
- Radio frequency
 - RF devices
 - Wide/ultra wide band
- Microwave frequency
 - High power microwave
 - Millimeter wave

Force Protection Study

114



Background

Weapons & Survivability



Non-lethal weapons technology

- Infrared
 - Chemical oxygen iodine laser
 - Hydrogen/deuterium fluoride lasers
 - Solid state lasers
- Visible light
 - Argon lasers
 - Isotropic radiators
 - Flashes, flares & strobes
- Ultraviolet
 - Lasers ionizes

Force Protection Study

115



Background

Weapons & Survivability



- Lethal / non lethal weapons use issues
 - Policy
 - Availability does not affect usage of lethal weapons
 - Not required to have zero probability of fatalities or permanent damage
 - Usage to complement lethal weapons
 - Criteria for use
 - Rules of engagement, treaty constraints, unpredictable results, legality
 - Utilization/decision making
 - Training, manned/unmanned, sensing, timing

Force Protection Study

116



Background

Weapons & Survivability



Passive counter measures

- Soldier protective equipment
 - Tactical body armor
- Vehicle protection
- Physical security
 - Command and control
 - Outside perimeter surveillance
 - Perimeter control
 - Fence systems and barriers
 - Senor based intrusion detection
 - Access control
 - Explosive and CB detection
- Blast and ballistics mitigation
- Chemical and biological detection and mitigation

Force Protection Study

117



Background

Weapons & Survivability



Dynamic large area illumination control

- Historic need for night time illumination over threat area since ancient times
- Threat night vision capabilities comparable to U.S.
- Gallium nitride is a new enabling technology
- Provide bright moonlight equivalent over large area > 50km²
- Extends use of existing visual sensors and weapons
- Dynamics
 - Area
 - Brightness

Force Protection Study

118



Findings

Illuminating Control Concept



- Mobile elevated high intensity light source for wide-area or selected zone illumination
- Features
 - High efficiency light weight LED light source (gallium nitride)
 - Tunable (color, intensity)
 - Flash or continuous
 - FW or LTA unmanned
- Uses
 - Dynamics usage – Dependent on threat, weather, tactics, and level of hostilities
 - Extends utilization of all visual sensors including human and UAV's
 - Detect penetration of restricted areas/complements other sensors
 - Disrupt threat operation
 - Aids perimeter surveillance
 - Reflection from clouds option

Force Protection Study

119



Findings – Needs Prioritization

Weapons and Survivability



	Protective Measures				
	Vulnerability Reduction	Prediction/Prevention/Preemption	Active Defense	Damage Control	Response (Counter Fire, etc.)
Indirect Fire	2	1	2	3	2
Direct Fire	2	1	3	3	2
Vehicle Delivery	2	1	2	3	3
Suicide Bomber	2	1	3	3	3

1. Highest potential payoff 2. Good potential payoff 3. Unlikely payoff

Force Protection Study

120

Technology Applications Prioritization		
	Highest Potential	Useful Potential
Indirect Fire	Multiple sensor integration Illumination control Armed UAV's	Bomb shelter Personnel areas ballistic protection Preventive point defense Counter fire
Direct Fire	Non-lethal Weapons Mine detection and neutralization Illumination control Armed UAV's	Commercial armored vehicles Personnel areas hardening
Vehicle	Remote explosive detection and neutralization	Inspection areas Air defense
Suicide Bomber	Stand off explosive detection and neutralization Human behavior screening	Isolation area for suspects

121

Conclusions

- The Army should define its capability needs and operational plans for the use of non-lethal weapons.
- The Army should identify the policies, legal, or treaty restrictions and make the necessary changes to ensure that non-lethal weapons can be effectively used.
- The Army should establish its own requirements for Non-Lethal Weapons.
- The Army should invest in future technology for preemption and defense of direct and indirect fire:
 - Dynamic large area illumination
 - More mine detection and neutralization
 - Point defense of ballistic fragment protected troop concentrations
 - Non-lethal weapons and sensors
 - Armed UAV's
- The Army should continue to invest in technology development to reduce vulnerability

122

Recommendations

- Dynamic large area illumination
- More mine detection and neutralization
- Preferential point defense of ballistic fragment protected troop concentrations and Command and Control
- Routine use of ballistic protected commercial vehicles
- Army needs to establish formal requirements and doctrine for the use non-lethal weapons

123

Technology Solutions Outline

- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

124



Automation and Robotics Technology for Force Protection



- Subpanel to Technology panel of the ASB Force Protection Study 2003
- Members:
 - Mark Hofmann
 - Prasanna Mulgaonkar - Lead
 - Mike Toscano

Objective: Evaluate robotics and automation technologies capable of increasing the effectiveness of soldiers doing force protection tasks

Force Protection Study

125



Automation and Robotics Background

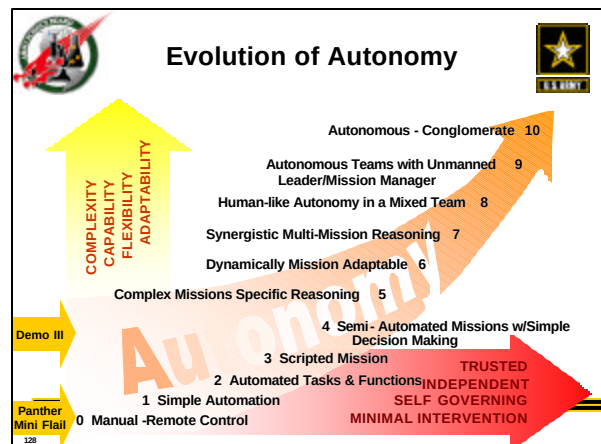
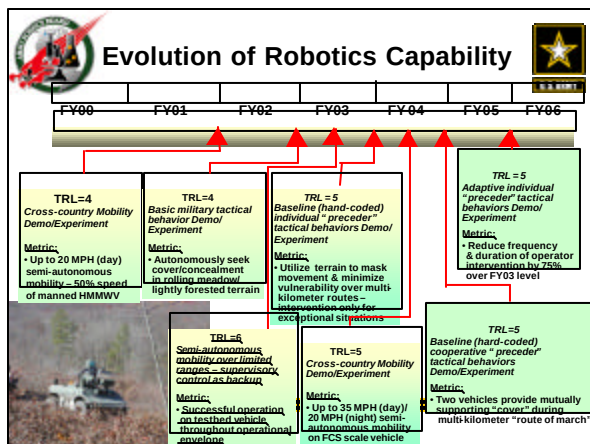


- Force protection is the first application where autonomous robotics can play a major role
- UAV and UGV technologies are maturing at a rapid pace
- Automatic sensor processing technology derived from the robotics community (in particular, video) can significantly reduce surveillance workload



Force Protection Study

126





Panel Focus



- Unmanned vehicles (ground and air)
 - Platforms for carrying sensor packages
 - Fixed site protection
 - Routine patrol of secured areas
- Automatic visual sensor processing
 - Improved surveillance without overload
 - Sensor net to cover urban areas
 - Connectivity into existing civilian camera systems

Moderately structured environments of force protection are ideal for applying today's autonomous robotics capability

Force Protection Study

129



Visits



Completed

- ARL - Chuck Shoemaker (Demo III, CART)
- PM-PSE – MDARS(E)
- JPO - Mike Toscano (Physical Security demo)
- Advanced Vision systems – CMU, UMD, Sarnoff
- OTTF - COL Bruce Jette (Lessons learned from Afghanistan)

Planned visits that could not be completed

- DARPA - Scott Fish, Sam Wilson, Doug Gage, Larry Stotts
- Sandia- Pat Eicker, Mark Swinson
- DARPA - Tom Strat, Jonathan Phillips
- NSA - Dave Murley
- ARDA - Randy Paul

Force Protection Study

130



Findings



- Structured (fixed or planned) site protection application appears to be amenable to today's automation and robotics
- Semi automated convoy operations are maturing through the ARL and TARDEC programs
- Programs (e.g., MDARS) underway to transition ARL and TARDEC UGV technology into user programs
- DARPA/ARL research in video surveillance technology mature enough to transition to the FP community
- No fully integrated testbed exists where technologies can be evaluated in a FP systems context, and leaders trained in their use

Force Protection Study

131



Findings (detailed)

Structured Site Protection





- PM-PSE making significant strides in technology for physical security
- TSWG supported Physical Security demonstrations in Quantico attended by 400 vendors spanning an entire range of technologies
- Fragmented marketplace with a few large systems vendors – mainly small component suppliers, and several one-of system integrators
- A system-of-systems methodology is lacking
 - Few common interface standards (Plug and Play)
 - No integration testbed or leadership

Force Protection Study

132



Findings (Detailed)

Transition of Robotics Technologies into Programs





- MDARS-E program is on track to move unmanned ground systems into operational use
- Product qualification and fielding at Hawthorne Army Depot in FY04
- Applicable for fixed sites with well-defined access paths and moderately controlled environments
- Effective transition of ARL automated robotics systems technology (e.g., multiple levels of collision and obstacle avoidance)
- Human-Robot interfaces is a continuing issue
- Minimal combined-UAV-UGV systems being transitioned or realistically experimented with at this time

Force Protection Study
133



Findings (Detailed)

DARPA/ARL Research in Video Surveillance





- Significant progress in
 - Object tracking
 - Video motion detection
 - Multi camera coordination
 - Activity understanding and monitoring
- On the verge of semi-automated capability to rapidly monitor large urban areas (DARPA Combat Zones that See program)
- Critical tool for remote understanding of evolving situation
 - Understand emerging threats before they become threats
- Technologies drawn from the robotics activities

Force Protection Study
134



Findings (Detailed)

Lack of an Integrated Systems Testbed



- All three services have identified the need for integrated testbeds
 - Air Force – Hanscom AFB, MA
 - Navy – North Island, CA
 - Army – Ft. Belvoir, VA
- Current emphasis is on evaluating available COTS components
- Lack of emphasis on
 - Architectures
 - CONOPS and TTPs
 - Training on users and commanders in the use of the technologies
 - Interservice commonality and reuse of knowledge/tools/etc.

Force Protection Study
135



Conclusions



- Autonomous robotics technology is mature enough for some force protection applications. It should be a focus within the Army resulting in accelerated deployment and enhancement of MDARS(E), robotic followers, and autonomous surveillance UAVs
- Autonomous robotics technology can significantly reduce manpower and cost required for force protection surveillance, patrol, and other routine functions
- Integrating UAVs and UGVs into combined teams (with humans) could provide significant improvements in coverage and surveillance response time
- Automatic sensor processing and fusion technology (in particular, video) could significantly reduce manned surveillance workload, especially in urban areas. Many of these techniques are at a maturity level appropriate for near-term fielding
- Unmanned autonomous systems could also address insider "threat"s typically found in overseas installations

Force Protection Study
136



Automation and Robotics Recommendations



- Increase the acquisition and insertion of autonomous robotic systems for force protection (for example, MDARS(E) for perimeter defense)
- Support and fund an Integrated Multiservice Force Protection Technology Testbed
- Create ATDs and sponsor ACTDs with capability to accelerate FP technologies from S&T into operational capabilities
 - Use the ATDs and ACTDs to foster tight coupling between all elements of the S&T community
- Develop the appropriate requirements, metrics, and technology-enabled TTPs

Force Protection Study

127



Automation and Robotics Recommendations (Detailed)



- Accelerate acquisition of autonomous systems for Force Protection
 - Procure additional prototypes
 - Deploy on an experimental basis at noncritical sites to gain operational experience
 - Determine required mission package payloads to maximize the utility of the platforms

Force Protection Study

128



Automation and Robotics Recommendations (Detailed)



- Force Protection Technology Testbed
 - Create a testbed controlled by a Force Protection Organization (FPCoE, belly button, etc.)
 - Fund comprehensive Army testbed to get a core of technology (COTS, GOTS, new technologies) to be integrated, maintained, and evaluated under realistic conditions
 - Define a “Chief Systems Engineer” for establishing standards for integrated FP systems

Force Protection Study

129



Automation and Robotics Recommendations (Detailed)



- ATD and ACTD Scope
 - Combine UAVs + UGVs
 - Leverage MDARS(E)
 - Leverage FCS UAVs and Micro Air Vehicles
 - Accelerate deployment of automated visual processing technology
 - Leverage DARPA programs on video surveillance, in particular the Combat Zones that See.
 - Transition vision technology from ARL robotics activity

Force Protection Study

130




Automation and Robotics Recommendations (Detailed)

- Develop requirements, metrics, TTPs
 - Assign tasks to a FP focused organization, e.g.:
 - School
 - Battle Lab
 - Requirements should have a broad FP focus (beyond just MP functions)
 - Create a culture where all officers undergo escalating levels of training in FP and risk management
 - Document FP best Practices and lessons learned

Force Protection Study

141




Technology Solutions Outline

- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

142




Sub-Panel Members

- Dr. Don Kelly, Co-Chair
- Ms. Ginger Lew, Co-Chair
- Dr. Prasanna Mulgaonkar
- Dr. Steven Kornguth
- Dr. Ira Kohlberg
- Advisors: Pete Van Syckle, CECOM RDEC

Force Protection Study

143




Outline

- Theme and Scope
- Study Schedule
- Briefings Received
- Network Technologies
- Findings and Recommendations

Force Protection Study

144



Theme and Scope



- Theme: How does the Army ensure network used to support force protection? Two timeframes are considered: short term (through 2006) and long term (2010-2015).
- Scope: Investigate promising high-payoff technologies for the two time periods. Networks are a broad subject, need tie-in to sensors and other areas.

Force Protection Study

145



Study Schedule



4/14-15	ARL	Tech Panel meeting
4/28	CECOM	Subject matter experts
5/6	Quantico	FP demonstrations
5/7-8	DC	Tech Panel meeting
6/10-11	LA	Tech Panel meeting
7/14-24		Irvine Summer Session

Force Protection Study

146



Site Visit To CECOM



Briefings

- JTRS Squad Level Comms
- FCS Comms
- MARCON-I
- MOSAIC
- On the Move SATCOM
- Advanced Antennas
- Dynamic Re-Addressing and Management (DRAMA)
- Free Space Optical Communications System (FOCUS)
- Adaptive Joint C4ISR Node (AJCN)
- Networked Sensors for the Objective Force ATD
- Tactical Wireless Network Assurance

Force Protection Study

147



Wireless Networking

The Network Includes Many Inter-Related Components

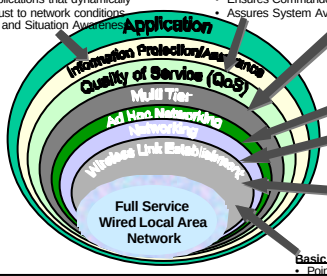


Applications

- Applications that dynamically adjust to network conditions
- C2 and Situation Awareness

Information Protection/Assurance

- Ensures Commanders Confidence
- Assures System Availability



Quality of Service (QoS)

- Reliable, fully mobile networking
- Priority and Precedence
- Dynamically managed bandwidth
- Self-Healing

Multi-Tier

- Additional Routing Paths

Ad Hoc Networking

- Fully mobile voice/video/data
- Minutes to configure
- Easy to join or leave network

Basic Networking

- Voice/video/data
- Limited mobility
- Days to configure/reconfigure
- Difficult to join/leave network

Basic Connectivity

- Point-to-Point
- Voice Only

Right Information, to the Right Destination at the Right Time

Force Protection Study

148




Network Findings Key Themes

- Most of the network technologies needed for force protection are also needed for combat and non-combat networks
- Low tech solutions, such as adhering to basic COMSEC practices, are extremely importance in network force protection
- Inadequate funding to develop the technologies needed by DOD that will not be developed commercially

Force Protection Study
149




Network Findings

Must Consider Both Low and High Tech Needs

Low Tech Force Protection Examples

- Each soldier trained to certain level on IT basics
- Physical security of all components of network
- COMSEC procedures
- Contractor and In-Country support

Higher Tech Network Force Protection Examples

- Quick purge of data
- Over-the-air re-keying
- Remote disable of users and nodes
- Re-routing of traffic to exclude persons or nodes
- Network intrusion detection

Force Protection Study
150




Network Findings

- Important areas lack sufficient funding (commercial and Government)
 - Network intrusion detection
 - COMSEC and multi-level security
 - Protocols and data formats for force protection and information assurance (C2 and SA messages)
 - “Guard” – Transfer info from one level to another, protection from unauthorized access at all levels
 - Interoperability with other and legacy systems, conforming to standards
 - Role-Based Access Control – Tie the network access of each soldier to his/her role rather than visibility
 - Group Key Management – Dynamic, flexible, rapid re-keying in battlefield, secure multicast (no commercial standard)
 - Ad Hoc, Mobile, Self Organizing Networks
 - Small, Easily Erectable Masts; Low Profile OTM Antennas; Smart antennas
 - Spectrum - Restricted Frequency Assignments; Geographically Impacted

Force Protection Study
151




Conclusions

Integrated Approach Is Needed. There are huge challenges in force protection of the network. These challenges are inherently inter-related, yet are often addressed in a piece-wise rather than integrated manner.

Army Development Focus. Until an integrated approach is adopted, it is difficult to define the level of S&T investment required. The Army should focus their development efforts on the totality of information management, data flow, network, and radios to support network-centric operations. Critical network force protection issues include network intrinsic dynamics protection, sensor fusion and data management, spectrum and RF bandwidth, multi-level security, software integrity and physical protection of the hardware.

Soldier IT Expertise. There is a need for an optimal, integrated approach that addresses Network force protection of the future will require IT expertise well beyond today's level. There is a need for a well-defined policy that explains which soldiers will have what expertise, how we will train our soldiers, what contractors will be used, any host network infrastructure used, and host nation IT personnel support needed for various scenarios.

Force Protection Study
152




Recommendations

- The Director of Army's CERDEC (CECOM) should direct the System Engineering Office (CERDEC ASE0) to be the responsible office for integrating and maintaining an Army-wide network force protection and policy.
- In addition, this office should be given the responsibility for determining how and what level of IT support will be needed through the various spiral development phases of network development for FCS. This should include the IT expertise required of the individual soldier, and how we will tie-in to any host-nation IT infrastructure.
- Action: CECOM CERDEC ASE0

Force Protection Study

153




Backups

Force Protection Study

154




Case Studies - Convoy

Capabilities

- Short-range, intra and inter-vehicles comms
- Robust connections to local sensors
- Reachback on-the-move data-links for comms and SA/Intel
- GPS for position w.r.t. global coordinates
- Localized positioning for blue force tracking, safety

Low Tech FP

- Each soldier trained to certain level on IT basics
- Physical security of local network components
- Good COMSEC procedures

Higher Tech FP

- LPI/LPD wireless, SATCOM for reachback
- Encryption, authentication, secure routers
- Passwords, fingerprint, retina identifiers

Force Protection Study

155




Case Studies - OCONUS

Capabilities

- Short-range base level comms
- Wired and wireless network components
- Networks of security sensors
- Reachback fixed data-links for comms and data

Low Tech FP

- Each soldier trained to certain level on IT basics
- Physical security of local network components
- Good COMSEC procedures

Higher Tech FP

- Secure local wireless, plus SATCOM and wired for reach-back
- Encryption, authentication, secure routers
- Passwords, fingerprint, retina identifiers
- Contractor and host-nation support – info assurance
- Use of host-nation infrastructure – info assurance

Force Protection Study

156




Army Network-Related Pacing Technologies

Networked Sensors

- Low power, small efficient fast signal correlators
- Jam resistant, LPI/LPD waveforms
- Energy efficient networking protocols and channel access

Advanced Antennas

- Dual mode VHF/UHF antennas
- Distributed reactive tuning
- Multi-element radiating structures
- Coaxial and slotted traps
- Genetic algorithm optimization
- Taped resistive loading
- Lumped circuit loading
- Distributed LRC networks

Force Protection Study

157




Army Network-Related Pacing Technologies

Tactical Wireless Network Assurance

- Advanced network access control
- Wireless intrusion detection
- Synchronized security management
- Tactical public key infrastructure
- Mobile code authentication

JTRS Squad-Level Communications

- Calable RF
- System-on-a-chip
- Software defined radio

Force Protection Study

158




Army Network-Related Pacing Technologies

Dynamic Re-Addressing and Management (DRAMA)

- AI enabled automated fault diagnostics
- Mobile agents and distributed intelligent agents for network management
- Protocols for dynamic re-addressing

Force Protection Study

159




Desirable Network Attributes

Robust (from internal breakdowns and external attacks or interference)

Secure (LPI / LPD)

Reconfigurable (ad hoc)

Latency

Power consumption

Human interfaces

Maintainable

Force Protection Study

160




Network High-Value Targets

Access points	IT personnel
Antennas	Maintenance folks
Software	Operators
Routers	Others with access to network
Fiber, wires	Power sources
Sensors	Interfaces between internal systems and external networks
Radios, repeaters	Fixed or mobile relays or facilities
GPS (as used for networks)	In-country assets used to support networks

Force Protection Study

161




Threats to Networks

Electromagnetic interference

- Wired and wireless
- Intentional and unintentional

External physical attacks, force / disruption

Soft attacks; disruption, deception, time wasting tactics

Internal software bugs and crashes, being able to detect that cause was internal

Force Protection Study

162




Means of Attack

Insertion of software viruses, bugs, back doors

Insertions of hardware bugs or taps

RF interference

Encryption, authorization, codes and means

Physical destruction of hardware

Physical, psyops on personnel

Deception, delay, confusion

Force Protection Study

163




Network Issues

Attributes of networks

Threat categories

What is being done, both stateside and overseas

Available and future technologies

Use of existing networks in occupied countries when forces are deployed

Force Protection Study

164



Findings (old)



Communications Networks

- Many stovepipe, legacy systems. Unclear how they will interoperate for FCS, CONUS or overseas
- During pre-deployment & deployment & initial ops, unclear what systems FCS will use.
- Policy on using existing comm systems in area of deployment unclear
- Very heavy reliance on contractor IT personnel, both peacetime, deployment, wartime

Force Protection Study

165



Findings (old)



Information Assurance

- Many challenges relating to authentication, encryption, RF interference, spectrum
- Physical protection of routers, fiber, wireless infrastructure, ports, rails, foreign comm systems critical
- Assurance of software – bugs, altered, back doors

Force Protection Study

166



Findings (old)



Data (Knowledge) Management

- Fragmented programs exist, performing critical functions. FP tools needed unclear
- Huge challenge, volumes of data, culling and sorting difficult, CDR needs for FCS
- Issue of where fusion should be done, locally or centralized, will continue to surface
- Not clear how services will work together

Force Protection Study

167



Network Findings



- The Army needs to ensure the Force Protection network during deployment and overseas. Consider two timeframes: 2004 and 2011.
 - Information assurance
 - Physical protection
 - Information management (secondary)
- There appears to be significant research in three network force protection areas:
 - Protection of RF Links. This includes the protection of data through the use of authentication and encryption.
 - Physical Protection of Hardware. This includes the physical protection of radios, self-destructing crypto gear, etc.
 - Physical Protection of Nodes. This includes perimeter security for command centers, etc.
- Future Information Technology needs will only continue to grow with "network-centric warfare." One FCS approach is that there will be no real "IT MOS," rather all soldiers will need a basic set of IT skills. This basic set of IT skills is yet to be well-defined, and it is unclear how much training will be required. In addition, it is likely that contractors and host nation IT personnel will continue to be required, possibly even at higher demand levels. Countering insider threat against hardware and software needs to be addressed as a Force Protection need.

Force Protection Study

168




Network Findings

- But, several other areas remain especially challenging:
 - The intrinsic dynamics of the network itself (control parameters), rather than the actual physical link, continue to be very vulnerable. Commercial denial-of-service attacks, as on the recent Microsoft DNS servers, are examples.
 - Sensor fusion is extremely challenging. If done at the lowest level, raw data is lost, if done at a higher level, large data pipes are required. A balance must be struck, and this balance will greatly influence the network data bandwidth requirements. It is likely much more difficult to protect a network that is higher data bandwidth and more fragile, versus a lower data bandwidth yet more robust.
 - The real bandwidth needs for Force Protection is a difficult challenge and has not been accurately accessed to date. Relating to this issue, DoD spectrum shortage is likely to become even worse. Force protection of spectrum may be key.
 - Use of coalition or host nation infrastructure for Force Protection IT is unclear; as in recent use of Kuwait internet to support DoD in Iraq.

Force Protection Study

169




Technology Solutions Outline

- Overview
 - Introduction
 - Findings and Conclusions
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids
 - Case Study Technologies
 - Recommendations
- What can we do immediately?
- Technology Team Reports
 - Sensors
 - Weapons and Survivability
 - Automation and Robotics
 - Networks
 - Decision Aids

Force Protection Study

170




Decision Aids Technology for Force Protection

- Subpanel to Technology panel of the ASB Force Protection Study 2003
- Members:
 - Gary Glaser
 - Mark Hofmann
 - Prasanna Mulgaonkar
 - Reed Mosher
 - John Reese - Lead
 - Paul Tilson
 - Jack Wade
 - Randy Woodson

Objective: Evaluate existing and emerging technologies that could make a significant contribution to the US Army Force Protection needs

Force Protection Study

171




Leverage

- Decision Aids provide leverage way beyond their cost if they can be correctly implemented
 - 9/11 (and most other attacks on Forces and Facilities) shows data were available but the data could not be turned into the correct information and knowledge to allow appropriate decision making and much of the decision support was not available.
- The Technologies to derive the appropriate knowledge and support command Decision Making are powerful and will become increasing powerful over the next 20 years

Knowledge is power if, and only if, it can be used to make correct decisions in a timely manner

Force Protection Study

172



Decision Aids Report



- Summary of Force Protection needs with respect to top Commanders' decision making
 - From the requirements panel
- Identification of specific decision criteria (inputs, outputs, algorithms) relevant to the problem
 - D.A. Technology that can support the commander in developing Force Protection planning and assessments in advance.
 - D.A. Technology that can support the commander in assessing the risks of attacks, the types of attacks, and the strategic and tactical warning of attack.
 - D.A. Technology that can support the commander as attacks are imminent or in progress to reduce the impact on his force, alert others of the attack characteristics, and support his response COA.
- Identification of available Decision Aid technology and future Decision Aid technology with timelines for TRL 6
- Assessment of Decision Aid technology impact on the Force Protection requirements will be developed primarily by the analysis panel
- Findings, Conclusions, and Recommendations for Decision Aid Technology implementation in the Force Protection solutions also cover synergistic impacts on other Army Missions
- Overview cost and schedule roadmap for Decision Aid technology integration into Army systems and operations

Force Protection Study

173



Scope of Decision Aids



- All information processing from FP
 - Fusion of more than one sensor set
 - To include Fusion of Multi_Ints
 - Specific Function sets (Perimeter, Personnel ID, Surveillance detections, ...)
 - Network allocation beyond technical communications allocation algorithms
 - Development of FP integrated data bases
 - Facilities, FP Packages, Weapon Effects,
 - Threat characteristics and current threat assessments
 - Allocation algorithms for FP assessments of
 - Facilities (fixed and mobile)
 - Complex environments (Weather, Terrain, Political, ...)
 - Intelligence analysis and collection management
 - Operations analysis and assessment tools
 - Survivability and lethality options developments
 - Analysis of likely threat attack locations (and ambush possibilities)
 - Interaction with other Echelons concerning FP options, threats and COAs
 - Peer group
 - Down Echelon / Up Echelon
 - Experts and centers of excellence

Force Protection Study

174



Weather & Building Decision Aids



- Weather essential to:
 - Sensor deployments, evaluation, and dynamic coverage assessments
 - Lethal and non-lethal weapon coverage and effectiveness assessment
 - Dynamic assessment of sensor performance in real-time as weather, threat, situation evolves
 - Integration of weather into other decision aids
 - Threat behavior
 - Intelligence fusion
 - Technical Threat Characteristics
 - IPB
 - Trafficability
 - Site planning
- NIOSH Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks (May, 2003)



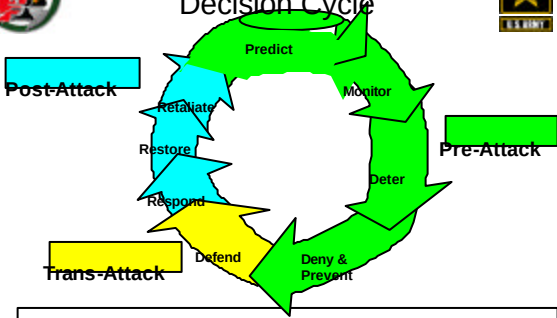

Force Protection Study

175



Force Protection Continuum Decision Cycle





Force Protection is clearly more than defense

Force Protection Study

176



Traceability to Threat & Operations Requirements



CONUS Base Operations Goals and Priority Requirements

- Goal: Maintain maximum operational capability of base with minimum casualties
- Priority Requirements:
 - Forecast attack in a timely manner: what, when, and where
 - Cue, localize, verify, and interdict attacks with community law enforcement
 - Secure the perimeter and control access
 - Harden facilities and protect personnel
 - Employ decoys and countermeasures
 - Prevent contamination of supplies
 - Keep threats beyond their effective range with community law enforcement
 - Preclude future attacks using all appropriate means

Intelligence Fusion Weather Decision Aids Structures Decision Aids Perimeter Decision Aids Personnel ID Decision Aids:

OCONUS Small Installation Goals and Priority Requirements

- Goal: Maintain maximum operational capability of small installation with minimum casualties and friendly force commitment
- Priority Requirements:
 - Forecast attack in a timely manner: what, when and where
 - Integrate in local community to gain intelligence
 - Create multiple dynamic perimeters to control access
 - Maintain assured secure communication
 - Harden small installation and protect personnel
 - Employ decoys and countermeasures
 - Introduce unpredictability into routine operations
 - Prevent contamination of supplies
 - Keep threat beyond their effective range

Intelligence Fusion Terrain Decision Aids Weather Decision Aids Personnel ID Decision Aids Mentoring/Collab. Aids:

Small Teams Goals and Priority Requirements

- Goal: Maintain maximum operational capability of individuals and small teams with minimum casualties
- Priority Requirements:
 - Forecast attack in a timely manner: what, when, and where
 - Cue, localize, verify, and interdict attacks
 - Integrate in local community to gain intelligence
 - Maintain assured secure communication
 - Harden transit means and protect personnel
 - Introduce unpredictability into routine activities
 - Provide rapid combat identification (CRI) of possible threat

Intelligence Fusion Perimeter Decision Aids Weapon Effects Aids Sensor Placement Aids UGS system Aids Chem Bio Aids:

Force Protection Study

177



Identified Technology



- Threat Behavioral I&W Mark
- Weather support Paul
- Terrain Support Prassana
- Structures and Vulnerabilities Reed
- Mobile Base Structures and Vulnerability Reed
- UGS systems and analysis Prassana
- Intelligence Fusion Gary
- Personnel Identification Prassana
- Perimeter Security John
- Chem. Bio Identification and dispersion Steve
- Modeling and simulation of effects and environments Ira
- Peer Collaboration Mark
- National Systems Tasking and Dissemination Paul
- Remote mentoring and Collaboration Mark
- Counter Manpads John
- AT/FP portal Jack
- "Red" teams support Jack
- Multi-sensor fusion Gary
- Geo-reference support tools for FP (SimCity) Stu
- Immune Building System Steve
- Decision Related Structures Jack

Force Protection Study

178



Decision Aid Impact on FP



- Commanders Decision Support System (DSS) elements**
 - Threat Behavioral I&W Mark 6.1& 6.2
 - Weather support Paul 6.3 - FOC
 - Terrain Support Prassana 6.1 - FOC
 - Structures and Vulnerabilities Reed 6.3 FOC
 - Mobile Base Structures and Vulnerability Reed 6.2 - 6.3
 - UGS systems and analysis Prassana 6.1 - 6.3
 - Intelligence Fusion Gary 6.1 - FOC
 - Personnel Identification Prassana 6.1 - FOC
 - Perimeter Security John 6.1 - FOC
 - Chem. Bio Identification and dispersion Steve 6.1 - FOC
 - Modeling and simulation of effects and environments Ira 6.1 - FOC
 - Peer Collaboration Mark 6.1 - FOC
 - National Systems Tasking and Dissemination Paul 6.3 - FOC
 - Remote mentoring and Collaboration Mark 6.1 - FOC
 - Counter Manpads John 6.3 FOC
 - AT/FP portal Jack 6.3 - IOC
 - "Red" teams support Jack 6.2 - FOC
 - Multi-sensor fusion Gary 6.1 - 6.3
 - Geo-reference support tools for FP (SimCity) Stu 6.1 - 6.3
 - Immune Building Tool Kit 6.1 - 6.3
 - Decision Related Structures Jack 6.1 - 6.2

undefined - some aspects TRUE now

Force Protection Study

179



DRS Tools



Simulation Technologies

- Agent Modeling
- Discrete Time Modeling

Domain Model

Analysis Technologies

- Metrics
- Formal Concept Analysis
- Combinatorics
- Dynamic Graph Drawing

Force Protection Study

180



The Calculus of Extremely Low Probability Events (Findings)



- Force protection requires commanders to assess risks, impacts, and mitigation costs associated with extremely low probability events
 - We termed these ELP events
- These events can occur over very long time periods, requiring continuous vigilance
- We could not identify any decision aids, computational theory, or tools that allow decision making under such extreme conditions

Force Protection Study

181



Extremely Low Probability Events: Findings(2)



- Decision making in this context is harder because human perception of such low probability, long timeline events is biased
- Why does this matter? Because rarity is a psychological phenomenon—it is what humans experience, not strictly what a formula or algorithm expresses
- Some well-known and critical areas of applied mathematics include Bayesian inference; epidemiology; logistic regression; combinatorial mathematics; sampling theory—formal means of describing assumptions about a population of events. These tools may have applicability for ELP events
- Some well-researched and critical areas of applied psychology which might apply, include sustained vigilance; pattern recognition/primed observation; naturalistic observation; judgment under uncertainty; situational awareness; individual and societal perception of time horizon; learning and memory processes; behavioral causal analysis; cognitive engineering/workload analysis --methodologies for capturing effects of human bias and cognitive limits on acknowledgement of and action on rare-events data

Force Protection Study

182



ELP Events: Conclusions



- Lack of appropriate mathematical tools and decision aids could result in commanders' failure to use available FP technologies, *simply because they cannot accurately assess the risk*
- Without appropriate quantification, it is difficult if not impossible to compare between multiple potential technology solutions
- No adequate cost-benefit analyses can be performed to determine where technology investments are needed

Force Protection Study

183



ELP Events: Recommendations



- We recommend that the Army should task ARL to immediately undertake a study or workshop to define a long term research program in the area of decision aids for ELP events.
- The study should consider at least these five key issues:
 - Memory consolidation
 - Human pattern recognition
 - Behavioural scripts
 - Quantification of expectations
 - Evaluation of risks
- The study should include experts in human cognition, statistical methods, and reach out to the insurance industry experts

Force Protection Study

184



An extensive number of FP Developments – an Example



USAF and USMC Programs
Performance Specification

for

Tactical Remote Sensor Systems (TRSS)

Advanced Air-Delivered Sensor (AADS)




Force Protection Study

185



Decision Support System- Force Protection



Threat Behavior Applications	Weather Support Applications	Structures Vulnerability Applications	UGS Systems and Analysis Applications	Intelligence Fusion Applications
Chem-Bio ID & Dispersion Applications	Terrain Support Applications	Mobile Structures Vulnerability Applications	Personnel Identification Applications	Peer and up/down Collaboration Applications
Counter Weapons (ManPads, Mines) Applications	Red Team Support and Exercise Applications	M&S of effects and environment Applications	Perimeter Security Applications	National / Joint Systems Tasking & CM Applications
Countermeasures & Survival Applications	Urban Terrain – Sim City like Applications	Immune Building Toolkit Applications	AT/FP Portal Applications	Multi Sensor Fusion applications
??	??	Vehicle -road vulnerability Applications	UAV, UGV systems Applications	Remote Mentoring Applications

Force Protection Study

186



DSS Integration Application



A Commander's Tool
Useable all FP phases

Integrated Into a
Services based Architecture

Maintained by A Center Of Excellence for FP

Compatible with

- GIG
- Army C3
- Obj. Force Systems / FCS

Supports FP training and Exercise (Red Team)

Threat Behavior Applications	Weather Support Applications	Structures Vulnerability Applications	UGS Systems and Analysis Applications	Intelligence Fusion Applications
Chem-Bio ID & Dispersion Applications	Terrain Support Applications	Mobile Structures Vulnerability Applications	Personnel Identification Applications	Peer and up/down Collaboration Applications
Counter Weapons (ManPads, Mines) Applications	Red Team Support and Exercise Applications	M&S of effects and environment Applications	Perimeter Security Applications	National / Joint Systems Tasking & CM Applications
Countermeasures & Survival Applications	Urban Terrain – Sim City like Applications	Immune Building Toolkit Applications	AT/FP Portal Applications	Multi Sensor Fusion applications
??	??	Vehicle -road vulnerability Applications	UAV, UGV systems Applications	Remote Mentoring Applications

Force Protection Study

187



The situation today

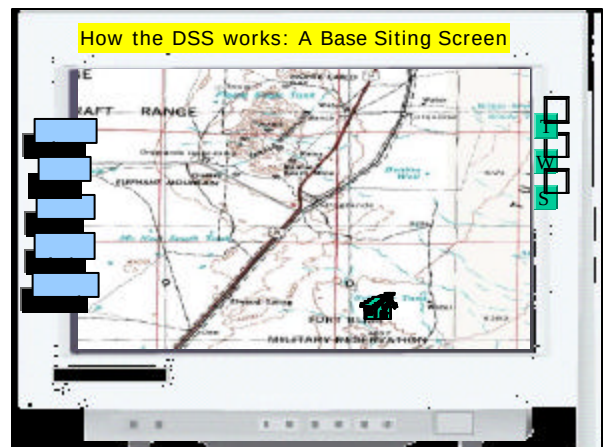
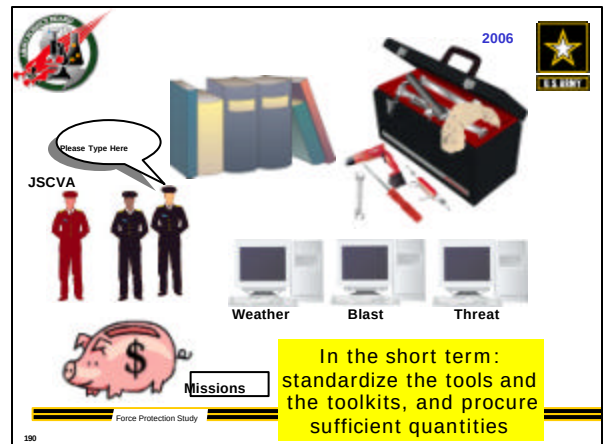
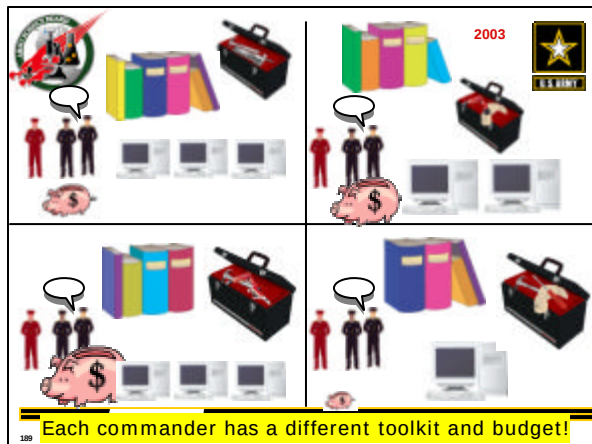


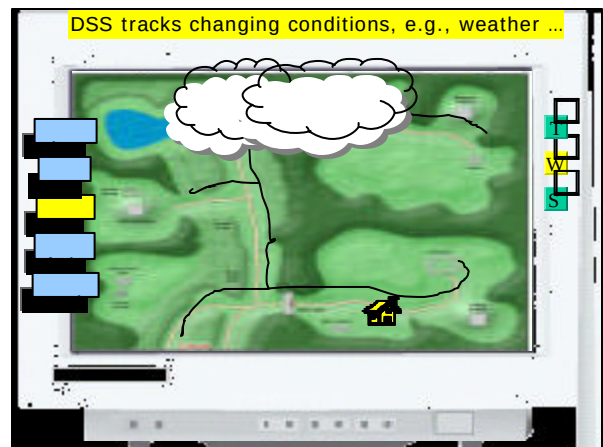
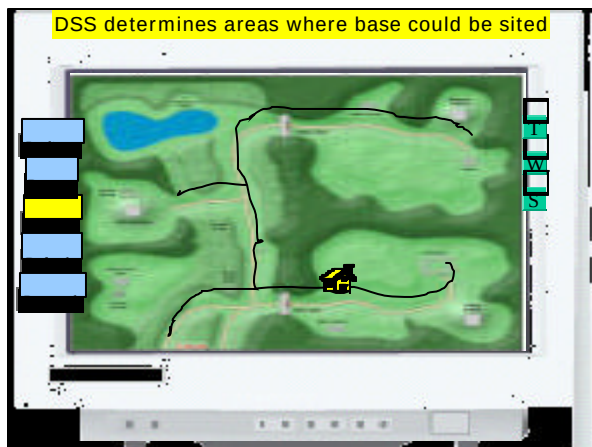
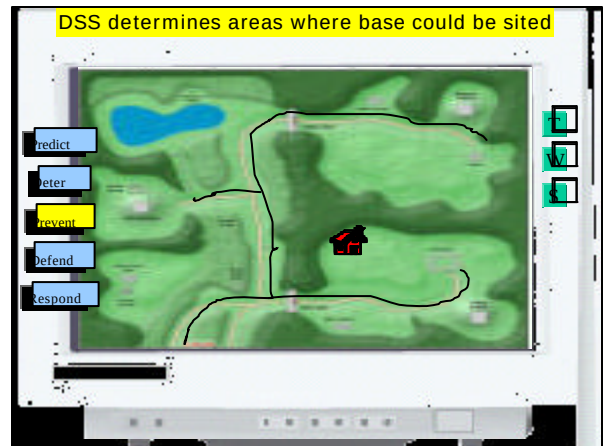
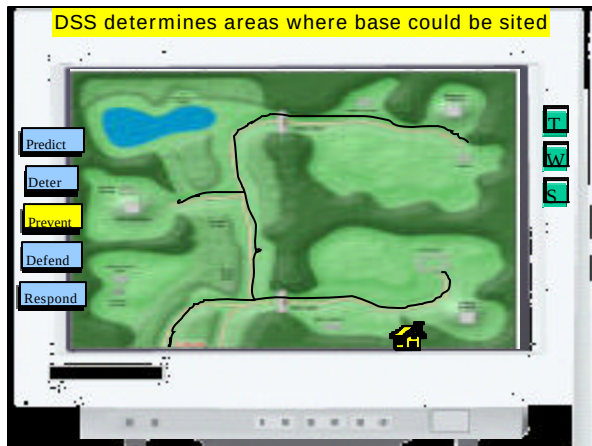


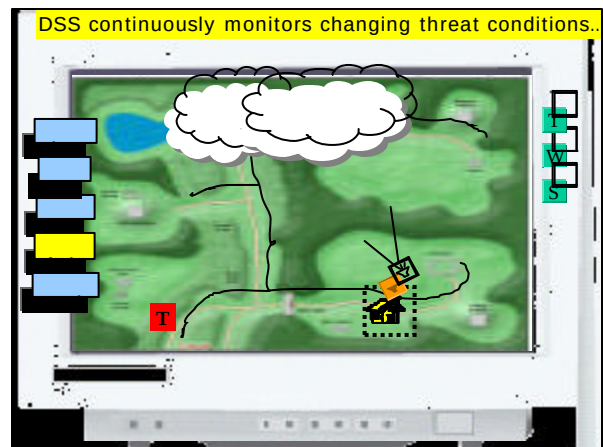
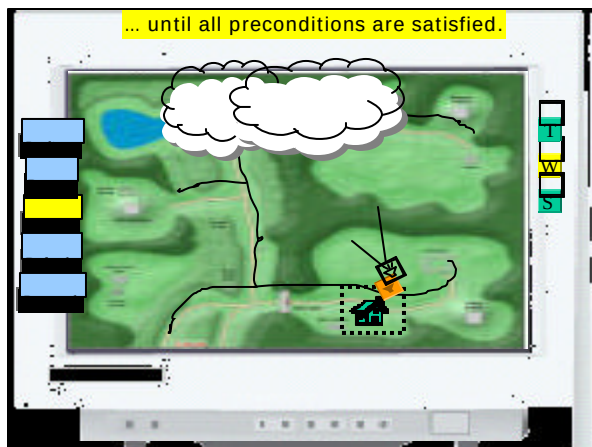
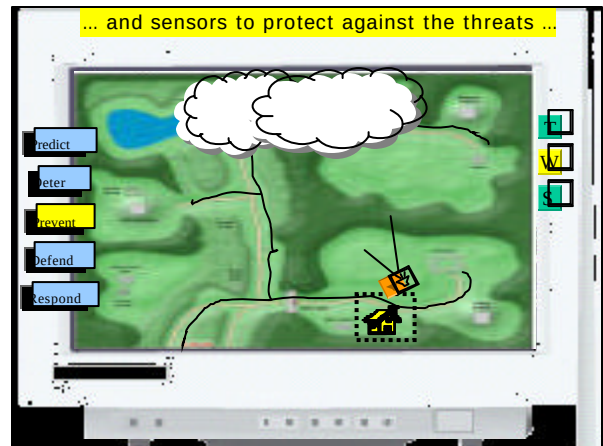
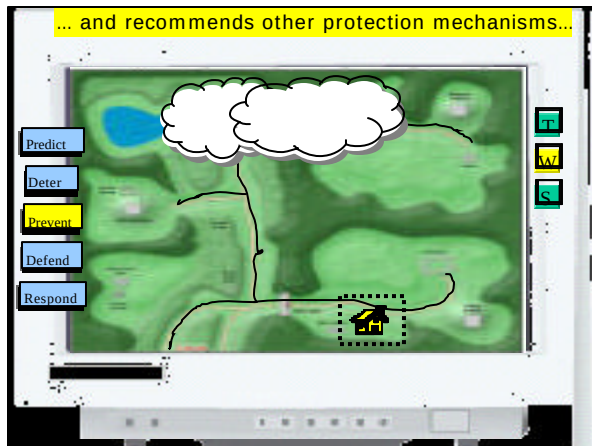
Each commander has a collection of force protection tools, decision aids, and a finite budget

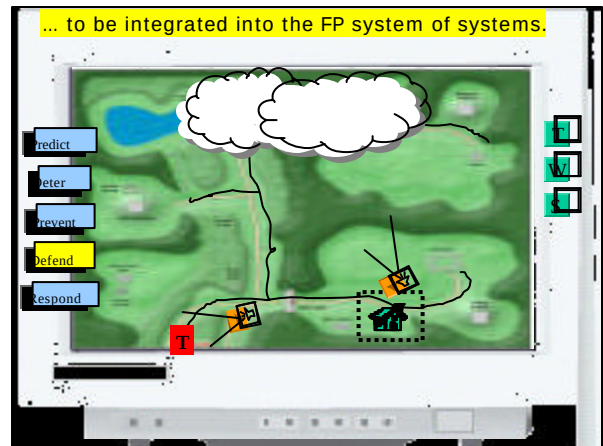
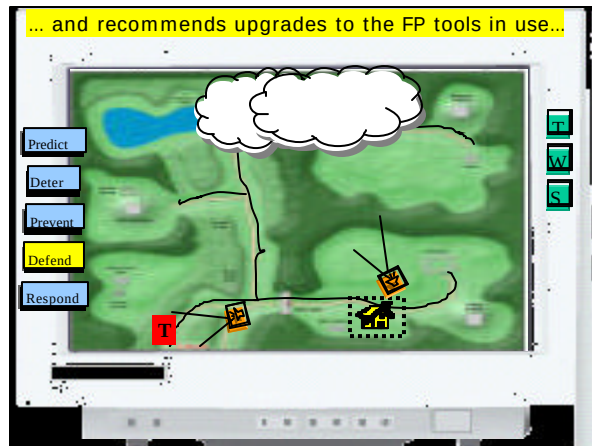
Force Protection Study

188









Convoy Protection – Commander's DSS

Predict Attacks

- Threat behavioral I&W develop likely attack modes
- Weather support use with terrain and M&S to predict areas of vulnerability
- Terrain support determine areas where attacks could occur vs. weapon
- Structures and vulnerabilities N/A
- Mobile base structures and vulnerability N/A
- UGS systems and analysis determine deployment to reduce threat access
- Intelligence fusion integrate all sensor data and reports over route
- Personnel identification provide ID of personnel in route areas
- Perimeter security mobile security UGS, UAV, Intel area denial, etc. trade offs
- Chem bio identification and dispersion assess route vulnerability, critical areas, weather
- Modeling and simulation of effects and environments assess route vulnerability weapons PK
- Peer collaboration - review other convoy ops within area of interest and beyond
- National Systems Tasking and Dissemination assess sync and utility of national coverage
- Remote mentoring and collaboration review with experts protection options
- Counter Manpads determine footprints and PK on route for UAV, helicopter
- AT/FP portal assess how to allow vehicles to exit enter compounds w/o delays
- "Red" teams support - use red teams to evaluate plans and input risks
- Multi-sensor fusion - prepare "optimum" sensor deployment options
- Geo-reference support tools for FP (SimCity) model routes and route options / risks

Force Protection Study

203

Convoy- Predict Attack

Threat Behavior Applications	Weather Support Applications	Structures Vulnerability Applications	UGS Systems and Analysis Applications	Intelligence Fusion Applications
Chem-Bio ID & Dispersion Applications	Terrain Support Applications	Mobile Structures Vulnerability Applications	Personnel Identification Applications	Peer and up/down Collaboration Applications
Counter weapons (ManPads, mines) Applications	Red Team Support and Exercise Applications	M&S of effects and environment Applications	Perimeter Security Applications	National / Joint Systems Tasking & CM Applications
Countermeasures & Survival Applications	Urban Terrain - Sim City like Applications	Immune Building Toolkit Applications	AT/FP Portal Applications	Multi-Sensor Fusion applications
???	???	Vehicle -road vulnerability Applications	UAV, UGV systems Applications	Remote Mentoring Applications

Blue = Critical DA

Green = Necessary DA

Yellow = Useful DA

Red = Not required DA

Force Protection Study

204

Convoy Protection – Commander’s DSS

- Deter attacks
 - Threat Behavioral I&W Develop likely attack modes
 - Weather support Use with Terrain and M&S to predict areas of Vuln.
 - Terrain Support Determine areas where attacks could occur vs. wpm
 - Structures and Vulnerabilities N/A
 - Mobile Base Structures and Vulnerability N/A
 - UGS systems and analysis Determine deployment to reduce threat access
 - Intelligence Fusion Integrate all sensor data and reports over route
 - Personnel Identification Provide ID of personnel in route areas
 - Perimeter Security Mobile security UGS, UAV, Intell. Area Denial, etc Trade offs
 - Chem. Bio Identification and dispersion Assess route Vuln, critical areas, weather
 - Modeling and simulation of effects and environments Assess route vuln. weapons PK
 - Peer Collaboration Review other convoy ops within area of interest and beyond
 - National Systems Tasking and Dissemination Assess sync and Utility of Nat. coverage
 - Remote mentoring and Collaboration Review with experts protection options
 - Counter Manpads Determine footprints and PK on route for UAV, Helicopter
 - AT/FP portal Assess how to allow vehicles to exit enter compounds w/o delays
 - “Red” teams support Use red teams to evaluate plans and input risks
 - Multi-sensor fusion Prepare “optimum” sensor deployment options
 - Geo-reference support tools for FP (SimCity) Model routes and route options / risks

Force Protection Study
205

Convoy- Deter

Threat Behavior Applications	Weather Support Applications	Structures Vulnerability Applications	UGS Systems and Analysis Applications	Intelligence Fusion Applications
Chem Bio ID & Dispersion Applications	Terrain Support Applications	Mobile Structures Vulnerability Applications	Personnel Identification Applications	Peer and up/down Collaboration Applications
Counter weapons (Manpads, Mines) Applications	Red Team Support and Exercise Applications	M&S of effects and environment Applications	Perimeter Security Applications	National / Joint Systems Tasking & CM Applications
Countermeasures & Survival Applications	Urban Terrain – Sim City like Applications	Immune Building Toolkit Applications	AT/FP Portal Applications	Multi-Sensor Fusion Applications
???	???	Vehicle -road vulnerability Applications	UAV, UGV systems Applications	Remote Mentoring Applications

Force Protection Study
206

Different Phases of Convoy Planning Utilize DA Applications Differently

Predict

Threat	Weather	Structures	UGS	Intell
Chem Bio	Terrain	Mobile	Personnel	Peer
Counter weapons	Red Team	M&S	Perimeter	National
Countermeasures	Urban Terrain	Immune Building	AT/FP Portal	Multi-Sensor
???	???	Vehicle	UAV/UGV	Remote

Defend

Threat	Weather	Structures	UGS	Intell
Chem Bio	Terrain	Mobile	Personnel	Peer
Counter weapons	Red Team	M&S	Perimeter	National
Countermeasures	Urban Terrain	Immune Building	AT/FP Portal	Multi-Sensor
???	???	Vehicle	UAV/UGV	Remote

Respond

Threat	Weather	Structures	UGS	Intell
Chem Bio	Terrain	Mobile	Personnel	Peer
Counter weapons	Red Team	M&S	Perimeter	National
Countermeasures	Urban Terrain	Immune Building	AT/FP Portal	Multi-Sensor
???	???	Vehicle	UAV/UGV	Remote

Prevent

Threat	Weather	Structures	UGS	Intell
Chem Bio	Terrain	Mobile	Personnel	Peer
Counter weapons	Red Team	M&S	Perimeter	National
Countermeasures	Urban Terrain	Immune Building	AT/FP Portal	Multi-Sensor
???	???	Vehicle	UAV/UGV	Remote

Deter

Threat	Weather	Structures	UGS	Intell
Chem Bio	Terrain	Mobile	Personnel	Peer
Counter weapons	Red Team	M&S	Perimeter	National
Countermeasures	Urban Terrain	Immune Building	AT/FP Portal	Multi-Sensor
???	???	Vehicle	UAV/UGV	Remote

Force Protection Study
207

Findings

- Force Protection Decision Aids (software applications) are widely available to the Commander for supporting FP decisions.
- Numerous FP DAs are under development by the Army, USAF, USN, USMC, DARPA, DTRA, TSWG, DHS, NIH, NIOSH and others.
- The commanders are handicapped by having a large number of independent applications. No integrating Force Protection Decision Support System (DSS) is being developed to provide the commander a single support system to support Force Protection decision needs.
- Selection of the applications to include in a DSS would require an assessment of the large number of “competing” applications to provide a development focus on the “best of breed”
- No single organization exists to develop, maintain, train, and support current decision aids or future FP integration of multiple DAs
- Force Protection often is associated with low probability events that occur over long time frames
- Decision aids are used in different ways and mixes for planning, protecting, responding, and retaliating.

Force Protection Study
208



Conclusions: Need for an Integrated Decision Support System for the Commander



- Individual decision aids (often not the "best") provide significant capability to support Commander in all three phases of FP
- The commander is required to accomplish optimization and tradeoffs across the individual decision aids with little support.
- A decision support system which integrates the "best" individual decision aids is required to support the Commander with the capability to determine the best FP COA and implementations
- Force protection decision support applications need to be hosted on the current and planned Army Strategic and Tactical IT structure (Architectures for networks, standards, equipments could support the DSS application)

Force Protection Study

209



Conclusion (Cont'd)



- The development and improvement of Force Protection decision aid applications will continue to improve the available support, but it is essential to better focus the development to reduce the number of duplicative applications (e.g. Blast assessment)
- Specific areas of emphasis for DAs need to include
 - Intelligence and information fusion
 - Decision related structures
 - Integrated decision system tradeoffs applications
 - Threat behavioral evaluations
 - Low Probability, infrequent events
 - DSS must address all phases of FP
- Security and multi-level security is an important aspect of a comprehensive decision support system



Force Protection Study

210



Recommendations



- Army RDECOM (SOSI/ARL) develop an Integrated Force Protection Decision Support System (DSS) for the Commander
 - Many individual Decision Support Technologies
 - Individual Technologies provide significant capability to support Commander in all phases of FP (defend, preempt, deceive, etc.)
 - However, it is currently difficult to accomplish cost benefit tradeoffs (to improve the DSS) across the individual decision aids and with no plan to solve this in the future
 - A decision support system which integrates the individual decision support systems is required to support the Commander with the capability to determine the best FP COA and implementations

Force Protection Study

211



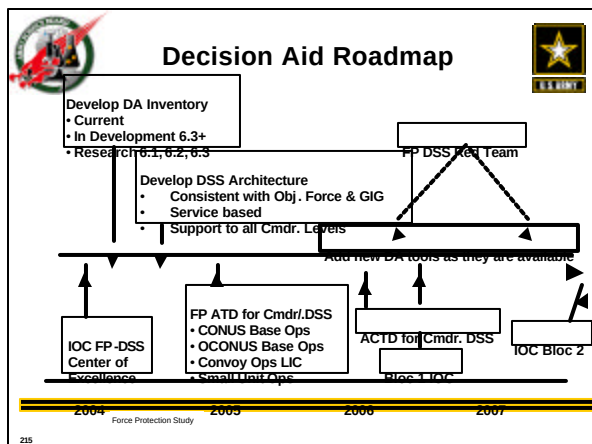
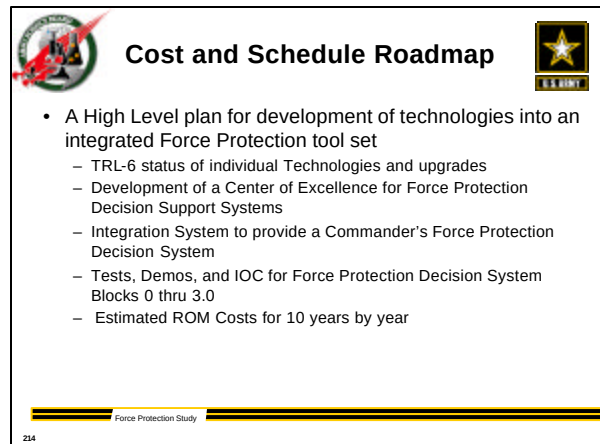
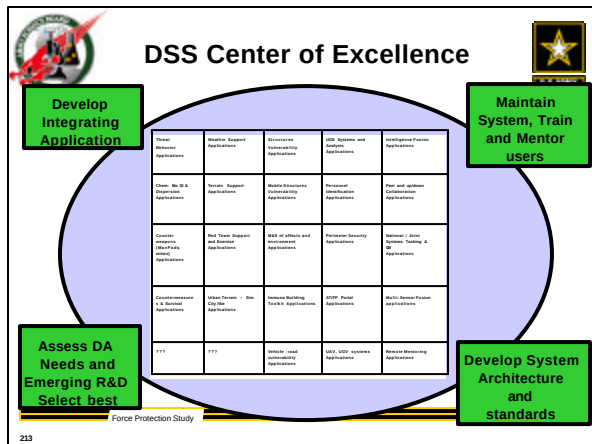
Recommendations for Decision Aid Technology Implementation



- Assess Decision Aids systems which should be accomplished
- Accomplish Integration of the aids into a decision support tool for the Commander
- Establish a center of excellence to:
 - Integrate the tools
 - Maintain the tools and update as required
 - Mentor the commanders and provide a focal point for real-time support
- Establish a clear interface to Threat Intelligence data and both Strategic and Tactical Threat I&W

Force Protection Study

212



Sensor Section

ASB Technology for Force Protection

2003 Summer Study

by Steve Kornguth - Chair

Sensors Section Technology Panel

Groups and Persons Visited

July 24 2003

BG Stephen Reeves Joint Program Executive Office Chemical Biological Defense

ITF6 list of B agents

Dr. David Cullins JPEOCBD

Dr. Ned Covington-Army Acquisition

Dr. Amy Alving- DARPA-SPO Director

Dr. Jonathon Phillips-DARPA

Dr James Southerland-Homeland Security C2 ACTD

Dr. James Valdes-ECBC (formerly SBCCOM)

MG Doesburg-ECBC

Dr. Joseph Rocchio DD Sensors and Electronic Devices ARL

Dr. Richard Taylor IR Countermeasures ARL

Dr. Kirkman Phelps Joint Service Materiel Group ECBC

Dr. John Fedrig Sensors DTRA

Dr. Jim Gillespie Sensors ARL

Dr. George Simonis EO Smart Sensor ARL

Dr. Harles Gundiff Sniper Detection ARL

Dr. John Eicke Networked

FORCE PROTECTION NEEDS WITH RESPECT TO SENSORS

Detect and Identify

This section addresses sensors for detecting potential threats to deployed forces in the context of Force Protection. The list below identifies the sources of potential threats to the mounted and dismounted soldier and platforms. While each of these threat situations will be addressed in the text, primary attention will be given to the detection and identification of biological warfare (BW) agents. The focus is on sensors for BW agents because such sensors are absent from almost all military platforms and the dismounted soldier. Sensors that enable perimeter protection in a cost-effective manner are also required. The guidance provided at the start of the summer study recommended that focus be placed on the greatest need to mitigate the following catastrophic circumstances:

- Biological (100 agents, Australia Group)
- Chemical agents (60 agents)
- Industrial chemicals
- Radiological/Nuclear materials (threats, hospital sources, facilities, civil source)
- HX (unexploded ordnance)
- Dismounted (snipers, IED, troops, non-combatants)
- Vehicles (tanks, APC, cars, ambulances)
- Individuals (friend/foe, children, etc.)
- Aircraft [Unmanned aerial vehicles (UAV), civilian]
- Booby traps, mines, and UHX and HX Storage
- Perimeter breach
- Quantitative measure of loss of vigilance and situation awareness (human performance)

The General Approach of the study group is:

- A system of systems approach is mandatory. The FCS is viewed as an organism with the sensors being the peripheral nervous system providing all environmental awareness to the organism.
- System is a set of tools at nodes and across networks.
- Spiral development as proposed for computational and network components with platform acquisition flexibility.
- A 2010 goal with 2004 reality (at least two time frames for systems approach).

Force Protection requires an integrated system of systems approach to ensure the viability of the forces and support structure. Force Protection must be pervasive in both CONUS and OCONUS. The key elements will include:

- Investment in Force Protection should be balanced for mission effectiveness, cost, etc.
- Protection for people, equipment, and facilities.
- Force Protection elements baselined with legacy or objective force capabilities.
- A systems of systems approach. The rate of change (delta) in technology equipment is required to ensure this approach.
- Force Protection system is an evolving capability.
- Responsibility/risk management for the commanders.
- The threat responds to the evolving Force Protection systems.
- A suite of tools is integrated into a common architecture (re-configurable) Reserve forces and support facilities need special attention.
- The experiences of the 507th Maintenance unit in Iraq on March 21-23, 2003 present a need to consider fatigue as major factor in mission accomplishment. Evoked potentials and q-t cardiac interval measures are two technologies that have capability to determine loss of vigilance unobtrusively

Current Paradigm

The Sensor Subpanel proposes to change the current paradigm of Force Protection within the Army. The current paradigm is based on:

- Stove-piped responses
- Individualized communication systems

New Paradigm

- Integrated sensor system that fuses data, presents knowledge in a comprehensible iconographic display (e.g., TADMUS)
- Integrated sensor alert system that detects all threat events with minimal false positive/negative events
- A seamless integrated communications capability that converts data to actionable information
- Novel pre and post event treatments

Available new technology allows the Army to move away from a stovepipe approach for sensors systems toward a system that has three main thrusts:

1. Use multi-array sensor systems with embedded archival local data sets and local data fusion.
2. Fuse data elements for each component into an iconographic display (TADMUS model).
3. Incorporate the Sensor Systems into a system of systems matrix with interchangeable nodes.
4. Network couple Force Protection with the organic strengths of the deployed forces.

5. Networked assessment of vigilance of Force in non-combat environments by unobtrusive physiological measures including evoked potentials and q-t cardiac interval. Both require PDA size devices and low power.

The emerging multi-array sensor system will support network centric warfare at the local and larger levels. The basis of the sensor system will be to provide excellent intelligence that is readily presented to the commander in a comprehensible, iconographic format. The multi-array sensor component of Force Protection requires an integrated system of systems approach to ensure the viability of the forces and support structure.

Specific Sensor Criteria Relevant to Detect Biological and Chemical Threats

Current Capabilities - Biological

The current biological defense capabilities are based on:

- Known genomic sequences of pathogenicity islands and threat agents
- Known antigenic determinants of critical agent antigens involved in binding target
- Separate detectors for each threat agent
- Traditional based vaccines, antibiotics, and antivirals
- Traditional post-event care delivery

Gaps in Technology for Biothreat Sensors

The following technology gaps exist:

- Small, lightweight, energy-efficient platforms that incorporate sample capture, binding materials and transducer (sensor), data fusion
- Reliable sources of critical reagents
- Continuously operating, self-regenerating sensor platform for 24/7 operating for weeks in autonomous, robotic mode

Observations for Biothreat Sensors

The study group made the following observations:

- All the gap issues are related to the engineering of field ready systems; interfacing biotechnology with platforms
- Many basic science issues have demonstrated solutions
- Systems integrations that provides fused actionable information for incident command are needed

System of Systems Approach

Integrated Multi-array Sensor

The multi-array sensor system detects all threat agents with minimal false positives/negatives. The requirements of such a system include:

- Seamless integrated communications capability converting data to information
- Small, lightweight, energy efficient platform for sample capture, binding, transduction, and fusion
- Reliable source critical reagents
- Continuously operating, self regenerating sensor platform 24/7 for weeks
- Autonomous, robotic operation
- Integrated data processing/reduction

Sensor systems that detect levels of chemical agents, radiological agents, pathogenic bacteria, viruses, or toxins in the environment will be essential elements of FCS platforms. The sensor systems' three levels of analysis will be 1) continuous sensing for signatures of airborne radiological, CW or BW threat agents in the environment with no need for consumables; 2) the initiation of more detailed tests for threat agent based on comprehensive and redundant arrays if the continuous sensor (1) is triggered; and 3) periodic human monitoring if exposure is suspected to have occurred in order to implement countermeasures.

Sensor Technology that can Support the Commander

Advance Development of Force Protection Plans and Assessments

- Deployment (hand, scatter, UAV/unmanned ground vehicle (UGV), stationary, soldier mounted, vehicle)
- Environmental sampling
- Direct (air, water, soil)
- Passive [optonic, long wave infrared (LWIR), radio frequency (RF), sound seismic]
- Active (RF, acoustic, LIDAR)
- Calibration (background/archival data)
- Change detection
- Data reduction/Local fusion
- Classification/Iconic display
- Status (sensor lifetime)
- Redundancy (multi-array for validation of false positive/negative)

Risk Assessment

To assess Risks of Attacks, Types of Attacks, and Strategic and Tactical Warnings of Attack, the following tools are used:

- -Calibration (background/archival data)
- -Change detection
- -Data reduction/Local fusion

- -Classification/Iconic display

Reducing Attack Impact

When attacks are imminent or in progress, to reduce the impact, alert others of the attack characteristics, and support response course of action (COA), the following tools are used:

- Calibration (background/archival data)
- Data reduction/Local fusion
- Classification/Iconic display
- Redundancy (multi-array for validation of false positive/negative)

UNOBTRUSIVE MEASUREMENTS OF PHYSIOLOGICAL MARKERS AS PREDICTIVE INDICATORS OF HUMAN PERFORMANCE IN STRESS AND COMBAT

The identification of physiological and biochemical markers that provide quantitative information regarding performance decrement is the goal. Unobtrusive monitors for these early warning markers will increase the likelihood of effective performance and reduce the risk of catastrophic failure.

Recent advances in the behavioral sciences, in neurophysiology, biochemistry, medical imaging and ergonomics provide the opportunity for developing early indicators of threat situations relating to human performance.

The development of unobtrusive monitors of human performance is a major goal and benefit of the proposed investigation. Use of these monitors on an ongoing basis, will provide feedback on an individual and systems basis as the organizational demands change or as crisis situations emerge at low and high vigilance states. A matrix correlating stressors with quantitative physiological measures is shown in Table 1.

Deliverables:

- 1) A miniaturized microelectrode based data acquisition, analysis and simulation system incorporated in a smart helmet for evoked potential determination and into multifunctional clothing for interbeat interval determination.
- 2) The correlation of objective physiological measures with performance capabilities in non-stressed and stressed environments.

- 3) The novel application of probabilistic techniques for precursor analysis to assess the utility of new countermeasures in extending high level performance.

INTRODUCTION

The primary focus of this report is to protect US forces in garrison and en route during deployment. The protection must extend to supply chains, small rear action forces, and the safety of immediate families in the continental United States (CONUS). The specific issues include perimeter protection; force protection in urban areas during peacekeeping activities; and rear area security/protection of humans. The locations involved include A/S, Point of Entry and Point of Departure, Initial Staging Bases (ISB), and intra-theater lift.

Problem: This section is concerned with new and emergent technologies to protect our forces from biological threats, chemical agents, toxic chemicals, radiological and nuclear hazard materials, unexploded ordnance, threat vehicles (ground and air), hostile persons, and booby traps (including mines). The role of fatigue in recent events in Afghanistan and Iraq (opportunistic attack on the 507th on March 23, 2003) emphasize the need to assess quantitatively state of vigilance of forces. From a biological defense perspective, the forces require protection from contamination by aerosol, ingestion of contaminated food or water, and exposure to infected persons in the garrison area. Additionally, fuel supplies must be protected from being fouled by microorganisms. The emergent threat from the production and potential use of biological and chemical weapons of mass destruction (WMD) in the Third World (e.g., Afghanistan, Iraq) has increased our focus on the development of sensor systems for these WMDs.

Approach: The sensor section will address the current capabilities in each of the areas as follows: biological threat, chemical threat, radiological/nuclear threat, mines and unexploded ordnance, vehicle platforms (ground and airborne), artillery/munitions, hypervelocity projectiles, human threats (snipers, suicide bombers, pathogen-infected human sources).

This report places emphasis on biological agent detectors and identifiers because of the absence of such detectors on almost all military platforms as well as on the dismounted soldier. There are two principal biological/chemical agent detection systems: point and standoff. The point detectors and identifiers come in intimate contact with the threat agent and recognize a molecular aspect of the agent. The standoff detectors do not come in contact but rather are identified by a spectral absorption characteristic or reflective characteristic of the agent. Standoff biological detectors take advantage of the restricted particle size of effective biological threat agents. Such agents are in the 0.5 to 15 micron particle range if they are to penetrate the lungs and adhere to the lining of the lungs. While this particle size range differs from that of many particulates in the air, e.g., diesel exhaust, combustion products), there is some overlap with smaller pollen particles that are in the 10-12 micron diameter range. A second property that is useful for standoff detection is the UV absorption range for proteins and nucleic acids, which are the building blocks of biological materials. Such biological materials have strong UV absorbance. At 210, 270-290 nm (proteins) or in the 255-270 range (nucleic acids). High-energy laser sources in these ranges have yet to be developed.

Sensor systems are comprised of an environment sampling component (a material that interacts with substances or conditions in the environment that are of interest), opto-electronic transduction component, data fusion component, archival data set to recognize significant changes in the steady state environment, and iconographic display for alerting military decision makers to a threat state. For applications involving network-centric systems, such as the Future Combat Systems (FCS), the sensor platform must be autonomous and self-regenerating over

extended periods of time. The sensors of interest are those that detect chemical, biological, radiological, and nuclear (CBRN) threats and high explosives in the form of mines.

Our approach transitions from the current stovepiped, single agent/event being detected and identified to a new paradigm that will be integrated, multi-array, and fused. The need is for an integrated sensor system that fuses data, presents knowledge in a comprehensible iconographic display (e.g., TADMUS) and detects all threat events with minimal false positive/negative events. This must be a seamless integrated communications capability that converts data to actionable information combined with novel pre and post event treatments.

Background

In August 1996, LTG Garner tasked the Army Science Board (ASB), through the Missile Defense Issue Group to address and make recommendations on technology programs. Two of the items are:

1. Improved detection and decontamination technologies against biological and chemical agents.
2. Enhanced passive defense policies, procedures, and technologies.

The Chemical/Biological study group from ASB completed their analysis in August 1998 and reported their findings to the US Army Space and Missile Defense Command in September 1998. The study group analyzed seven key areas:

1. Agent Detection and Identification
2. Decontamination
3. Protective Clothing, Equipment, and Shelter
4. Pharmaceutical Countermeasures
5. DOTLMP
6. Post-Engagement Ground Effects Model
7. Diplomacy as a passive defense

The study group discussed nerve agents (sarin, GB), vesicants (sulfur mustards), and blood agents (cyanides). The biological agents they considered included those causing anthrax, brucellosis, plague, q fever, tularemia, Venezuelan (Eastern and Western) Equine encephalitis, viral hemorrhagic fevers (yellow fever and Lassa fever), and toxins including ricin, botulinum, enterotoxin B, and T-2 mycotoxin.

Most Critical Needs

The study group identified the Most Critical Needs as:

1. Increased defense capability against biological warfare (BW) because of the heavy emphasis of the defense community on chemical warfare (CW) agents in the past.
2. Expediting implementation of enzymatic, scavenger, supercritical fluid, foam, ozone, and light technology systems for CW decontamination.
3. Critical capability for anthrax and plague vaccine production.
4. Better integration between Joint Staff and Services in BW/CW responses.

Significant progress has been made on detoxification systems for CW agents (item 2 above) and on integration between Joint Staff and Services on CW responses (item 4 above). Unfortunately, little progress has been realized in Force Protection from BW agents and even modest success in developing a critical capability for anthrax or plague vaccine production has not been achieved by 2002. Currently Bioport is the only facility in the US producing an anthrax vaccine, but this facility has experienced prior difficulties in meeting production goals and needs. The following are secondary findings of the study group relevant to agent detection, identification, and decontamination:

1. Multiple systems are currently required to detect all near term BW and CW agents; no single system was technically possible in 1998.
2. Emphasis on detection was a priority because Force Protection requirements were not fulfilled.
3. Current equipment for personal decontamination (DECON) is primitive and not suited for massed units.
4. DECON solutions were corrosive to equipment.
5. Protective mask design and filter composition for BW agents needed improvement to enhance shelf life and usable time during deployment.

By 2003, multi-array sensor technologies have become a reality for BW agents. These sensors can detect and identify threat agents as point detectors but not as standoff detectors. The ability to produce agent detectors and identifiers that can regenerate functional surfaces and sustain operation for extended periods of time in an autonomous/robotic mode is yet to be realized. The great advance in biotechnology accompanying the sequence of the human genome in 2002 has yielded extensive knowledge regarding the genome of almost all BW threat agents and has offered some understanding of elements of the human genome that predispose to infection. Progress in the other areas identified has yet to be realized; protective clothing for BW and CW agents that permit full field of vision and comfort needed during operational activities are not available. The current 2003 Summer Study of the ASB will consider Force Protection from the threat agents identified by the Australia Group agents in Table 1.

Table 1. Threat Agents for CW and BW

CW Agents	BW Agents
Nerve agents (sarin, GB)	Bacillus Anthracis
Vesicants (sulfur mustards)	Brucella tularensis
Blood agents (cyanides)	Yersinia Pestis
	Francisella tularensis
	Venezuelan Equine encephalitis virus
	Ebola virus

The agents in Table 2 have been studied as potential warfare by nations and have been considered weaponizable.

Table 2. Australia Group Biological/Toxin Warfare Agents

Table 2. Australia Group Biological/Toxin Warfare Agents

Viruses	V1.	Chikungunya virus
	V2.	Congo-Crimean hemorrhagic fever virus
	V3.	Dengue fever virus
	V4.	Eastern equine encephalitis virus
	V5.	Ebola virus
	V6.	Hantaan virus
	V7.	Junin virus
	V8.	Lassa fever virus
	V9.	Lymphocytic choriomeningitis virus
	V10.	Machupo virus
	V11.	Marburg virus
	V12.	Monkey pox virus
	V13.	Rift Valley fever virus
Viruses	V14.	Tick-borne encephalitis virus (Russian Spring-Summer encephalitis virus)
	V15.	Variola virus
	V16.	Venezuelan equine encephalitis virus
	V17.	Western equine encephalitis virus
	V18.	White pox
	V19.	Yellow fever virus
	V20.	Japanese encephalitis virus
Rickettsiae	R1.	Coxiella burnetti
	R2.	Bartonella Quintana (Rochlimea quintana, Rickettsia quintana)
	R3.	Rickettsia prowasecki
	R4.	Rickettsia rickettsii
Bacteria	B1.	Bacillus anthracis
	B2.	Brucella abortus
	B3.	Brucella melitensis
	B4.	Brucella suis
	B6.	Clostridium botulinum
	B5.	Chlamydia psittaci
	B7.	Francisella tularensis
	B8.	Burkholderia mallei (pseudomonas mallei)
Bacteria	B9.	Burkholderia pseudomallei (pseudomonas pseudomallei)
	B10.	Salmonella typhi
	B11.	Shigella dysenteriae
	B11.	Vibrio cholerae

Table 2. Australia Group Biological/Toxin Warfare Agents

	B13.	Yersinia pestis
Genetically Modified Micro-organisms	G1.	Genetically modified microorganisms or genetic elements that contain nucleic acid sequences associated with pathogenicity and are derived from organisms in the core list.
	G2.	Genetically modified microorganisms or genetic elements that contain nucleic acid sequences coding for any of the toxins in the core list, or their subunits.
Toxins	T1.	Botulinum toxins
	T2.	Clostridium perfringens toxins
	T3.	Conotoxin
	T4.	Ricin
	T5.	Saxitoxin
	T6.	Shiga toxin
Toxins	T7.	Staphylococcus aureus toxins
	T8.	Tetrodotoxin
	T9.	Verotoxin
	T10	Microcystin (Cyanginosin)
Viruses (Warning List)	WV1.	Kyasanur Forest virus
	WV2.	Louping ill virus
	WV3.	Murray Valley encephalitis virus
	WV4.	Omsk hemorrhagic fever virus
	WV5.	Oropouche virus
	WV6.	Powassan virus
	WV7.	Rocio virus
	WV8.	St Louis encephalitis virus
Bacteria (Warning List)	WB1.	Clostridium perfringens
	WB2.	Clostridium tetani
	WB3.	Enterohaemorrhagic Escherichia coli, serotype 0157 and other verotoxin producing serotypes
	WB4.	Legionella pneumophila
	WB5.	Yersinia pseudotuberculosis
Genetically Modified Micro-organisms	WG1.	Genetically modified microorganisms or genetic elements that contain nucleic acid sequences associated with pathogenicity and are derived from organisms in the warning list.
	WG2.	Genetically modified microorganisms or genetic elements that contain nucleic acid sequences coding for any of the toxins in the warning list, or their subunits.
Toxins	WT1.	Abrin

Table 2. Australia Group Biological/Toxin Warfare Agents

(Warning List)	WT2.	Cholera toxin
	WT3.	Tetanus toxin
	WT4.	Trichothecene mycotoxins
	WT5.	Modecin
	WT6.	Volkensin
	WT7.	Viscum Album Lectin 1(Viscumin)
Animal Pathogens		
Viruses	AV1.	African swine fever virus
	AV2.	Avian influenza virus
	AV3.	Bluetongue virus
	AV4.	Foot and mouth disease virus
	AV5.	Goat pox virus
Viruses	AV6.	Herpes virus (Aujeszky's disease)
	AV7.	Hog cholera virus (synonym: Swine fever virus)
	AV8.	Lyssa virus
	AV9.	Newcastle disease virus
	AV10.	Peste des petits ruminants virus
	AV11.	Porcine enterovirus type 9 (synonym: swine vesicular disease virus)
	AV12.	Rinderpest virus
	AV13.	Sheep pox virus
	AV14.	Teschen disease virus
	AV15.	Vesicular stomatitis virus
Bacteria	AB3.	Mycoplasma mycoides
Genetically Modified Micro-organisms	AG1.	Genetically modified microorganisms or genetic elements that contain nucleic acid sequences associated with pathogenicity and are derived from organisms in the list.
Plant Pathogens		
Bacteria	PB1.	Xanthomonas albilineans
	PB2.	Xanthomonas campestris pv. citri
Fungi	PF1.	Colletotrichum coffeanum var. virulans (Colletotrichum Kanawae)
	PF2.	Cochliobolus miyabeanus (Helminthosporium oryzae)
	PF3.	Microcyclus ulei (syn. Dothidella ulei)
	PF4.	Puccinia graminis (syn. Puccinnia graminis f. sp. tritici)
	PF5.	Puccinia striiformis (syn. Pucciniaglomerum)
	PF6.	Pyricularia grisea/ Pyricularia oryzae

Table 2. Australia Group Biological/Toxin Warfare Agents

Genetically Modified Micro-organisms	PG1.	Genetically modified microorganisms or genetic elements that contain nucleic acid sequences associated with pathogenicity derived from the plant pathogens on the list
Awareness Raising Guidelines		
Bacteria	PWB1.	Xanthomonas campestris pv. oryzae
	PWB2.	Xylella fastidiosa
Fungi	PWF1.	Deuterophoma tracheiphila (syn. Phoma tracheiphila)
	PWF2.	Monilia rorei (syn. Moniliophthora rorei)
Viruses	PWV1.	Banana bunchy top virus
Genetically Modified Micro-organisms	PWG1.	Genetically modified micro- organisms or genetic elements that contain nucleic acid sequences associated with pathogenicity derived from the plant pathogens identified on the awareness raising list.

The newly emergent Severe Acute Respiratory Syndrome virus (corona-like SARS virus) should be considered a likely threat. SARS emerged in 2003 in the People's Republic of China and exhibits a 4-10 percent mortality rate.

Time Differences between a B Agent Attack vs. other WMD Attack

Bioterrorism events OCONUS and CONUS differ from other WMD events. The differences in time and effect are:

- The time delay between the release of the agent and the appearance of disease in the target population (typically 72-192 hours) increases the possibility of disease dissemination.
- Exposed persons continue the threat to others because of the infectious quality of the threat agent.
- The effects of nuclear, chemical, and high explosive (HX) materials on a target are apparent within seconds to minutes of the event.
- Radiological materials will manifest their adverse effects on a target within hours if the dosage is high; it may take weeks to years to observe the full consequences of the threat materials at lower doses. Standard detectors of alpha, beta, or gamma emission can readily determine that a radiological material has been released in a particular location.

Biological Threat

Targets (human, animal, or plant) generally exhibit clinical signs of exposure 3 to 8 days after the release of the threat agent. The delay between exposure and appearance of clinical signs will cause the nature of the responder and the management strategies to differ from other WMD events. Because the individual exposed to contagious infectious agents (various viruses and bacteria) continues to serve as persistent sources of threat agent to society (infected humans, animals, and agricultural crops), managing the threat differs from other WMD scenarios. The

threat agents of primary concern include those identified by the Australia Group. The agents listed in Table 2 have been weaponized by threat nations.

Recognition of Event

Immediate Detection. If sensor systems detect threat agents at the time of release, authorities present at or near the scene of the event can take immediate action. Such action includes securing the perimeter and treating exposed persons with appropriate antibiotics, antivirals, and anti-toxins. In this case, the care providers are the authorities present or care persons who may be called to the scene of the incident.

Later Detection. The likely scenario is that a BW threat agent will not be immediately detected at the time of release. The recognition of an event is dependent on the first appearance of and identification of clinical signs that are not consistent with patterns of normal illness in the community. This new appearing illness will occur typically 3 to 8 days after release of the threat agent. The first responder in this situation will be the health care provider in an emergency medical service environment, an emergency room, a private physician, the pathologist, a pharmacist, or a family member. Recognizing an illness as a result of new emergent disease or bioterrorist activity will be confounded by two realities: 1) many illnesses appear similar to common flu at early stages (enteric or respiratory signs) and 2) the differential diagnosis process requires the assumption of first ruling out most probable cause of illness before assigning cause to unlikely causes. Because bioterrorist events are very low probability, but high consequence situations, the differential diagnosis process mitigates against recognition of such an event.

This section recognizes three operational situations related to biological threat: the pre-event, period of minutes to hours surrounding the event of release, four or more hours post-event.

Pre-event. Protective measures in the pre-event period include pharmaceuticals and protective covering.

Pharmaceuticals include:

- Vaccination
- Storage and maintenance of vaccines, antivirals, and antibiotics

Protective Covering includes

- Body-cover similar to that used in surgical suites
- Face masks that cover the mouth, nose, ears, and eyes

In the absence of skin abrasions or puncture wounds, biological threat agents (i.e., viruses, bacteria, fungi, and toxins) will generally not penetrate intact skin. BW threat agents may be ingested, inhaled, sexually-transmitted, or injected.

Minutes-to-Hours after Release

In the minute-to-hours period after the release of a BW threat agent, sensors will activate alerting personnel to the presence of the agent. Intelligence activities will begin to identify the source. The threat condition can be affected by meteorological events.

Four or more Hours after Release

Host response markers of infection and clinical illness will become apparent. The operational situation will require treatment and management of the exposed population, decontamination of equipment, water sources, and first responder personnel.

Biological Agent Detection and Identification

The ECBC and their university partners have developed specific binding molecules for biological threat agents and for chemical agents. Current military platforms usually have chemical and radiological sensor systems, but the platforms do not possess sensors to detect and identify the majority of BW threat agents. The Biological Integrated Detection System (BIDS) detects only two organisms, anthrax and plague. BIDS also detects several toxins including enterotoxin B. The emerging danger from BW threat agents requires that existing deployable sensors, requiring low energy and weight, be rapidly field-hardened and deployed as a spiral technology.

To detect BW threat agents, the sensors require technology that permits rapid scanning of many samples for the presence of specific genomic or epitopic sequences, and with very few false positives/negatives. The sensors also require the development of recognition molecules that bind threat agents with very high affinity and specificity. Establishing correlated databases will provide information on incidence of disease and workforce absenteeism in communities where major defense forces are located. A critical unmet need is a communication system that allows critical information sharing with the national security, medical community, and public sectors. The concern involves resource allocation, public safety coordination, perimeter management, and extended telemedicine care (24 hours per day, 7 days per week, for several months). Technology available in 2003 permits: 1) producing materials that bind threat agents with high selectivity and affinity; 2) developing platforms and opto/electronic signal transducers that signal an event; and 3) fusing data for use by an operator.

The binding materials include antibodies, nucleic acid probes, and aptamers. Platforms available at this time include optical detection based on the Luminex system (Austin, TX), optical detection systems involving the Cepheid system, oxidation/reduction methods similar to Therasense model, and the electronic tongue method. Other sensors of interest include the Invader System of Third Wave Technology (Madison, WI). In most cases the antibodies used for detection and identification show cross-reactivity with non-threat but related organisms [e.g., bacillus, cereus (minimal threat), and bacillus anthracis (high threat)]. The antibodies can be used to detect intact organisms with no requirement for amplification. Nucleic acid probes when properly designed can provide highly specific detection of pathogens. Such nucleic acid detection systems require amplification of the threat sample to yield sufficient signal for detection and identification.

Archival data sets have been established through partnership with state Departments of Health in CONUS and with the military community to provide normal disease incidence CONUS and OCONUS. Current capabilities in various hospitals permit large-scale, real-time tentative diagnoses of patients from Emergency Medical facilities to be collected electronically using Commercial-off-the-Shelf (COTS) methods (e.g., CERNER system). Current cooperative efforts between the various school districts in the US permit determination of school absenteeism in real time (within 48 hours of the absence from the school). Current technology also permits real-time acquisition of purchase data of over-the-counter pharmaceuticals that may be used to treat

infectious disease. All these data sets provide a capability to assess early indicators of illness in a community that can be networked to yield continued screening of disease outbreak.

Microfabricated analytical devices offer significant potential advantages over standard laboratory instrumentation such as speed, cost, sample/reagent consumption, contamination, efficiency, and automation. The devices have capability in development of an automated/integrated chip-based process that will function as a prototype for ultimate microfabrication of “on chip” integrated pumps, valves, and reagent reservoirs capable of “one chip does all” iterative processing.

In the above paragraphs of this section, general principles of detection have been addressed. Several commercial platforms have been identified as having three binding materials for threat agent including antibodies, nucleic acid probes, and aptamers. The following paragraphs address specific binding agents and conditions for detection of biothreat agents.

Very high affinity antibodies ($K_d < 10^{-10}$) to the PA anthrax toxin have been prepared by phage screening methods and these antibodies have demonstrated diagnostic and therapeutic applications. These antibodies have been developed to bind to the anthrax PA toxin 20 times more tightly than currently available antibodies. These antibodies provide 100 percent protection of test animals to the anthrax PA antigen at levels that would have resulted in the death of all the test animals.

Similar strategies can be used to develop high affinity diagnostic antibodies to hemorrhagic fever viruses. Several facilities CONUS can perform definitive studies on live threat agents to determine efficacy of the sensors [e.g., Southwest Foundation for Biomedical Research (SFBR) in San Antonio, TX]. SFBR has a working BL4 laboratory, one of only three in the US and the only non-governmental highest-level containment laboratory.

Pathogenic bacteria possess numerous unique and conserved virulence genes. Because different virulence factors are associated with different disease syndromes, the pattern of genes present in an isolate predicts the pathogenic potential and the type of disease likely to be caused by that isolate. The information about these virulence genes and the pathogenicity islands on which they reside may be used to design rapid detection methods for identifying potential pathogens in the environment or in patient samples. DNA arrays that have sequences representing the entire *E. coli* K-12 chromosome and additional sequences found in pathogenic *E. coli* strains have been prepared and shown to detect *Shigella flexneri* and *Shigella dysenteriae* genes. Each class of threat agent is likely to give a distinct hybridization pattern that will serve as a fingerprint for that type of pathogen. Radix BioSolutions utilizes the Luminex xMAP™ system to develop commercial bioassay kits and reagents for the detection of proteins, nucleic acid sequences, enzyme activity, and receptor/ligand interactions. The xMAP™ system provides a rapid, flexible, and inexpensive platform to perform a variety of bioassays. A primary focus of Radix BioSolutions is to develop a well-rounded palette of bioassays that can be utilized for biological agent detection. The ability to simultaneously detect both the genetic material as well as the proteins of specific pathogens on the same detection platform provides invaluable confirmatory results when monitoring for presence of pathogenic agents.

Effector-activated ribozymes (aptazymes) are capable of transducing molecular recognition of ricin and other toxins into an easily read signal. It will be possible to develop aptazymes that will function inside of cells as biosensors, and that effectively convert an organism to a sentinel.

Infection Signatures and Defense Strategies

In humans and other mammals, bacterial and viral infections cause shifts in mRNA and protein synthesis (e.g., acute phase proteins, cytochrome P450, and Glutathione S-transferase). The host response to infection in various individuals is a function of their genome. A genetic assay for those genes involved in disease susceptibility and any variations (polymorphisms) in humans is being developed rapidly at this time. This approach will predict an individual's response to infection, infectability, and the response of individuals to antivirals or antibiotics.

Gene expression signatures may provide an early indication of infection and may differentiate different types of infection. The approach utilizes mRNA expression analysis with micro-arrays to identify candidate genes. Affymetrix-like oligonucleotide microarrays using Digital Optical Chemistry systems (Texas Instruments) are currently available tools. One of the primary computational biology focuses has been on polymorphism prediction from *de novo* sequence to enable a more efficient directed search for phenotype causing mutations (such as infectability or response to infection), genomics sequence annotation, and automated discovery of hidden knowledge via computer text data mining.

Current approaches focus upon data collection and transmission issues. The methods include: image acquisition, analysis, and wireless transmission to support a mobile detection platform, as well as the optical design issues for microbead-based detectors. Substantial work on software for a portable image acquisition and data transmission system to support sensor platform is completed. Since the system's geographical position would be critical in evaluating the extent of an agent's release, Global Positioning System (GPS) receivers with the image acquisition system are essential.

BW threat agents contained within hydrophilic polymeric aerosols in the 1–10 micron diameter range and chemical agents that are organic compounds in the same size range may be monitored from airborne platforms. Such droplets are sufficiently small to remain airborne for significant periods of time, especially if the agents are negatively charged to inhibit coagulation. Threat analyses suggest that, when dispensed, these agents would appear as long, cylindrical clouds between 100–1000 feet above the ground. BW and CW threat agents represent maximum danger while remaining airborne, but the threat is greatly reduced after deposition on the ground. Both trajectory and the CAMQ model can be used to study the dispersion, concentrations, and deposition of these threat agents. Meteorological features that could affect tactics in deployment of these weapons, such as atmospheric stability, can be modeled.

Chemical Threat

Chemical agent detection and identification is currently achieved by means of the Chemical Agent Monitor (CAM), the FOX vehicle, M21 Remote Sensing Chemical Agent Alarms, and the BIDS. The first three systems detect CW threat agents by point methods. Standoff detection of threat from CW agents can be achieved in some cases by LIDAR methods. A point detection system, the FOX platform samples air and soil by a coupled chromatographic and mass spectroscopic system. The equipment is relatively large, more than 10 pounds, and requires significant power input. The signal output is paper but can be transformed to electronic signals required for network centric communication systems. When modified with the M21 Alarm, remote sensing of CW agent vapor is possible at standoff distances of 5 kilometers (ASB Study 1998). These systems are not roboticized in 2003 and remain labor intensive (a skilled operator is required). ECBC has demonstrated the utility of a near-IR laser system to discriminate blister

agent from other chemical agents at a range of 30 kilometers. The system uses laser-induced fluorescence for this purpose. Electro-spray ionization mass spectroscopy mass absorption laser desorption (MALDI) has demonstrated utility in the characterization of protein toxins and protein signatures in the less than 15,000 dalton range. Major advances realized by ARL and their university colleagues in the production of laser sources at the 340-nanometer (nm) range open a promising area for detecting chemical agents in a standoff manner. The production of high-energy lasers in the wavelength region below 340 nm has yet to be realized.

Commercial Biological and Chemical Detection Systems

This section describes a portfolio of technologies currently available in the private sector for the detection of chemical or biological threat agents. This list was selected to show different approaches for point detection and is not intended to be all encompassing.

BIOCAPTURE 550 is a MesoSystems product that serves as a portable, handheld air sampler for concentrating biothreat agents. The device traps particles in the 0.5-10 micron diameter range and processes 150 liters per minute. The particles are captured on a membrane for further processing.

THIRD WAVE TECHNOLOGY, Madison, WI, uses the Invader technology to detect RNA or DNA genetic material from the threat agent. Invader technology is sensitive enough to detect several thousand copies of agent and can detect a single nucleic-acid change in the RNA or DNA. To detect a threat agent in the field, the Invader system must be coupled with a sample collector and mechanism by which the nucleic acid is released from the agent. It is anticipated that within five years this technology will automatically detect host response to exposure to a threat agent.

SIONEX uses differential ion mobility to detect chemical threats at the parts-per-billion level. Within one year SIONEX expects to use the high electric field spectrometer on a chip (20,000 volts per centimeter) for detection of certain proteins.

IGEN uses capture of biological toxins on micro-particles to activate electro chemical luminescent assays. The reaction between ruthenium and tripropylamine in the presence of the micro-particle bound toxin generates a detectable flash. The system is currently used in tests for food contamination.

RADIX BioSolutions utilizes nucleic acid probes bound to fluorescent micro-particles to detect threat agents in a complex mixture. A thousand samples per hour can be sampled simultaneously in a multiplexed manner. Amplification of the genome is currently required.

RESEARCH INTERNATIONAL uses the raptor technology developed by the Navy to detect neurotoxins in an environment. The system utilizes living cells, which are exposed to chemicals in the environment in a controlled manner.

TERRORIST WEAPONS IDENTIFICATION SPECIALISTS (TWIS) utilizes surface acoustic wave technology to detect chemical threat agents (VX, GA, GB, GD, GF, HD, and HN3) and toxic industrial chemicals (arsine, chlorine, diborane, fluorine, ethylene oxide, ammonia, and hydrogen sulfide) in the 1-20 mg per cubic meter. TWIS also produces a probe of sodium iodide (TI) for detecting gamma emitters (20-3000 KeV). The shelf life of the **SAW** devices is five years. The systems operate on 8-30 Volts DC.

IDAHO TECHNOLOGY INC has developed a gene based RAPID System for detecting biothreat organisms causing anthrax, brucellosis, tularemia, plague, and botulism as well as

listeria, E. coli 0157, salmonella and campylobacter. The technology is deployable and is available as a Commercial-off-the-Shelf (COTS) system that weighs 50 pounds.

Radiological and Nuclear Detection

The detection and identification of radiological agents is facilitated by multiple modeling codes. For example the development of Vanguard nuclear detection sensors allows development of networked systems capable of detecting and identifying nuclear and radiological sources for transport pathway analyses. A current threat situation exists in North Korea because it produces, and can potentially export, nuclear weapons. The standard codes included are MCNPX, 1DB, SOURCES, ORIGIN-ARP, ORIGIN2, NJOY, GENII, Microshield, and Microshine. The sensor integration includes multiple nuclear detectors whose measurements may be correlated to define a singular event. Various nuclear sensors can be employed in these network designs to look for neutrons from plutonium; gammas from highly enriched uranium (HEU) and radiological devices; and airborne radiation resulting from radiological weapons. These sensors may be utilized as WMD early warning systems, WMD portal monitoring systems, as well as tools to provide critical information during WMD response actions.

One of the key systems used to detect and deter the smuggling of special nuclear material (SNM) are portal monitors. These monitors are passive radiation detection systems designed to detect neutron and/or gamma ray emissions from weapons material (specifically plutonium and HEU). There are several types of portal monitors including pedestrian, vehicle, and rail systems. The detection of smuggled SNM on railroad cars is of paramount importance to apprehend potential smugglers. A study was performed to analyze various rail portal monitors to determine the optimal configuration of monitors to provide the largest possible detection signature.

University collaborations with the Department of Energy (DoE) through Los Alamos National Laboratory (LANL) and Sandia National Laboratory have yielded progress on the Second Line of Defense (SLD) project. SLD is a multi-laboratory effort to install radiation detection equipment in strategic locations throughout the world to increase the capability of detecting and deterring the illicit trafficking of nuclear materials. The system prepares network interdiction models, data development, data mining, detector system analysis, and analyses of smuggler perceptions and characteristics.

A difficulty encountered in attempting to secure Russia's international borders from the smuggling of Russian nuclear materials is the large territorial border to be monitored. The US DoE (through the SLD program) collaborates with the Russian Federation State Customs Committee (RF SCC) to help strengthen the overall capability to prevent illicit trafficking in nuclear materials, equipment, and technology. SLD's goals are accomplished primarily by installing, at strategic border locations, equipment capable of detecting nuclear material. This methodology uses a database of information concerning geographic regions in Russia, a multi-attribute utility method for developing a network model, and a stochastic network interdiction technique is used to determine optimal detection points. Using this methodology, the SLD program determined the optimal allocation of resources to outfit the numerous customs locations on the border of Russia; however, it also found that existing analysis techniques were incapable of efficiently and rapidly determining an optimal solution for networks with additional complications. Such complications include a network of smugglers with a broad range of rules governing their behaviors.

The lessons learned in the SLD project can be used to aid in securing the US border and garrisoned regions. The network would involve simulating terrorists attempting to penetrate into the US through legal and illegal border crossings, seaports, and international airports and then proceeding to a target within the US. There are other US organizations focusing on some of the details needed to secure the border: for example, scientists at LANL are developing radiation detection equipment that can detect minute quantities of nuclear material and data on terrorist groups. However, significantly less effort is being expended on developing the methodologies needed to determine how to use this data and where these detectors are to be located.

Detection of Mines , High Explosives and Unexploded Ordnance

Mine detection approaches have used ground penetrating radar (GPR), microwave radiometry (1-10 GHz), thermal Infra Red (3-5 micrometers and 8-14 micrometers), and SAR. Live animal systems have also been tested with rats and bees. APOPO developed an integrated system for training rats to detect samples spiked with HX materials as well as detecting vapor samples from suspected minefields. Rats evaluate the occurrence of explosive trace vapors in field samples. Rats can detect very small levels (picograms) of explosives in the sample. Positive samples are reconfirmed using several rats to provide a very high level of detection accuracy, comparable to dogs. Laboratory rats have demonstrated the ability to evaluate 340 filter samples from various areas in 30 minutes. The work above was reported by the Office of Naval Research (ONR) Europe in 2002. <http://www.onrifo.navy.mil> Laser, Joint Service Warning and Identification Light Detecting & Ranging (LIDAR) (JSWILD) have been proposed to have utility to detect out-gassing from mines at a distance of tens of meters, but the technology is at a very early stage of development. These new technologies when reduced to practice will have applicability in detecting unexploded ordnance and storage of ordnance. At the present time the capabilities are limited.

Non-WMD Force Protection Issues

COTS and Government-off-the-Shelf (GOTS) and advanced research activities at Army Research Lab (ARL) and Edgewood Chemical and Biological Command (ECBC) address many of the sensor needs for the Army's Force Protection. ARL, together with their university partners, have developed leading edge infrared (IR) sensors, high-energy laser detection and ranging (LADAR) applications, radio frequency and microwave, kinetic energy, and active protection.

Protection from Ground and Airborne Platforms

ARL and private sector entities have made marked advances in the detection and identification of ground and airborne platforms. ARL has demonstrated the utility of LADAR applications for ground-to-ground Reconnaissance, Surveillance, & Target Acquisition (RSTA). The reflective modulated LADAR system (using multiple laser wavelengths) has demonstrated its ability to detect tanks and vehicles under camouflage and proposed a fused three-dimensional LADAR system for recognition of aerial platforms, smart munitions, and individual persons. The ability to differentiate tanks and other large platforms is attainable at distances of several hundred meters. The Department of Energy has developed a Vehicle Bomb Guidance Project that provides guidance regarding types of bombs, security systems that may assist in protection against such intrusion, and architectural/structural features of base design to mitigate effects of such bombs.

Protection from Small Arms, Large Weapons, and Hyperkinetic Projectiles

ARL has demonstrated the utility of forward-looking IR (FLIR) for troop and asset protection from proximity fused indirect fire munitions, artillery, mortars, and rockets. Protect ranges over hundreds of meters. LADAR in the low-to-midwave region has potential utility to detect live individuals and locate sources of small arms or large weapon firing. Differential midwave IR vs. low-wave IR may be used to resolve the edge of a bullet (shell). ARL has demonstrated the utility of IR proximity sensors for defeat of hypervelocity projectiles in a direct line-of-sight (LOS) environment. The IR detectors identify muzzle flash. The utility of this system in non-LOS, or parabolic hypervelocity attack appears very limited. Mid-wave to low-wave IR systems have been shown to reveal patterned mine fields and provide signatures of rocket plumes. Then acoustic coupling with seismic sensors has been shown to locate artillery fire sources. Ground based radar systems have been shown to reveal small arms on individual persons at a range of several hundred meters.

Protection from Non-traditional Combatants and Saboteurs

Soldiers must be protected from suicide attacks and exposure to individuals infected with highly contagious diseases, as well as pathogen-based sabotage of food and water supplies. Current technologies do not detect threat persons specifically or the presence of suicide bombers from a standoff position. The experience in the Israel over the last decade and in Iraq and Afghanistan highlight the need to develop these capabilities.

Ultra-wideband radio frequency (RF) platforms have demonstrated limited utility in through-the-wall imaging and in robotic navigation systems in open environments. The utility of the ultra-wideband RF for force protection in urban environments appears to be limited at this time.

Perimeter Protection

Sensors can be used for a perimeter protection system to prevent a perimeter breach. The perimeter protection system must be cost effective in saving money and lives.

RECOMMENDATIONS

The study group recommends that current capabilities be examined and investment be made in radio frequency (RF), LADAR, microwave, and radar detection for vehicles and persons. Critical areas with low capabilities must be evaluated and investment made in energy efficient, portable systems to detect/identify B agents and suicide bombers. Investment must be made in a cost-effective large area perimeter protection system.

CONCLUSION

Current Strengths

The Army already has large, bulky pieces of equipment that detect and identify B and C agents. The equipment works but is not easily portable and falls short of meeting all of the soldier's needs. The Army's capabilities also include:

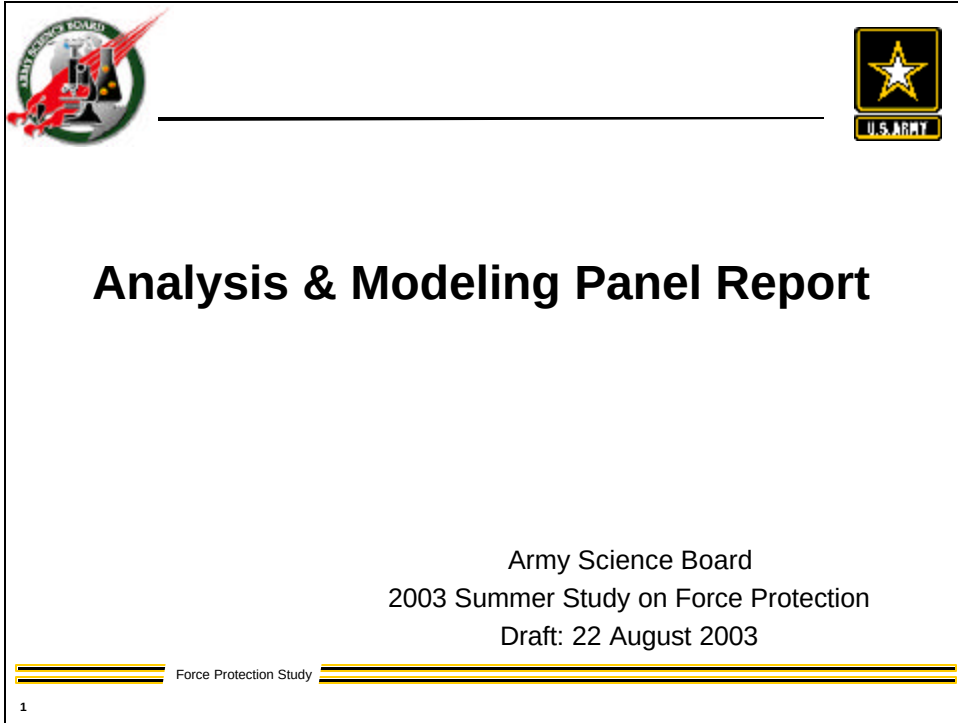
- Detecting radar and microwave from a distance
- Detecting both high- and low-velocity projectiles
- Identifying friendly persons

- Performing nuclear source identification

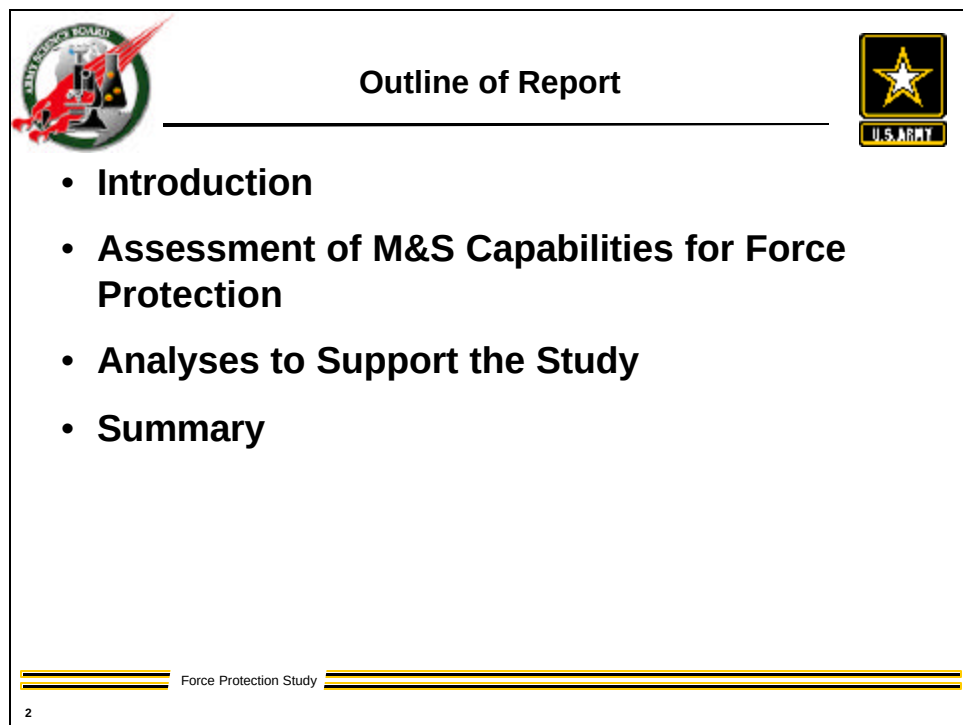
Critical Unmet Needs

The Army critical unmet needs include a portable, energy-efficient system to detect and identify B agents. The Army must have:

- Perimeter protection that is cost-efficient and effective to protect US soldiers
- Integratable/fusable sensor information
- System to detect and identify human suicide bombers
- Methods to rapidly detect and identify infected humans in LDC



This report summarizes the deliberations of the Analysis & Modeling Panel of the 2003 ASB Summer Study on Force Protection.



This is the outline of the report. First we will provide an Introduction to the report, describing the Panel's mission, identifying the members of the Panel, and identifying the organizations that we visited. Second, we will discuss our findings and recommendations on existing and planned M&S to support force protection (FP) functions. Third, we will describe briefly the results of the analyses that

were performed in support of this summer study. Finally, we will summarize the Panel's major findings and recommendations.

The Main Report is supported by several appendices. Appendix A provides supporting information about the M&S and associated analyses associated with the protection of mobile Blue forces. This work is based on the products and processes developed by the USMC's Project Albert. Appendix B describes the tools and analyses associated with the protection of fixed installations. This work is based on the products and processes developed by Sandia National Laboratories (henceforth referred to as Sandia). Appendix C contains a list of abbreviations and acronyms. Appendix D provides a list of references and useful web sites.



Panel Objectives



- Identify initiatives to improve the utility of models and simulations (M&S) in support of key force protection functions; e.g.,
 - Education and training (E&T)
 - Support to operations
 - Assessment/Experimentation
 - Acquisition
- Conduct analyses to shed light on the contribution that proposed changes in Doctrine, Organization, Training, Materiel, Leadership & Education - Personnel, Facilities (DOTMLPF) can have on force protection effectiveness and efficiency

Force Protection Study

3

We had two related jobs to perform. First, we were charged with identifying and assessing the capabilities of existing M&S tools to support four key FP functions: education and training (E&T), support to military operations, assessment and experimentation, and acquisition. Based on that assessment we were asked to recommend M&S initiatives for each of those functions.

Second, taking advantage of appropriate M&S tools, we were asked to perform analyses to highlight those capabilities across the areas of Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities (DOTMLPF) that were needed to enhance FP appreciably. These latter analyses were performed in concert with the Operations and Science & Technology (S&T) Panels. Initially, we performed parametric analyses to help those panels focus their efforts.

Subsequently, we performed selected analyses to help quantify and rank order promising materiel and operational options that those panels identified.



Analysis & Modeling Panel Members



- Team members
 - Stuart Starr, MITRE (Chair)
 - Dan Rondeau, Sandia
 - Ira Kohlberg, IDA (shared with Technology Panel)
- Government advisors
 - Maj Tedd Dugone, AMSO
 - Mike Macedonia, PEO STRI
- FFRDC advisor
 - Sarah Johnson, MITRE

Force Protection Study

4

The Analysis & Modeling Panel's membership is listed on the above slide. The Panel would also like to acknowledge the invaluable assistance of a number of individuals who contributed to several of the analyses described in this report. In particular, Mike Phillips, DTRA/TD, supported the assessments of fixed installations subject to biological and chemical attacks. In addition, Cal Jaeger and Tommy Woodall, Sandia, contributed to the assessments of fixed installations subject to high explosives attack. Furthermore, Dell Lunceford, Director, AMSO, played a significant role in providing guidance and advice to the Panel and hosting several of its meetings. Finally, the Panel would like to acknowledge the contributions of Peter Cherry, SAIC, who assisted in the Panel's initial formulation of the problem.



Key Visits

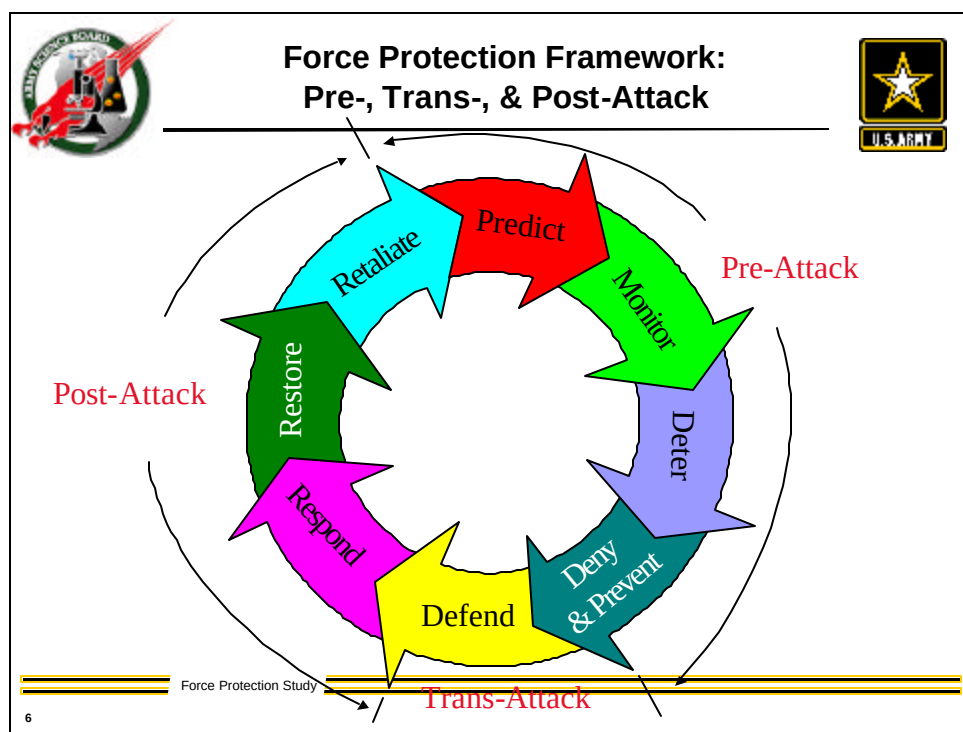


- Washington, DC
 - IDA
 - Project Albert
 - AMSO
 - J-8, Joint Staff
 - DARPA
 - DTRA Operations Center - WMD Analysis Cell
 - Toffler Associates
- Monterey, CA
 - Project Albert International Workshop (Naval Postgraduate School)
 - TRAC-Monterey
- Los Angeles, CA
 - RAND
 - Institute for Creative Technologies (ICT)
- Albuquerque, NM
 - Sandia National Labs
 - Kirtland AFB

Force Protection Study

5

The Panel visited a broad set of organizations to acquire the inputs needed to achieve the Panel's objectives. In the Washington, DC, area, the team met with a variety of organizations to identify and discuss key M&S tools (e.g., Project Albert, DTRA, DARPA), to discuss the results of FP analyses (e.g., IDA; J-8, Joint Staff; Toffler Associates), and to explore new M&S management options (e.g., AMSO). In Monterey, CA, several members of the team participated in the Project Albert International Workshop to apply existing agent based models to FP issues. In addition, contact was made with TRAC-Monterey to discuss their experiences with the military operations in urban terrain (MOUT) Focus Area Collaborative Team (FACT) and to discuss their recent MOUT analyses. In Los Angeles, CA, discussions were held with RAND on their assessments of convoy vulnerabilities and a visit was made to the Institute for Creative Technologies (ICT) to discuss their most recent training tools. Finally, in Albuquerque, NM, extended discussions were held with the Sandia staff to discuss relevant FP M&S, technologies that are being developed to enhance FP effectiveness and efficiency, and lessons learned in conveying very hazardous materials. In addition, a discussion was held with personnel at Kirtland AFB to explore current FP systems and procedures.



In order to establish a common framework with the other panels, the FP problem was initially subdivided into pre-, trans-, and post-attack phases. As depicted in the slide, these phases were subsequently divided into a sequence of functions that must be performed by Blue Forces. In addition, specific sub-functions were identified; these are documented in Annex A of this report. This framework was employed as an organizing principle in identifying relevant FP M&S tools and in conducting the analyses for the individual cases of interest.

It is observed that one of the key objectives in FP is to invest across these functions in a balanced way to leverage the benefits of proactive actions (e.g., predict and monitor adversary action to preempt potential attacks; take steps to mitigate the effects of an attack) while ensuring effective defense, response, and restoration in the case that an attack is launched.



Outline of Report



- Introduction
- **Assessment of M&S Capabilities for Force Protection**
- Analyses to Support the Study
- Summary

Force Protection Study

7

This chapter of the report assesses M&S capabilities for FP. We address M&S in support of the functions of education & training, operations, assessment/experimentation, and acquisition. For each of those functions, we identify key needs for M&S in support of FP, identify selected M&S tools, and summarize our major findings and recommendations.



Key Functional Needs for M&S in Support of Force Protection (1 of 2)



- Education & Training (E&T) (including exercises)
 - Support all force protection participants (e.g., Commander to “strategic private”)
 - Provide just-in-time, anywhere, anytime
 - Support force protection exercises more efficiently (quicker, better, cheaper)
- Support to operations
 - Consistent with pre-, trans-, and post-attack needs
 - Tools should be
 - Faster and easier to set up and use
 - More credible (e.g., dealing with the human dimension)

Force Protection Study

8

To establish some yardsticks to aid in the assessment of the adequacy of existing and proposed M&S to support FP, the Panel developed strawman functional needs for M&S in support of E&T, operations, assessment/experimentation, and acquisition.

In the area of E&T it is observed that FP imposes unique needs in several dimensions. First, in FP, the actions of the lowest ranking soldier can have major operational and strategic implications (the so-called “strategic private”). For example, if the private is not trained on how to deal effectively with a potentially lethal confrontation at a checkpoint, he can stimulate a riot that has profound geo-political ramifications. Conversely, the education and training of many senior leaders focuses on tactical and operational issues and they have not been trained on how to deal with the many strategic challenges associated with FP. As an example, LTG Zanini (USA, ret) emphasized this issue when he described the consequences of the kidnapping of a GI from the Seoul metro by demonstrators. This incident had serious ramifications in the social domain (e.g., signs in restaurants proclaiming “Americans not welcome”), the economic domain (e.g., businessmen electing to restrict their investments in Korea), and the alliance domain (e.g., fraying of relationships between the senior military of Korea and the US). Since US forces are frequently being asked to deploy anywhere in the world with little advanced warning, it is important that E&T for all echelons is available just-in-time, anywhere, anytime. This suggests that it must be tailorable to reflect the unique cultural and social attributes of the Area of Responsibility (AOR). Finally, the Panel believes that an essential element of training is frequent, routine exercising. Currently, FP is rarely a key dimension of routine exercises. To change that mind set, tools are needed to address FP in exercises quicker, better, and cheaper.

In the operations domain, there is a need to develop, field, and develop proficiency with a broad spectrum of M&S tools in support of all phases of operations. This includes all of the sub-functions associated with pre-, trans-, and post-attack operations (see page 6). In particular, the Panel was informed during its visits that these tools must be faster and easier to set up and use than the current generation of fragmented decision support tools. If they are to be more credible, they must be able to deal more realistically with the human dimension of the problem (e.g., the behavior of crowds manifesting high levels of anger and fear).



Key Functional Needs for M&S in Support of Force Protection (2 of 2)



- **Assessment/Experimentation**
 - Enhance the ability to evaluate the impact of proposed changes to DOTMLPF on force protection effectiveness, efficiency
 - Enhance the quality of key performance assessment tools (e.g., plume prediction)
 - Acquire tools to support optimization of FP investments (e.g., S&T)
- **Acquisition**
 - Develop resources (e.g., M&S, data, infrastructure) to support the Simulation & Modeling, Acquisition, Requirements, Training (SMART) paradigm
 - Gather better environmental and human behavior data

Force Protection Study

9

In the assessment/experimentation domain, many of the proposed enhancements to FP transcend materiel issues and require consideration of new doctrine, organizations, concepts of operation, training and leadership (i.e., many of the factors inherent in DOTMLPF). Consequently, analysts and experimenters will need tools that will enable them to flexibly modify all of those factors to assess their impact on FP effectiveness, efficiency, and risk. At a more technical level, the threat of weapons of mass destruction requires the development of tools to address the physics, chemistry, and biological dimensions of the problem. As one example, it is recognized that current tools that predict the dispersion of plumes of contaminants are seriously flawed for important operational environments, such as urban canyons. Finally, this Summer Study has demonstrated that there are a broad set of options that could be taken to mitigate many of the challenges associated with FP. However, because of significant resource constraints (e.g., funding, manpower) and varying perceptions of acceptable risk, it will be necessary to formulate and assess alternative FP portfolios. The analysis community will require appropriate tools to support the optimization of FP investments in several areas (e.g., science and technology).

In the acquisition domain, senior Army decision makers have been embracing the paradigm of Simulation and Modeling for Acquisition, Requirements, and Training (SMART). In this concept, an integrated environment (of M&S, data, and infrastructure) is created and employed to enhance cross-disciplinary coordination across the usual acquisition “stovepipes” (e.g., requirements formulation, development, production, test and evaluation, training, maintenance). This concept is intended to enhance program quality (e.g., minimize total cost of ownership, enhance system performance) and facilitate the acquisition of future, related programs. If SMART is to be applied to the FP problem, it will require the creation and evolution of a tailored integrated environment. One of the key elements of this integrated environment is data that have been verified, validated, and certified. Since environmental and human behavior are key dimensions of the FP problem, special attention must be paid to the acquisition of those data.



FP E&T: Selected Tools, Findings



- Selected Tools
 - Support to squad, company training
 - USMC Combat Decision Range (CDR)
 - ICT Full Spectrum Warrior and Think Like a Commander (TLAC)
 - Base and installation training
 - USAF Eagle Defender
 - PEO STRI Virtual Emergency Response System (VERTS)
 - Support to exercises -- Counterintelligence and Human Intelligence Exercise Scripting Support System (CHESSS)
- Findings
 - There exist some useful (albeit limited) tools
 - Key voids include
 - Support to the Commander and Institutional training
 - Full suite of Joint exercise support tools
 - Training tools to support convoy operations



Think Like A Commander

Force Protection Study

10

During the Panel’s visits, we encountered a variety of tools, several from other Services, that could help satisfy some of the Army’s FP E&T needs. At the squad level, the USMC has developed and

deployed widely the Combat Decision Range (CDR) (Reference 1). This tool is hosted on a PC and uses branching video to expose the squad leader to a broad set of FP issues (e.g., dealing with a mob; responding to sniper attacks). Currently, a Marine can not be certified as a squad leader if he has not successfully coped with the CDR scenarios. Furthermore, the Institute for Creative Technologies (ICT) has developed Full Spectrum Warrior, a small unit urban warfare simulation, for the Microsoft X-box console (Reference 2). This product is still in an early development stage and it may require additional adaptation to enhance its utility for the FP problem. At the company level, ICT is pursuing the Think Like a Commander (TLAC) project (Reference 3). TLAC is investigating the role of storytelling and interactive dialogue with virtual characters to support leadership development for US Army soldiers. The first prototype, entitled "Power Hungry", has been developed as a PC application for lieutenants and captains, and aims to develop in these officers a greater appreciation for the leadership challenges that face company commanders.

At the base, installation level, the Panel identified two interesting tools. The USAF employs Eagle Defender to support Air Force Security Forces training for Air Force base defense (Reference 4). PEO STRI has developed the Virtual Emergency Response System (VERTS) to train first responders and National Guard Civil Support Teams on performing homeland defense or natural disaster missions using virtual simulations (Reference 5). First responders and civil support teams react to weapons of mass destruction, bio-terrorism, terrorism or natural disasters that occur throughout the country, including on military installations. Since environmental hazards, safety, and cost restrictions often preclude soldiers and other first responders from live training on this type of scenario, VERTS helps fill an important segment of this critical training gap.



FP E&T: Selected Tools, Findings



- Selected Tools
 - Support to squad, company training
 - USMC Combat Decision Range (CDR)
 - ICT Full Spectrum Warrior and Think Like a Commander (TLAC)
 - Base and installation training
 - USAF Eagle Defender
 - PEO STRI Virtual Emergency Response System (VERTS)
- Support to exercises -- Counterintelligence and Human Intelligence Exercise Scripting Support System (CHESSS)
- Findings
 - There exist some useful (albeit limited) tools
 - Key voids include
 - Support to the Commander and Institutional training
 - Full suite of Joint exercise support tools
 - Training tools to support convoy operations



Think Like A Commander

Force Protection Study

11

In support to exercises, the Panel found that most of the planning, execution, and after action reporting systems are largely manual and manpower intensive. One notable counter-example is the US Army Pacific Counterintelligence (CI) and Human Intelligence (HUMINT) Exercise Scripting Support System (CHESSS) (Reference 6). This web-based tool is limited in its scope to the CI, HUMINT dimension of the problem, but, as discussed in the main report of the Summer Study, these are critical facets of FP. Initial applications of this tool have revealed the following benefits: saving time, money,

and valuable resources in preparing scripts and other supporting documentation and materials; enhancing the quality of the training experience; and promoting the reuse of exercise material. As described above, the Panel concluded that there exist several useful (albeit limited) E&T tools. Key voids that must be filled include the need for training tools to support convoy operations; training tools to satisfy the FP needs of the Commander; and a full suite of joint exercise support tools.



FP Operations: Selected Tools, Findings



- Selected Tools
 - Prediction: DARPA tools (Willis); Sandia tools on convoy route risks
 - Monitoring: DARPA initiatives (e.g., “Combat Zones That See”); Sandia monitoring of convoys
 - Deter, Deny, Prevent: Sandia risk assessment tools (fixed installations; critical infrastructure); Project Albert Agent Based Models
 - Defend: Plume prediction models (e.g., HPAC, JEM)
 - Respond: Tools from HLS ACTD (e.g., collaboration); Sandia database of emergency responders
 - Restore: Geographic Information Systems (GIS)
 - Retaliate: SOF tools (e.g., SOFPARS and MPARS)
- Findings
 - There are key shortfalls in existing tools (e.g., plume prediction, representation of crowd and terrorist behaviors)
 - Interesting individual tools are emerging which have not been integrated into an orchestrated set
 - Emerging operational support tools entail a new E&T burden for the users

Force Protection Study

12

As depicted on this slide, there is a broad set of existing and emerging decision support systems to support all of the functions associated with FP. However, with one notable exception, these tools are stand-alone products developed by several Services and Agencies. The one example of an integrated suite of tools that address a broad range of FP functions is Sandia’s products to support the conveying of very hazardous materials (e.g., nuclear weapons). In this suite, tools have been created to assess the risks associated with alternative convoy routes, to monitor the status of the convoys while they are in transit, and to identify and locate emergency responders to mobilize in the event of an incident. In addition, the participants in this process are compelled to undergo frequent and stressful testing. Although it is not feasible to implement such a comprehensive capability to support the conveying of routine logistics products, this system could be viewed as a bounding case against which future capabilities can be measured.

The slide also identifies several tools in each of the functional categories that are worthy of consideration for future FP decision support systems. Additional information on many of these tools is available on the web sites identified in Appendix D.

- Prediction. This summer study has concluded that enhanced tools and techniques are needed to improve the ability to predict potential adversary action. The work by Larry Willis, DARPA, provides an interesting point of departure.

- Monitoring. Based on predictions of adversary intent, steps must be taken to monitor key precursor events (e.g., suspicious traffic activity). Several DARPA programs (e.g., “Combat Zones That See”, which fuses information from multiple closed circuit television systems) could contribute usefully to this function.

• Deter, Deny, Prevent: Sandia has developed a broad array of tools to help identify actions to mitigate the effects of potential attacks against fixed installations or critical infrastructures. One of those tools, Hazard Assessment and Mission Enhancement of Resources (HAMER) (Reference 7), was used extensively by this Panel. In addition, several of the agent based models being developed by the USMC's Project Albert appear to be relevant to the FP problem (see Appendix A) although additional work is required to represent crowd and terrorist behavior more credibly. One of those agent based models (or distillations), Mana (Reference 8), was used by this Panel to explore FP issues for mobile Blue forces.



FP Operations: Selected Tools, Findings



- Selected Tools
 - Prediction: DARPA tools (Willis); Sandia tools on convoy route risks
 - Monitoring: DARPA initiatives (e.g., "Combat Zones That See"); Sandia monitoring of convoys
 - Deter, Deny, Prevent: Sandia risk assessment tools (fixed installations; critical infrastructure); Project Albert Agent Based Models
 - Defend: Plume prediction models (e.g., HPAC, JEM)
 - Respond: Tools from HLS ACTD (e.g., collaboration); Sandia database of emergency responders
 - Restore: Geographic Information Systems (GIS)
 - Retaliate: SOF tools (e.g., SOFPARS and MPARS)
- Findings
 - There are key shortfalls in existing tools (e.g., plume prediction, representation of crowd and terrorist behaviors)
 - Interesting individual tools are emerging which have not been integrated into an orchestrated set
 - Emerging operational support tools entail a new E&T burden for the users

Force Protection Study

13

• Defend. In the event of a CBRN attack, it is important to be able to predict plume dispersion accurately and responsively. The current community standard, Hazard Prediction and Assessment Capability (HPAC) (Reference 9), is useful but limited (see NRC monograph, Reference 10). HPAC has been used by this Panel to provide broad assessments of the risks associated with hypothetical biological or chemical attacks against fixed installations. The Joint Effects Model (JEM) program, directed by SPAWAR, is exploring options to ameliorate many of the shortcomings of HPAC (Reference 11).

• Respond. Under the leadership of DISA, a Homeland Security (HLS) ACTD is underway that is exploring options to enhance information flow among DoD, DHS, regional, state, and local responders. As one of their initiatives, they are exploring the utility of collaborative environments to facilitate the coordination and control of response activities.

• Restore. In the immediate aftermath of the attack on the World Trade Center, Geographic Information Systems (GIS) proved very useful in assessing the extent of the damage and providing useful insight to guide restoration. Similarly, the USAF has used ESRI's Arcview GIS tool for FP studies (Reference 12).

• Retaliate. In support of retaliatory actions, Special Operations Forces have developed several useful planning and rehearsal tools (e.g., Mission Planning and Rehearsal System (MPARS))(Reference 13). Based on these observations, the Panel derived the following findings on M&S to support FP operations. First, there are key shortfalls in many of the existing tools. Particularly notable are the

shortfalls in plume prediction and the ability to represent crowd and terrorist behaviors. Second, although selected interesting individual tools are emerging, they are being developed in isolation by a variety of Services and Agencies. Consequently, mechanisms are not in place to integrate these products into an orchestrated set of decision aids. Finally, it must be recognized that emerging operational support tools will entail a new E&T burden for the users. Thus steps must be taken to provide adequate training on the application of these tools as they are introduced and (hopefully) integrated.



FP Assessments: Selected Tools, Findings



- Selected Tools
 - Constructive, mission-oriented M&S; e.g.,
 - JANUS
 - OneSAF Testbed and One SAF Objective System
 - Joint Conflict and Tactical Simulation (JCATS)
 - Hazard Assessment and Mission Enhancement of Resources (HAMER)
 - Distillations (e.g., Mana, Pythagoras, PAX)
 - USAF Joint Tactical Simulation Model
 - Resource allocation tools (e.g., Sandia's Advanced DARPA Integrated Decision Support System (ADIDSS))
- Findings
 - Existing tools
 - Are generally difficult to set up and employ (particularly if non-materiel options are to be assessed)
 - Need refinement to represent human behavior more credibly
 - Should be augmented with optimizing algorithms, techniques (e.g., genetic algorithms)
 - It is currently difficult to manage, link all the complex data associated with FP



Force Protection Study

14

FP has long been a topic of interest in the analytical community. As an example, Lanchester's equations were used to support naval convoy analyses during World War II (Reference 14). The current analytical community tends to rely more on constructive, mission-oriented M&S to support FP analyses. The above slide identifies several of the M&S tools that the Panel encountered during its visits. Additional information on these tools can be found in Appendices A and B, and on the web sites identified in Appendix D.

As an additional task, analysts are also asked to structure and mine the relevant literature in a mission area. For example, to support this process in the area of the Future Combat Systems (FCS), Sandia recently created the Advanced DARPA Integrated Decision Support System (ADIDSS))(Reference 15).

The Panel concluded that existing M&S to support FP analyses are deficient in several important areas. First, they are generally difficult to set up and employ, particularly if non-materiel options (e.g., new tactics, techniques, and procedures (TTPs)) are to be assessed. Second, they need refinement to represent human behavior more credibly. Finally, most of the tools that were identified are designed to simulate a specified set of conditions. There is a need to augment them with optimizing algorithms and techniques to help identify preferred options, consistent with specified cost functions and constraints. For example, promising research is being performed in the use of Genetic Algorithms in concert with agent based models to identify optimal options (Reference 16).

FP has long been a topic of in the analytical community (see <http://diana.gl.nps.navy.mil/~washburn/Files/Lanchester.pdf> for a discussion on Lanchester's square law used for naval convoy analyses in WWII).

We identified a number of tools:

OneSAF <http://www.onesaf.org/>

JCATS http://www.jwfc.jfcom.mil/about/fact_jcats.htm

HAMER <http://www.dtic.mil/ndia/security2/jaeger.pdf>

MANA and other agent-based simulations used by Project Albert

<http://www.mcw1.quantico.usmc.mil/divisions/albert/research/index.asp>

ADIDSS See <http://www.ciao.gov/resource/PCCIP/sdranddrecs.pdf>

There is also promising research into the area of Genetic Algorithms (GAs) for developing learning agents to represent human behavior.



FP Acquisition: Selected Tools, Findings



- **Selected Tools**
 - Currently, there are no specific Army tools that have been assembled to support the acquisition of FP systems
 - However,
 - The FCS program has assembled and employed relevant M&S tools (e.g., MATREX and SOSIL)
 - The USAF Force Protection Battlelab has created a robust M&S capability
- **Findings**
 - Existing tools are inadequate to support a SMART acquisition of an integrated Force Protection system
 - However, the foundation for a useful capability could be created by leveraging the resources of FCS and the USAF

Force Protection Study

15

The Panel was unable to identify any specific tools that the Army has assembled to support the acquisition of FP systems. However, the FCS program has assembled and employed several tools that could conceivably be adapted to support the needs of the FP acquisition community. As an example, the Modeling Architecture for Technology and Research Experimentation (MATREX) will reach across all labs within RDECOM to ensure that the necessary architecture is in place to facilitate modeling and simulation experimentation and improved interoperability with the FCS Lead Systems Integrator, the Army Test and Evaluation Command (ATEC), and Training and Doctrine Command (TRADOC). In addition, the USAF has established the Force Protection Battlelab (FPB) in San Antonio, TX. The FPB also has a robust M&S capability and has conducted multiple performance-based assessments that include analytical models and numerous force-on-force exercises using human-in-the-loop simulations.

The Panel concluded that there is little emphasis on FP in key Army acquisition related activities (e.g., the TRADOC Battle Labs, RDE MATREX). Consequently, existing tools are inadequate to support a SMART acquisition of a potential future integrated FP system. However, the foundation for a useful SMART capability could be created by leveraging the resources of FCS and the USAF.



Selected Recommendations: Modeling and Simulation (1 of 3)



- Overall
 - Generate a Plan of Action and Milestones (POAM) for FP M&S
 - Create a Force Protection Focus Area Collaborative Team (FACT) to
 - Institutionalize a Army-led FP Community of Interest
 - Prioritize the allocation of resources for FP-related M&S activities
- Education & Training (E&T)
 - Develop a family of E&T tools to support the just-in-time force protection needs of all echelons (e.g., from theater commanders to “strategic privates”)
 - Enhance the ability to address force protection issues in exercises
 - Make force protection an integral part of future routine, regular exercises
 - Develop automated tools to enhance efficiency, effectiveness of planning, executing, and evaluating force protection exercises (e.g., extend and exploit the capability provided by emerging web-based tools such as CHESSE)
 - Collect data during those exercises to characterize force protection proficiency


Force Protection Study


16

Since there are several key M&S needs that cut across all of the functions that M&S supports, an overall Plan of Action and Milestones (POAM) for FP M&S is required. This plan should help to identify and prioritize the most critical M&S investments needed to enhance FP and establish organizational initiatives to facilitate communications and coordination across the heterogeneous FP community. One mechanism for enhancing community communications and coordination would be to adapt a concept that the Army Modeling and Simulation Office (AMSO) has created: the Focus Area Collaborative Team (FACT). Historically, the goal of such teams is to promote shared, collaborative research from credible sources and subsequently eliminate duplicate efforts (Reference 17). The Panel recommends that the FP FACT transcend that goal to explore all the collaborative efforts needed to research, develop, and apply relevant FP M&S products. We believe all of the other Services should be integral members of the FP FACT and that other affected organizations (e.g., DTRA, DARPA, DHS, allies) should be participants.

In the area of E&T, it is recommended that a family of E&T FP tools be developed to support the just-in-time FP needs of all echelons. To “jump start” this process, the Army should adapt useful products from other Services (e.g., the USMC CDR) and prototypical tools (e.g., ICT’s Full Spectrum Warrior) and evolve them to meet future needs. Particular attention should be given to the development of the tools needed to provide E&T for senior decisionmakers so that they are prepared to deal with the strategic ramifications of FP incidents. As one element of that tool kit, additional emphasis should be given to seminar games (e.g., future versions of the Installation Transformation Wargame sponsored by the Office of the Assistant Chief of Staff for Installation Management (OACSIM) and organized by the US Army Corps of Engineers (Reference 18)).

Furthermore, steps should be taken to enhance the DoD’s ability to address FP issues in exercises. As an immediate action, FP must be stressed as an integral part of future routine, regular exercises. To make sure that these exercises can be conducted efficiently and effectively, given resource limitations, it is important to develop automated tools to support exercise planning, execution, and evaluation. It is recommended that the US Army Pacific’s web-based tool, CHESSE, be considered as a point of

departure for the development of a more complete exercise support tool. Those tools could also help analyze the data collected during those exercises to help characterize FP proficiency.



Selected Recommendations: Modeling and Simulation (2 of 3)



- Operations
 - Develop an integrated family of decision aids to help the commander and his staff conceptualize and formulate force protection strategies (e.g., assess risks associated with alternative courses of action)
- Assessment/experimentation
 - Develop a flexible tool kit of M&S and associated data bases (including upgraded versions of HAMER and selected agent based models) that enable the analyst to explore the implications of changes in DOTMLPF on force protection
 - Develop and employ tools to assess the impact of tactical force protection incidents at operational and strategic levels (e.g., IDA's SENSE)
 - Adapt Sandia's ADIDSS to support planning and investing in FP-related activities

Force Protection Study

17

In support of operations, many disjoint decision aids are emerging. Consistent with the recommendation of the Science & Technology Panel, we recommend that an *integrated* family of FP decision aids be developed to help the commander and his staff conceptualize and formulate FP strategies. These tools should support the full range of functions throughout the pre-, trans-, and post-attack phases of FP. This will preclude the creation and fielding of many independent systems with disparate data bases and human-machine interfaces (requiring the “fat fingering” of data among them). Since these tools will help the commander and his staff assess risks associated with alternative courses of action, it will require extensive education on how to interpret the products of these tools as a basis for sound decision making.

In support of assessment/experimentation, it is recognized that there is no single tool that can be developed to support the full needs of the analyst/experimenter. Consequently, we recommend that a flexible *tool kit* of M&S and associated data bases be developed to enable the user to explore the implications of changes of many dimensions of DOTMLPF on force protection. Based on the Panel’s experiences in performing analyses to support the summer study, we recommend that upgraded versions of HAMER and selected agent based models be considered for inclusion in that tool kit. A variant of this tool kit should be developed, which can be run on PCs, that the operational user can take to the field. Second, we recommend that assessment tools be developed and employed to assess the impact of potential tactical FP incidents at the operational and strategic levels. As a point of departure, consideration should be given to building on IDA’s SENSE product, a generalizable architecture for desktop distributed interactive simulation capable of simultaneously addressing economic, social, political, and military issues (Reference 19). Finally, to support the planning and investing in portfolios of FP-related products and activities, consideration should be given to adapting Sandia’s ADIDSS technology.



Selected Recommendations: Modeling and Simulation (3 of 3)



- Acquisition
 - Establish a Joint FP testbed with the USAF
 - Develop FP enablers and components for OneSAF
- Research
 - Enhance human behavioral representation in agent based models, and integrate into OneSAF
 - Improve the performance of key force protection decision support applications (e.g., plume prediction and course of action formulation for an urban environment)
 - Examine the use of Graphic Processing Units (GPUs) to support the high-performance computing requirements of FP models

Force Protection Study

18

The Panel recommends that a joint FP testbed be created to support the acquisition of FP systems. This testbed should subsume multiple subordinate testbeds reflecting the difference between the protection of fixed installations and mobile units (e.g., convoys, small squads). Since the USAF is interested in acquiring integrated base defenses for high value installations (e.g., airbases), the Army should work closely with them. If these testbeds are designed appropriately, they should enable the application of the SMART paradigm to FP acquisition.

OneSAF will be a composable, next-generation computer generated force (CGF) that can represent a full range of operations, systems, and control processes from individual combatant and platform to battalion level, with a variable level of fidelity that supports all M&S domains (Reference 20). We recommend that the requirement to support FP be added to the OneSAF program. This will require the development of FP enablers and components for OneSAF.

During the course of its deliberations, the Panel recognized that selected research activities were required to satisfy the needs of many of the recommended FP models and simulations. Three specific recommendations have been identified. First, it is important to enhance human behavioral representation in agent based models. It may be desirable to integrate the resulting tools into OneSAF. Second, research is required to improve the performance of key FP decision support applications. There is particular interest in improving our ability to do plume prediction and course of action formulation for an urban environment. Finally, the Panel recommends that Graphic Processing Units (GPUs) be considered to support the high performance computing requirements of FP models. With the increasing programmability of commodity GPUs, these chips are capable of performing more than the specific graphics computations for which they were originally designed. They are now capable coprocessors, and their high speed makes them useful for a variety of FP-related applications. They are particularly well-suited to numerical simulations such as those employed in plume prediction calculations (Reference 21).



Outline of Report



- Introduction
- Assessment of M&S Capabilities for Force Protection
- **Analyses to Support the Study**
- Summary

We are going to switch now from the subject of M&S tools and approaches and turn to the analyses that the Panel performed to support the summer study. First, we will discuss the key cases and issues of interest. Then we will summarize the insights that we derived from analyses of those cases. For each of the cases we will identify the postulated attack, characterize key issues and associated measures of merit, and identify who performed the analysis and the tool that they used. We will then depict key results that were derived by the application of the tool. We conclude each case by summarizing key lessons recorded from the assessment, potential options that might be pursued to mitigate the effects of the attack, and suggested analysis actions that should be taken to improve our ability to assess such cases in the future.



Approach to Analyses



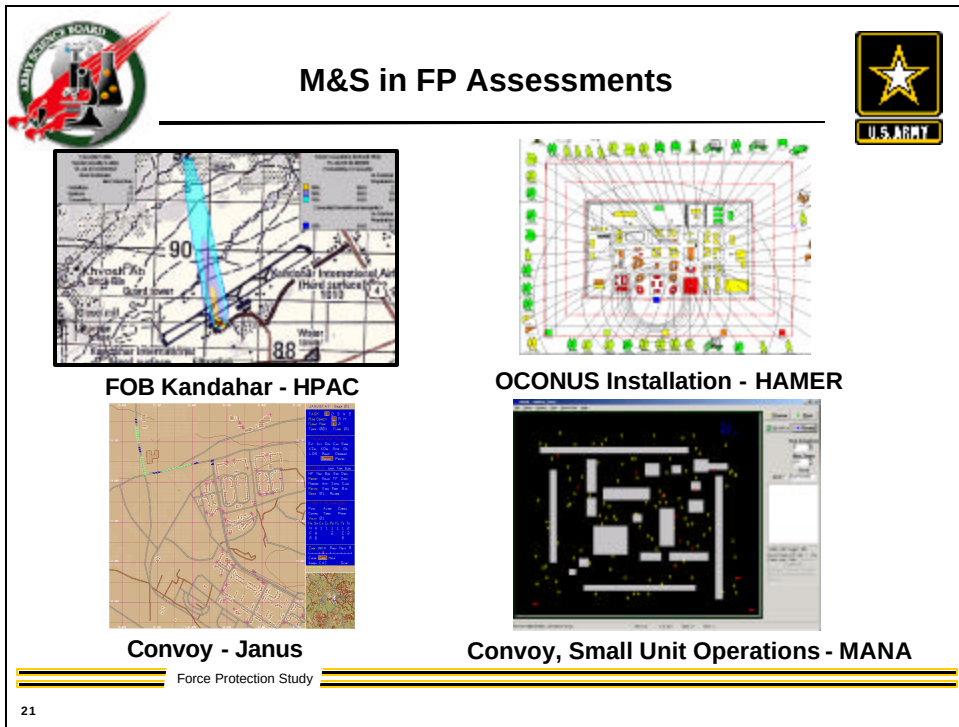
- Work within the functional framework developed to help structure the force protection problem (in concert with the Operations Panel)
- For selected cases, conduct parametric analyses to identify opportunities for enhanced force protection effectiveness and efficiency, drawing on
 - Lessons learned from operations
 - Operations Research tools (e.g., queuing analysis)
 - Constructive M&S (e.g., JANUS, HAMER)
 - Agent Based Models (e.g., MANA)
- Consistent with the candidate enhancements proposed by other panels, perform more focused DOTMLPF assessments

Force Protection Study

20

The Panel employed the following approach to its analytical efforts. First, it worked with the Operations Panel to develop the functional framework of FP activities cited above. That effort entailed decomposing the FP problem into phases (e.g., pre-, trans-, and post-attack), decomposing the phases into functions (e.g., predict, monitor, deny), and then identifying the key associated sub-functions (e.g., predict the likelihood that a potential adversary will launch an attack, using specified means, at a given time and place). An enumeration of these sub-functions is provided in Annex A. These results were used to provide a common frame of reference for the various panels supporting the overall study. Second, the Panel conducted a series of parametric studies for the six force protection cases selected by the study leadership. These initial studies were performed drawing on a variety of techniques. These include lessons learned from operations (e.g., articles collected by the Center for Army Lessons Learned on issues such as convoy protection (Reference 22)) and the use of relatively simple operations research techniques (e.g., the use of queuing analysis to explore the length of queues that can be anticipated as more stringent Force Protection Conditions (FPCONs) are implemented for alternative TTPs and mixes of portal sensing technologies). The bulk of the parametric analyses were performed using several constructive M&S that are depicted and discussed on the following page. These results were shared with the other panels to focus them on force protection problems that required mitigation.

Subsequently, when the other panels proposed materiel and non-materiel options to mitigate those problems, the panel performed analyses to provide initial estimates of their impact. These latter assessments were performed largely using Mana.



This slide depicts screen shots of the four tools that the Analysis and Modeling Panel used most extensively throughout the study. These tools were selected because they were well matched to the nature of the issues in question and their use was consistent with the constraints of the study (e.g., they were relatively simple to set up and run; we had access to analysts with extensive experience in the creative application of the tool).

HPAC is a plume protection model that is employed extensively to assess the consequences of biological and chemical emissions. Analysts from DTRA helped us apply the tool for assessments of the consequences of biological and chemical attacks to fixed facilities in CONUS or OCONUS.

HAMER is a physical damage assessment model for high explosive attacks against fixed installations. It was developed by Sandia and is currently hosted on a PC.

Janus is a high resolution constructive simulation that is widely employed by the assessment community. Rand used this tool to assess convoy vulnerability to ambushes and a variety of mines.

Mana is a distillation that models the behavior that emerges from the interaction of a specified set of Blue, Red, and non-combatant agents. This tool was originally developed by the New Zealand MoD to help them plan and assess stability and support operations in East Timor. The Panel had access to the High Performance Computer Center at Maui, HI, enabling us to perform responsively many runs of the model over a broad range of assumptions.



Selected Cases for Analysis



- CONUS Base
 - Norfolk (biological attacks)
- OCONUS Bases
 - Main Operating Base (MOB) - Kandahar (chemical attack)
 - Forward Operating Base (FOB) – Vehicular High Explosive (HE) Attack
 - Small Installation (FARP) -- Vehicular HE Attack
- Convoy
- Small Team (support to SASO)

Force Protection Study

22

This chart identifies the six cases that were selected for preliminary assessment. They were chosen to sample an interesting set of force protection cases.

The first four cases focus on fixed installations that are subjected to a variety of adversary attacks, including biological, chemical, and high explosives. Consistent with the focus of the overall study, emphasis is placed on fixed installations in the AOR. The latter range from relatively extensive concrete and wood facilities to hasty installations (e.g., tents) that are established to respond to tactical needs (e.g., a Forward Arming and Refueling Point (FARP)).

The final two cases focus on mobile Blue forces. These include a logistical convoy of trucks protected by escort vehicles and small teams performing a variety of SASO missions (e.g., patrolling in a market place).



Comments on Analyses



- A set of illustrative analyses have been performed for a representative set of FP Cases to
 - Assess Blue vulnerabilities
 - Identify options to mitigate Blue vulnerabilities
- The cases have been structured to reflect
 - Increasing probability of occurrence
 - Decreasing consequence
- Potential mitigating actions include
 - Detect
 - Delay
 - Respond

Force Protection Study

23

It must be emphasized that the analyses that the panel performed should be viewed as illustrative. They were conducted to illuminate potential Blue vulnerabilities and to suggest the potential benefits that could be achieved by the mitigating options identified by the other panels. In all cases, there was inadequate time and resources to perform the detailed exploration of the problem space that a thorough, rigorous analysis would demand. Thus, for each case we have suggested some of the additional analysis steps that should be taken to assess the issues further.

The six cases that have been selected represent an interesting continuum with respect to probability of occurrence and consequence. As one goes from Case I (i.e., protection of a base in CONUS against a biological attack) to Case VI (i.e., protection of a small team of soldiers on patrol), the probability of occurrence increases, but the consequence of the attack decreases.

Based on the insights developed in the analyses, the panel identified several potential mitigating actions. To structure these options, the panel used the taxonomy employed by Sandia.

- Detect: The actions taken by Blue to discover adversary actions.
- Delay: The actions taken by Blue to impede the progress of an adversary's attack.
- Respond: The actions taken by Blue to prevent adversarial success (e.g., interruption, neutralization).



Case I: CONUS Base (Norfolk)



- Attack
 - Biological agents (anthrax, smallpox)
 - Released from crop duster off shore
- Key issues
 - What is the consequence of such attacks?
 - What steps could be taken to mitigate those consequences?
- Measures of Merit
 - Population exposed
 - Numbers likely to get ill, die
- Assessment
 - Primary contributor: DTRA
 - Tool: HPAC (v4.03)

Force Protection Study

24

Case I envisions a biological attack from a crop duster flying off the coast near the Norfolk region of Virginia. That area is of particular interest to the DoD because of the large concentration of Army, Navy, and Air Force installations in the region.

The key issues of concern for such attacks include the potential consequences and the steps that could be taken to mitigate those consequences. In order to assess those issues, estimates are needed of the population exposed to the attack and the numbers of individuals likely to get ill and/or die.

DTRA has a WMD Analysis Cell at its Operations Center that is capable of assessing these measures of merit in near real time. The following results were generated by them using HPAC (V4.03).



Case IA: Norfolk Anthrax Attack



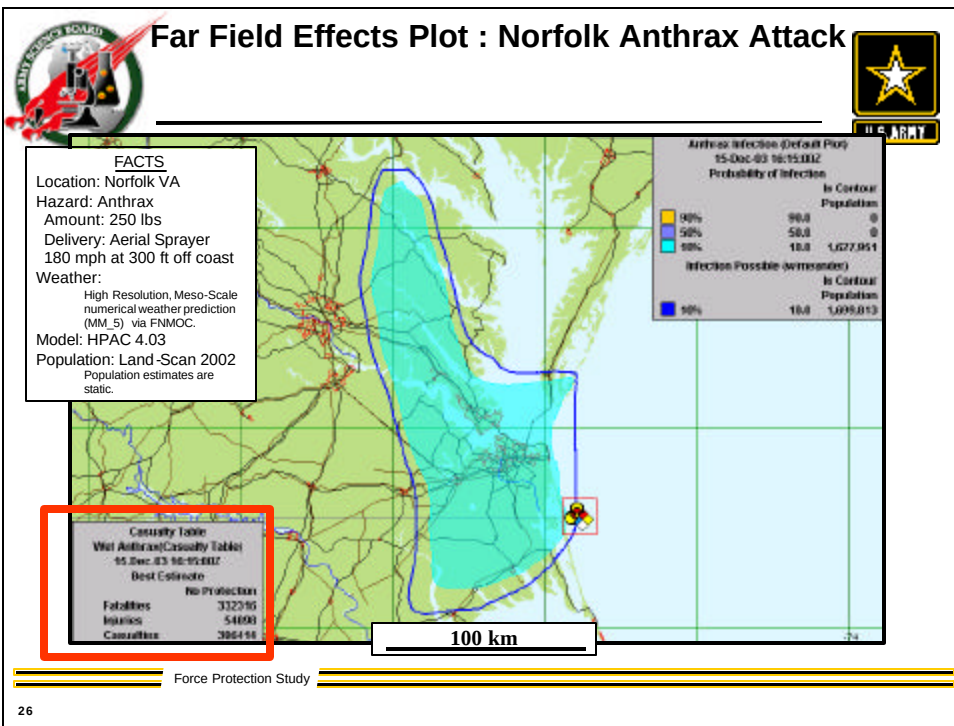
- Incident
 - Terrorist attack using anthrax against Norfolk area
 - Aerial sprayer
 - Starts at 36.55174N/075.7727W
 - 180 mph heading due North and spraying for 50 miles at 300 ft
 - 55 gallon drum (250 lbs at 20% efficiency, 20% pure and 50% dry)
 - Start time: 0100Z15Dec2003 (2000 local).
 - Comments:
 - Terrorist sprays just off shore anticipating early winter's evening sea breeze will spread anthrax inland to populated areas
 - Terrorist achieves low level dose (10% probability of casualty) over a very large area
- Analysis
 - Performed by DTRA
 - Model Used: HPAC (v 4.03)



Force Protection Study

25

As an initial case, it was assumed that the attackers employed an aerial sprayer on the crop duster to dispense anthrax. The specific geometry and dynamics of the attack are indicated on the slide. The calculations assume that the terrorist sprays just off shore anticipating that a characteristic early winter sea breeze will spread anthrax inland to populated areas. The geographic coverage of the attack is depicted on the following slide.



This slide depicts the far field effect plot for the anthrax attack generated using HPAC. It can be seen that the resulting anthrax cloud would cause a 10% probability of infection rate for a large area subsuming approximately 1.7 million people. DTRA estimated that in the absence of protection, approximately a third of a million people would die from the attack. Clearly, that number could be reduced substantially in the event of prompt, effective medical treatment.



Case IB: Norfolk Smallpox Attack



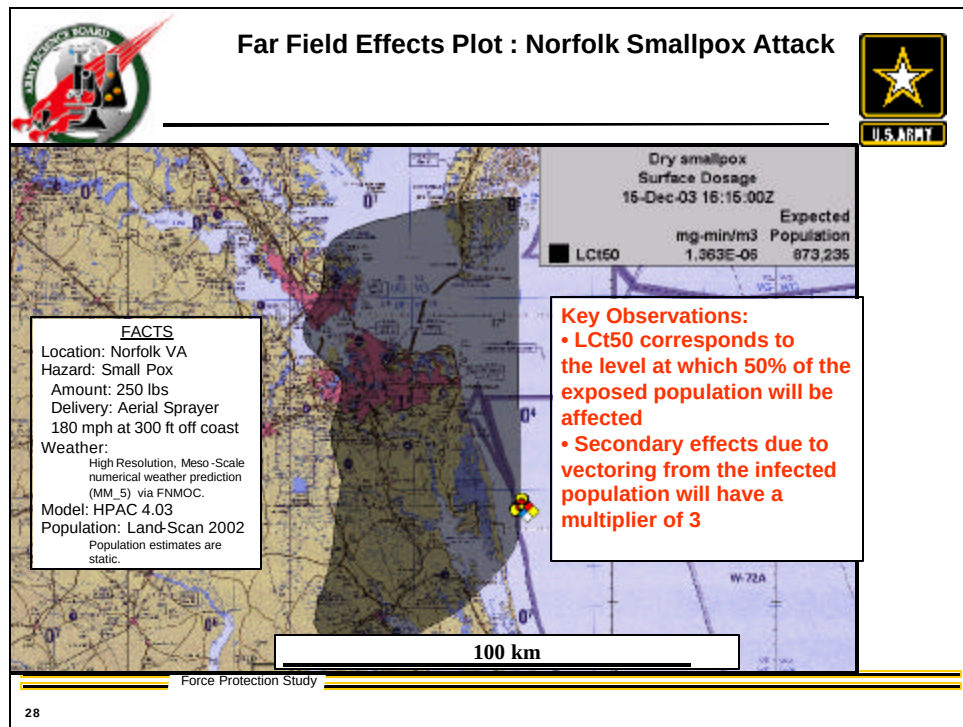
- Incident
 - Terrorist attack Norfolk with encapsulated smallpox
 - Aerial sprayer
 - Starts at 36.55174N/075.7727W
 - 180 mph heading due North and spraying for 50 miles at 300 ft
 - 55 gallon drum (250 lbs at 20% efficient and 20% pure)
 - Start time: 0100Z15Dec2003 (2000 local).
 - Comments:
 - Terrorist sprays just off shore anticipating early winter's evening sea breeze to spread smallpox inland to populated areas .
 - Terrorist achieves low level dose over a very large area.
- Weather
 - Historical Climatology from AFCCC based on 10 year data accumulation
- Analysis
 - Models Used: HPAC (v 4.03)
 - Comments: Standard Assumptions. Analyses only accounts for initial infection via airborne agent; secondary vectoring (person to person) not incorporated. Human effects limited to LCT-50 contour.



Force Protection Study

27

Since anthrax is not contagious, we requested that DTRA explore an alternative scenario in which the crop duster sprays encapsulated smallpox, a highly contagious disease against which most individuals are not vaccinated. The relevant assumptions are depicted on the slide.



The consequences of the smallpox attack are depicted on the above slide. The concentration of the cloud on the slide corresponds to the level at which 50% of the exposed population will be affected (i.e., LCt50 or $1.363\text{E-}06$ mg-min/m³). DTRA estimated that nearly 900,000 people would be exposed to that level of smallpox (or that approximately 450,000 people will become infected). However, since smallpox is highly contagious, the likelihood that it will be transmitted during its infectious stage can be described by a probability function. In a recent study by the Washington Institute (Reference 23), they elected to use an average of $R_0 = 3$. Thus, to a first approximation, the secondary effects due to vectoring from the infected population will have a multiplier of 3. Consequently, for the hypothetical attack, nearly 1.5 million people are expected to contract smallpox, a large percentage of whom are likely to die in the absence of prompt, effective medical treatment.



Case I: Preliminary Observations (1 of 2)



- Lessons Recorded
 - A biological attack will produce mass casualties, disruption
 - The worst case would be a contagious agent, due to vectoring
 - There are substantial advantages in reducing key time delays (e.g., detection, response)
- Mitigating Options
 - Detect -- as context, enhance intelligence to cue, warn key systems; e.g.,
 - Airborne Early Warning (AEW) aircraft
 - Data collection of contaminants
 - Clinical monitoring (e.g., hospitals, pharmacies)

Force Protection Study

29

Based upon these preliminary analyses, the following lessons were recorded. The analyses confirmed the hypothesis that a biological attack would produce mass casualties and disruption to the targeted area. Because of the multiplicative effects of vectoring, the worst case (with respect to infected victims and consequent fatalities) would occur if the adversary employed a contagious agent. Given the timeline of such an attack and its consequences, it is concluded that there are substantial advantages to reducing key time delays in detecting the attack and responding to it.

There are several potential mitigating options that could ameliorate some of the consequences of such a hypothetical attack. Early detection could be of value at several points in the timeline. First, if reliable HUMINT could warn of the imminence of such an attack, key airborne assets could be positioned to support the early detection and neutralization of the attacking vehicle. In this case it would require placing Airborne Early Warning (AEW) aircraft on orbit supported by airborne interceptors on combat air patrol. Under suitable rules of engagement, it might be feasible to detect, track, classify, and neutralize the crop duster before it were capable of fully discharging its biological agent. Second, if the crop duster were able to discharge its load, there would be substantial benefit in being able to detect and predict the path of the contaminant plume as early as possible. This would enable the decision maker to take steps to minimize the population's exposure to the agent (e.g., directing the population in the effected region to stay indoors). Finally, if the crop duster and contaminant plume escaped detection, there would be substantial value in detecting the presence of the disease in the community as rapidly as possible. This could be effected by implementing a clinical monitoring program to detect the early presence of the disease in hospitals or the atypical purchase of over-the-counter drugs to treat the initial symptoms of the disease.



Case I: Preliminary Observations (2 of 2)



- Mitigating Options (Concluded)
 - Delay -- understand characteristic timescales of key phenomena; e.g.,
 - Cloud (to apply mitigating agents)
 - Disease (to respond accordingly)
 - Respond
 - Medical response (based on ordered decision process, including situation assessment and associated C2)
 - Clean-up operations (e.g., applications of sprays, foams)
- Analysis Actions
 - Upgrade our ability to deal with plume detection and monitoring
 - Improve data collection
 - Upgrade HPAC (through Joint Effects Model (JEM))
 - Improve displays (reflecting probabilistic nature of the phenomena)
 - Train analysts and decision makers on tools and their use
 - Develop and deploy tools to support consequence management (perhaps agent based models); e.g.,
 - Traffic flow
 - Medical operations

Force Protection Study

30

Second, if the characteristic timescales of several key phenomena associated with the attack are known, it may be feasible to undertake selected delaying actions to mitigate the effects of the attack. For example, if the diffusion characteristics of the contaminant cloud are understood, it might be feasible to spray mitigating agents on the cloud to limit its impact. Sandia is developing such agents to neutralize the effects of biological and chemical contaminants. In addition, a knowledge of the characteristic timelines of the disease can help the medical community take action to mitigate its effects.

Finally, if the medical community is able to achieve effective situation assessment and associated command and control of its resources, it should be able to implement an ordered decision process to minimize the loss of life and disruption to the community. Furthermore, in the aftermath of such an attack, there is a need to mount coordinated clean-up operations (e.g., applications of appropriate sprays and foams) to restore the affected area. This latter operation may be of particular significance if the attack were designed to hinder the ability of the military to deploy military forces from the affected region.

Analytically, there are a number of actions that should be taken to enhance our ability to cope with such an attack. First, as cited earlier in this report, there is a need to upgrade our ability to deal with plume detection and monitoring. As discussed in a recent National Academy of Sciences report (Reference 10), this will require four orchestrated actions. First, improve the data collection process (e.g., increased spatial and temporal sampling of the environment). Second, improve the prediction algorithms that are currently employed. Steps are underway to do so in the Joint Effects Model (JEM) program (Reference 11) which are developing algorithms to improve plume prediction for a broad set of important operational conditions (e.g., inside buildings). Third, improve how the prediction is displayed to the decision maker to reflect the probabilistic nature of that prediction. Finally, analysts and decision makers must be educated on the capabilities and limitations of such tools and trained on their effective use.

Furthermore, there is a need to develop and deploy a suite of tools to support consequence management. This would include credible traffic models to explore the potential consequences of options to evacuate the population from the effected area and models of medical operations to support the allocation of scarce medical resources. Agent based models may of value in these latter assessments.

Tools such as HPAC are less accurate modeling CBRN effects in certain environments where definite FP implications exist, therefore, improvement of the current suite of tools capable of performing accurate CBRN analyses is required to make the best FP decisions.

We must also explore the need for tools to support consequence management (first responders). This is an area that has been overlooked for too long but has become more prominent with regard to today's situation.



Case II: OCONUS MOB (Kandahar)



- Attack
 - Chemical agent (Sarin)
 - Delivered by mortar
- Key issues:
 - What losses are incurred by such an attack?
 - To what extent can the losses be reduced by extending keep out range?
- Measure of Merit
 - Population on Main Operating Base (MOB) that is killed, incapacitated
- Assessment
 - Primary contributors: DTRA, Sandia
 - Tool: HPAC (v4.03)

Force Protection Study

31

Case II envisions a chemical attack delivered by a hastily set up and fired mortar against the Main Operating Base (MOB) at Kandahar, Afghanistan. This facility is particularly vital to US SASO efforts in the region. It is hypothesized that an adversary might employ Sarin, a non-persistent chemical agent that Aum Shinrikyo employed in their attack in the Tokyo subway system.

The key issues of concern include the potential losses that might be incurred by such an attack and the potential mitigation that can be achieved by extending the keep out range around the base. In order to assess those issues, estimates are needed of the potential number of people on the MOB who would be exposed to the nerve agent and the potential number of casualties.

To illuminate those issues, the Panel again utilized the services of the DTRA WMD Analysis Cell. The following results were generated by them using HPAC (V4.03).



Case II: Kandahar Chemical Attack

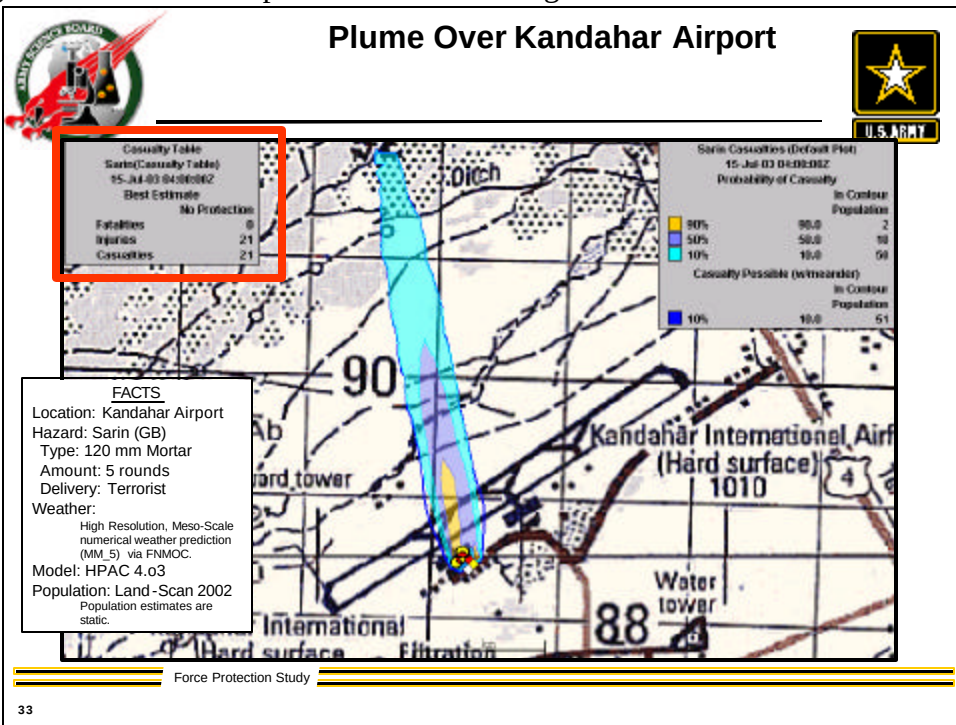


- Incident
 - Terrorist chemical attack on Kandahar Airport, AF
 - 5 chemical rounds from a 120 mm mortar
 - 31.49963N/065.84522E
 - 2.6 kg of Sarin (GB) in each round
 - Time: 0400Z15Jul2003
 - Event: Five round mortar attack
- Weather
 - High Resolution Numerical Weather Prediction: MM-5 from AFWA
- Analysis
 - Performed by DTRA
 - Model Used: HPAC (v 4.03)

Force Protection Study

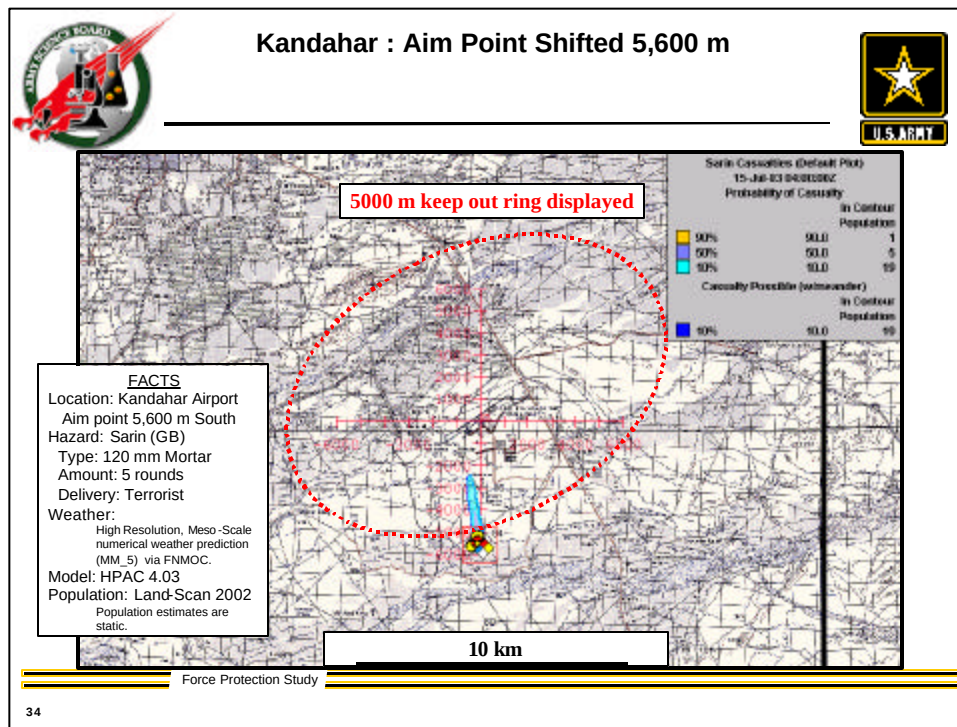
32

As an initial case, it was assumed that the attackers rapidly set up a 120 mm mortar, 600m from perimeter of the Kandahar MOB, and fired fire rounds, each filled with 2.6 kg of Sarin. Meteorological conditions that are representative for a mid-July day were also assumed. The geographic coverage corresponding to that attack are depicted on the following slide.



This slide depicts the resulting plume for the Sarin attack generated using HPAC. It can be seen that the resulting cloud would subsume 2 people with 90% probability of casualty, 10 people with 50% probability of casualty, and 50 people with 10% probability of casualty. These numbers are relatively

robust because in the event that the plume would meander, it is estimated that 51 people would be subject to 10% probability of casualty. Consistent with those statistics, it is estimated that in the event that no protection were available to the the personnel on the MOB, there would be no fatalities arising from the attack, but there would be 21 casualties.



To explore the impact of increasing the keep-out range, DTRA evaluated the consequence of shifting the aim point of the Sarin attack to a distance 5.6 km from the MOB. As can be seen in the accompanying slide, the resulting plume provides considerably less coverage of the Kandahar MOB. The corresponding probability of casualties is also reduced appreciably (e.g., the resulting cloud would subsume 1 person with 90 % probability of casualty, 5 people with 50% probability of casualty, and 19 people with 10% probability of casualty). These numbers are relatively robust because in the event that the plume would meander, it is estimated that 19 people would be subject to 10% probability of casualty.



Case II: Preliminary Observations



- Lessons Recorded
 - Consequences of chemical attack are less dramatic than a biological attack (e.g., non-persistent, fewer casualties)
 - Value of enhanced early warning, stand-off
- Mitigating Options
 - Detect
 - Sensors to detect weapons/adversaries at extended ranges
 - Timely location of weapon launch point
 - Respond
 - Improved MOPP gear
 - Enhanced training, exercises
- Analysis Actions
 - Deploy site analysis tools (e.g., assist in selecting sites, siting sensors)
 - Develop a family of decision aids (e.g., help predict Red intent)
 - Provide operational commander with physical security tools to help identify, ameliorate vulnerabilities

Force Protection Study

35

These preliminary assessments reveal that the consequences of a chemical attack against a fixed installation would be considerably less dramatic than the biological attacks described above. By comparing the two cases it can be seen that the biological attack would give rise to several orders of magnitude more casualties than the non-persistent chemical attack. In addition, even these relatively modest casualties arising from the chemical attack could be reduced appreciably with enhanced early warning and increased stand-off distance.

There are several potential mitigating options that could ameliorate some of the consequences of such a hypothetical attack. First, sensors could be deployed around the periphery of the MOB to detect weapons/adversaries at extended ranges. If this information were fused and presented to the decision maker in a timely way, it might provide enough lead time to vector resources to the area (e.g., a patrol, an attack helicopter, an armed UAV, high power microwaves) to facilitate a pre-emptive strike against the attackers. If that were not feasible, it might be desirable to have a counter-mortar capability at the base to detect, locate, and characterize the attack. Although this capability would not help avert the attack, it might be able to support an effective retaliatory strike against the attackers.

Several response options may be feasible to mitigate the effects of the attack. First, improved MOPP gear (e.g., light weight, properly fitted masks) would serve to reduce the number of casualties in such an attack. Second, enhanced training and exercises would ensure that Blue forces are well-versed on TTPs to minimize their exposure to the chemical agents.

Analytically, there are a number of actions that should be taken to enhance our ability to cope with such an attack. First, site analysis tools should be deployed to assist the decision maker in selecting sites and siting sensors around the facility. Second, a family of decision aids should be developed to help support the actions that should be taken prior to an attack (e.g., help predict adversary action; identify factors that should be monitored as precursors of an attack; understand prevailing meteorological conditions). Finally, the operational commander should be provided with security tools (e.g., a variant of Sandia's suite of tools) to help identify and ameliorate vulnerabilities.



Case III: Forward Operating Base (FOB) (Central Asia)



- Attack
 - HE delivered by a vehicle
 - HE range: 1,000 - 30,000 lbs TNT (equivalent)
- Key issue
 - What level of adversary stand-off must be achieved if damage sustained is to be “acceptable”?
- Measure of Merit
 - Level of damage sustained by buildings on the FOB
- Assessment
 - Primary contributor: Sandia
 - Tool: HAMER

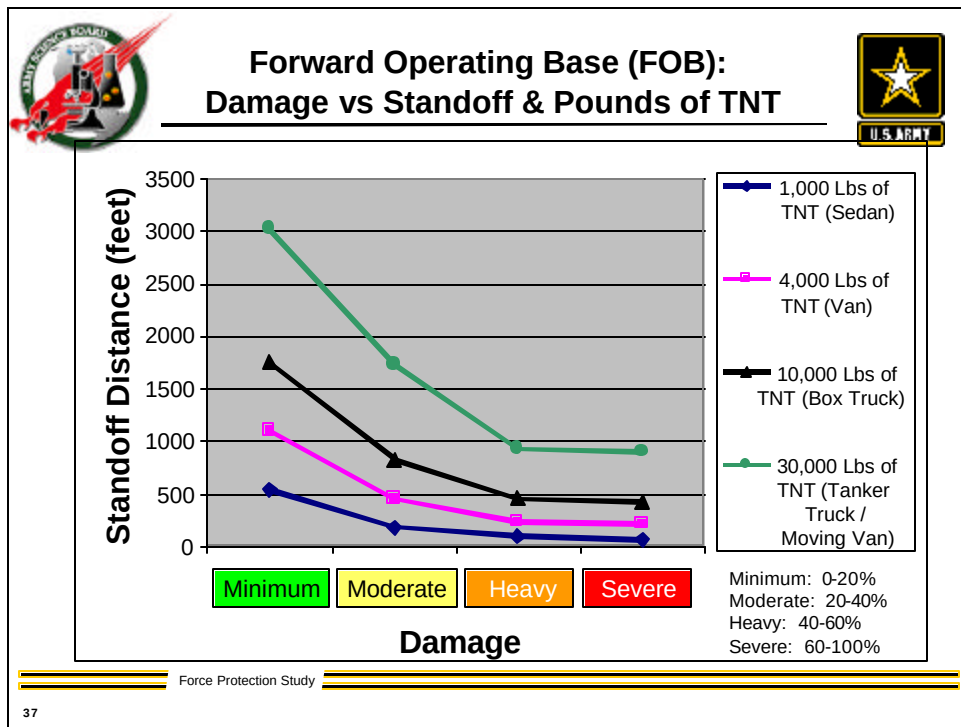
Force Protection Study

36

Case III envisions a high explosives (HE) attack against an OCONUS Forward Operating Base (FOB). The hypothetical base in question is comprised of a mix of concrete and wooden buildings that one might find at a future FOB in Central Asia. A variety of vehicular threat options are feasible ranging from the equivalent of 1,000 pounds of TNT (which could be secreted in a sedan) to the equivalent of 30,000 pounds of TNT (which would require a vehicle the size of a tanker truck or a moving van). The key issue is the standoff distance that must be achieved (as a function of the type of delivery vehicle/amount of HE) if the resulting damage is to be “acceptable”.

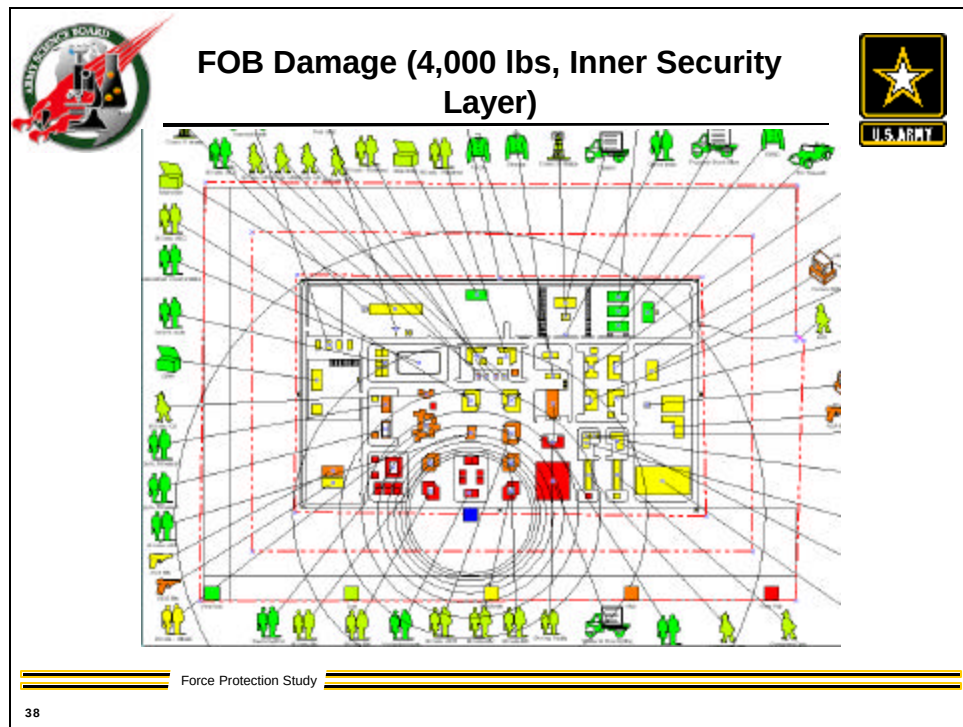
In order to assess that issue, the level of damage sustained by buildings on the FOB must be calculated as function of the amount of HE employed and the location where the bomb is detonated. Damage is measured as percentage of the FOB destroyed. (i.e., 0-20% destruction equates to minimal damage, 20 - 40% to moderate damage, 40 - 60% to heavy damage, and 60 - 100% to severe damage).

Sandia conducted the analysis utilizing a tool called HAMER. It is a physics-based model capable of accurately representing different properties within a selected base of operations including numerous structural designs. HAMER then calculates the blast effects against selected targets of interest on the base. It is capable of calculating damage to physical structures as well as the occupants, materiel, and other infrastructure within the base. Other features allow the user to test “what if” countermeasures to mitigate the effects of the attack and compare several courses of action (COAs), ultimately assisting leaders in making informed decisions on what are the most effective FP measures to implement. Tools like HAMER can be run on a PC/laptop and could be available to the commander to support FP decisions.



The slide illustrates the percentage of damage to the FOB from varying yields of high explosives as a function of the distance from the perimeter of the FOB at which it is detonated. These results can be used to identify the stand-off performance that the FP system must achieve if the risk of damage to the FOB is to be minimal (i.e., in the 0 to 20% range). Thus, as bounding cases, the mix of FP systems and procedures must ensure that suspicious cars are kept at stand-off distances beyond 500 feet while suspicious moving vans or tanker trucks are kept at stand-off distances beyond 3,000 feet. If it is infeasible to achieve these stand-off distances because of siting restrictions, the slide reveals the risk of damage that the Commander must be willing to assume (e.g., if the stand-off distance for a tanker truck can not be kept at ranges beyond 1,700 feet, the Commander must be willing to tolerate moderate damage in the event of an HE attack characterized by 30,000 pounds of TNT equivalent). In addition, the slide indicates that once the attacking vehicle is close enough to achieve heavy damage, very small reductions in stand-off will cause severe damage. These consequences are so severe that extreme steps must be taken to ensure that, with very high confidence, an adversary is not able to get within these limited stand-off ranges. These factors should be factored into the rules of engagement that the Commander implements.

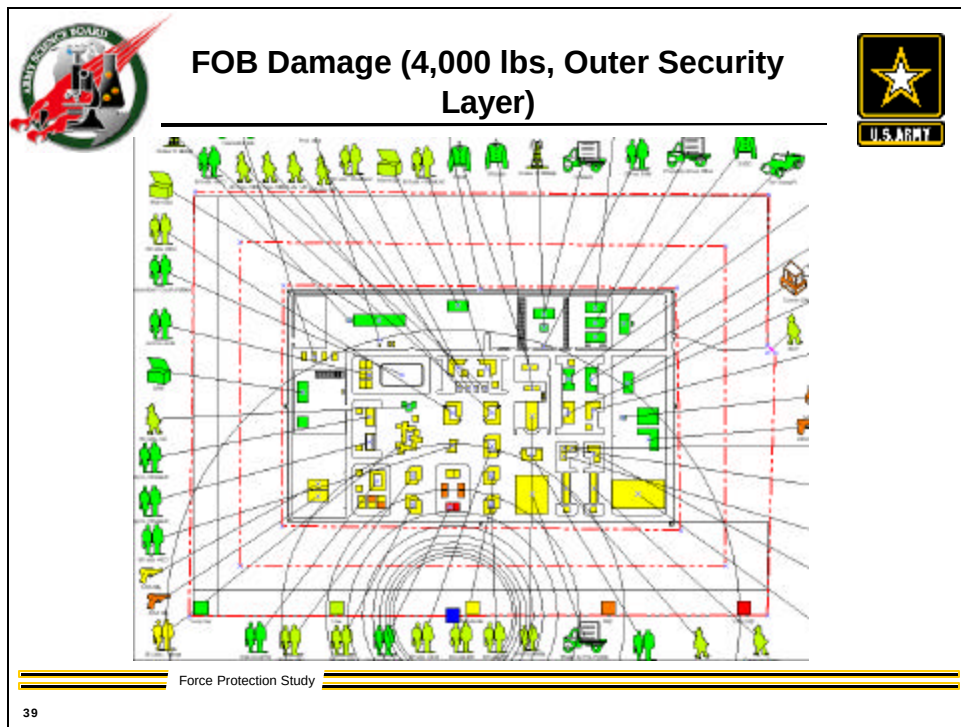
Note that these stand-off values are appropriate for the mix of facilities assumed for a canonical FOB. It is vital that the Commander of a specific FOB employ actual facility data to compute the corresponding curves for his base.



To illustrate the insights that can be derived using HAMER, this slide and the following one depict the damage to the FOB that would be sustained if a van filled with the equivalent of 4000 pounds of TNT were to be detonated at two different stand-off ranges.

In the above slide, the van is presumed to detonate at the Inner Security Layer. The bright blue square is the point of detonation with pressure ring waves (in increments of 1 psi pressure wave rings out to 10 psi) going out from that point. The colors of the buildings reflect the calculated blast damage while the symbols around the site layout represent a range of asset categories at risk (e.g., mission critical personnel, vehicles). The scale provided below characterizes the calculated percent damage level and damage description corresponding to the indicated color. Blast damage is derived from empirical data developed from a variety of sources (e.g., Navy). The blast effects were determined from an assessment of the impact of an incident blast wave.

- Red - 60-100% - severe; collapse of structure/massive destruction
- Orange - 40-60% - heavy; large deformation of structure members
- Yellow - 20-40% - moderate; some deformation of structural members, extensive nonstructural damage
- Green - 0-20% - minimal; light or local damage.



The above slide differs from the preceding slide in the offset distance where the van (loaded with 4,000 pounds of TNT equivalent) is presumed to detonate. In this case the explosion occurs at the Outer Security Layer, 600 feet further away from the facilities on the FOB. A comparison of the two slides indicates a dramatic reduction in the number of buildings and FOB assets that are subjected to heavy or severe damage. This difference highlights the value of being able to achieve enhanced stand-off ranges through an effective mix of physical barriers, systems, and procedures.

Case III: Preliminary Observations (1 of 2)

- Lessons Recorded
 - HE is a high probability of occurrence, moderate consequence threat
 - Achieving extended stand-off can mitigate significant damage to materiel, loss of life
 - Enhancing structural integrity (e.g., kevlar) can make a significant difference
- Mitigating Options
 - Detect
 - Stand-off detection, identification of vehicles, HE (e.g., use of robots, sniffers)
 - Delay
 - Implement barriers (fixed, pop-up), portals
 - Respond
 - Install blast deflectors, inhibitors (e.g., kevlar foam bladders that are deployed on warning)

Force Protection Study

40

Recent history has demonstrated that HE is a high probability of occurrence, moderate consequence threat [note: “moderate” suggests that loss of life can be limited to hundreds, vice the many thousands that may ensue from weapons of mass destruction]. The US has been subjected to HE attacks at barracks, embassies, and, more recently, tactical targets in Iraq. As suggested by the illustrative analyses in this study, significant damage to materiel and loss of life can be mitigated if stand-off ranges consistent with the size of the threat can be achieved. These ranges constitute benchmark values against which existing and proposed FP system performance can be measured. In addition, Sandia has performed additional analyses which demonstrate that if structural integrity can be enhanced (e.g., by deploying kevlar filled blankets over buildings), the damage to those facilities can be reduced substantially.

There are a variety of mitigating options that should be pursued to deal with this high probability threat. First, systems are needed to enhance the stand-off detection and identification ranges against threat vehicles and the HE that they are carrying. For example, the S&T community is exploring robotic vehicles containing HE “sniffers” that could be deployed at extended perimeters around FOBs. Second, to delay the progress of a potential attacker, a variety of barriers could be implemented (e.g., fixed, pop-up) and portals established to restrict their freedom of movement. Finally, to respond to an actual explosion, FOBs could be protected by installing blast deflectors or inhibitors. As an illustration of the latter, kevlar foam bladders could be prepositioned that would be deployed on warning of an imminent attack.

High explosive vehicular attacks have a high probability of occurrence, however the consequences of these attacks can be mitigated by employing varying FP strategies.

Achieving the necessary standoff distance required to mitigate the damage to men and material is the most effective FP countermeasure.

However, other FP options currently exist or are being developed to diminish the risks associated with this type of attack. Some options are: enhancements to structural integrity, standoff explosives detectors, threat vehicle identification systems, barriers (fixed or pop-up), and blast deflectors.



Case III: Preliminary Observations (2 of 2)



- Analysis Actions
 - Provide decision aids to operational users (e.g., upgraded HAMER) and train them on their use
 - Assemble enhanced, classified data bases for commanders of FOBs to assist them in their planning and operations

Analytically, there are a number of actions that should be taken to enhance our ability to cope with such an attack. First, decision aids should be provided to operational users and they should be trained on their use. One element of that suite of decision aids should be Sandia's HAMER, updated to reside on a modern platform. Because of time and resource limitations, this study did not pursue timeline analyses to explore the options that are available (e.g., evacuation of high risk facilities) if adequate delays can be inflicted on the attacker. However, such timeline analysis tools are available and, with adaptation, they should be added to the commander's suite of tools. Second, these tools are of limited utility unless an enhanced, classified data base for the FOBs is collected, converted, verified, validated, and certified. By doing so it will greatly enhance the responsiveness of the commanders of FOB as they conduct their plans and operations.



Case IV: Forward Arming and Refueling Point (FARP) (Middle East)



- Attack
 - Moderate yield HE attack (1,000 - 10,000 lbs of TNT, equivalent)
 - Vehicular delivery
- Key issue
 - What level of adversary stand-off must be achieved if damage sustained is to be “acceptable”?
- Measure of Merit
 - Damage to installations (e.g., tents, fuel bladders)
 - Damage to weapons platforms
- Assessment
 - Primary contributor: Sandia
 - Tool: spread sheets



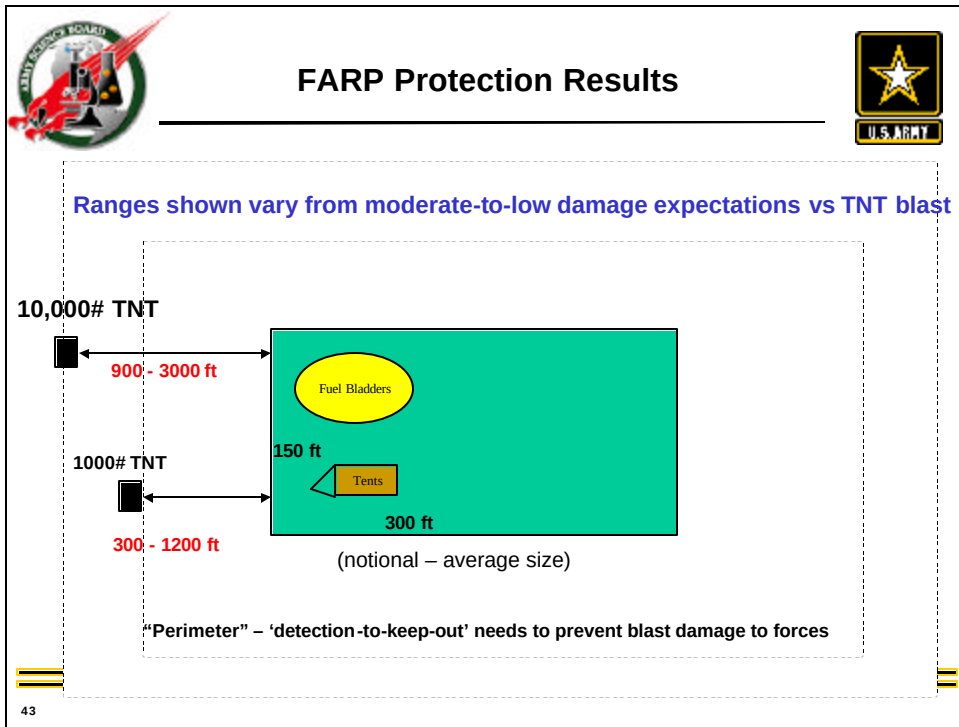
Force Protection Study

42

Case IV envisions an HE attack on an OCONUS FARP. It is assumed that the FARP was established with little pre-planning to satisfy tactical logistical needs. The FARP structures are relatively soft (e.g., tents, fuel bladders) and the perimeter is generally delineated by concertina wire. The hypothesized method of adversary attack is by vehicle (e.g., car or truck carrying HE).

The key issue analyzed is the level of adversary stand-off that must be achieved if damage sustained to the FARP is to be “acceptable”. The primary measure of merit is the damage that the structures and facilities on the FARP sustain if a specified explosive is detonated at a specified stand-off distance. Attention is focused on determining the conditions when the damage corresponds to moderate-to-low levels.

The primary contributor to this analysis was Sandia utilizing several spread sheet tools to perform the calculations.



Two hypothesized threats were examined: a car carrying the equivalent of 1,000 pounds of TNT and a truck carrying the equivalent of 10,000 pounds of TNT.

Standoff ranges were calculated to determine the minimum amount of standoff distance required to ensure that any losses to the FARP facilities (e.g., tents, fuel bladders) resulting from this type of attack would be acceptable (i.e., moderate-to-low damage).

For example, to sustain low damage from a car carrying the equivalent of 1,000 pounds of TNT, a standoff distance of 1,200 feet is required; moderate damage can be expected if the standoff range is shortened to 300 feet. The corresponding standoff distances for a truck carrying the equivalent of 10,000 pounds of TNT are 3,000 feet (for low damage) and 900 feet (for moderate damage).

The challenge is to determine a mix of physical (e.g., temporary barriers), materiel (e.g., sensors; non-lethal weapons such as high power microwaves), and TTP (e.g., patrols) options consistent with the standoff distances depicted above. In many instances, the commander's freedom of action will be limited by physical constraints (e.g., presence of proximate buildings) and rules of engagement.



Case IV: Preliminary Observations



- Lessons Recorded -- Due to inherent vulnerabilities of a hasty base
 - Site planning is critical
 - Extended detection, identification, and keep-out ranges are vital
- Mitigating Options
 - Detect
 - Mix of long range sensors (e.g., radars, FLIRs, multispectral imagery)
 - Delay
 - Mobile techniques to enforce keep out (e.g., HPM)
 - Respond
 - Readily transportable barriers
- Analysis Actions
 - Develop a family of decision aids for operational users
 - Incorporate hasty base defense in training M&S

Force Protection Study

44

Establishing and operating a FARP is an inherently vulnerable mission. FARPs are normally hastily established, lightly defended, and expose soldiers to many potential threats.

HE vehicular attacks have a reasonably high probability of occurrence so site planning is critical.

Choosing a FARP site that allows for extended detection ranges and increased standoff distance is vital to mitigate damage to personnel and materiel.

Strategies for ameliorating damage exist and include a mix of long range sensors for early detection, identification, and classification (e.g., radars, forward looking infrared (FLIR), multispectral imagery); techniques to delay attacks (e.g., high power microwaves); and easily transportable and erectable barriers to extend keep out ranges. However, these strategies are predicated on good site selection to achieve the standoff distances cited above for the various categories of threats.

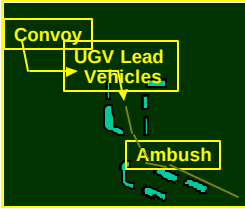
Analytically, there are a number of actions that should be taken to enhance our ability to cope with such an attack. First, a family of decision aids should be developed for operational users to help them perform all of the functions associated with pre-, trans-, and post-attack. Second, training M&S tools should be augmented to incorporate planning and implementing hasty base defense.



Case V: Convoys



- Attack
 - Dismounted ambush party using mine detonation to initiate attack on friendly convoy
- Key issue
 - What losses are incurred by such an attack?
 - What DOTMLPF changes are necessary to improve FP of convoys?
 - What are the near and far term materiel enhancements (e.g., armed UGV, UAV, use of obscurants, ballistic appliqué, improved C2)
- Measure of Merit
 - Average convoy losses
- Assessment
 - Primary contributor: MITRE, AMSO
 - Tool: MANA
 - Prior convoy assessments
 - RAND's support to ASB, Counter-mine studies (JANUS)
 - Sandia's assessments of convoy ambushes (JBS)



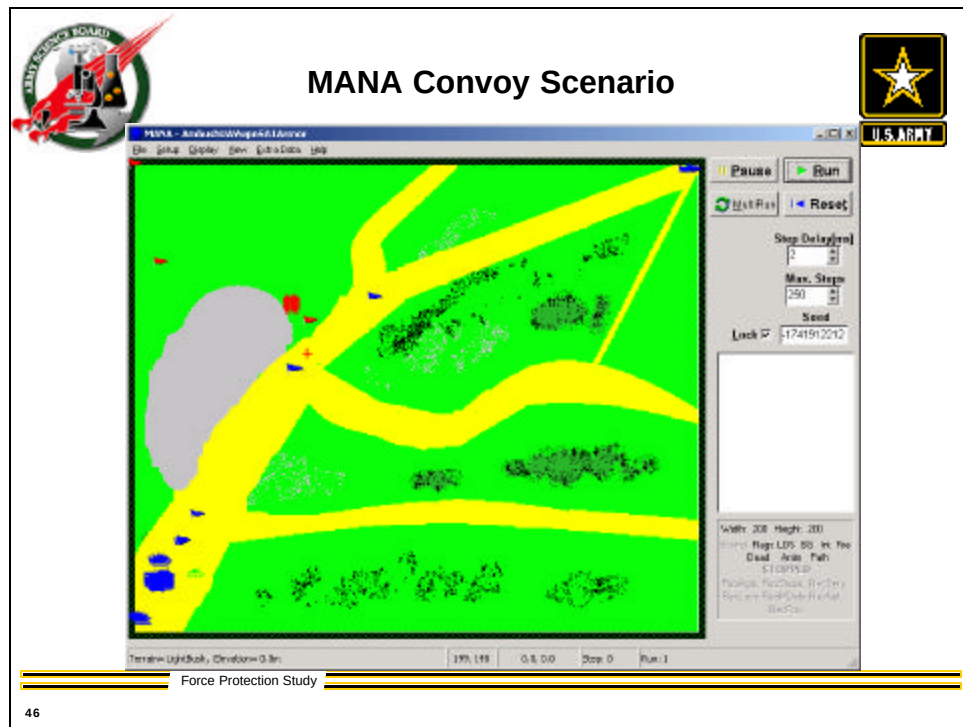
Force Protection Study

45

Case V envisions a dismounted armed ambush on a convoy carrying logistical products (e.g., food, ammunition, petroleum, oil, and lubricants (POL)). It is assumed that the attack is initiated by detonation of a mine.

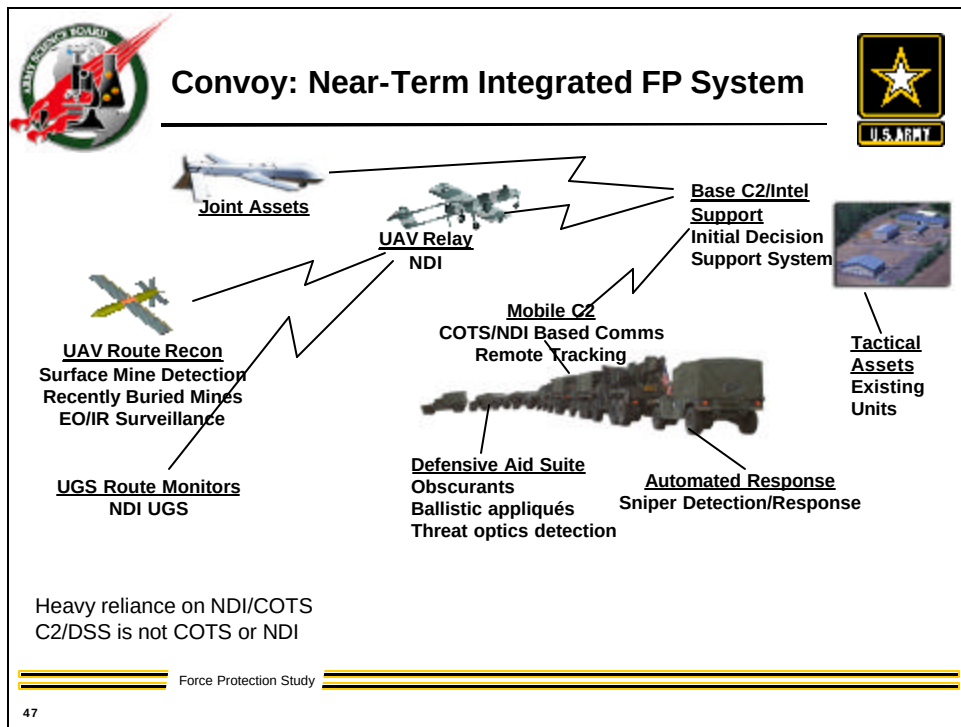
A variety of issues were addressed during the course of this analysis. These include the losses that are incurred by such an attack, the changes in DOTMLPF that are needed to improve FP of convoys, and the contribution of near- and far-term materiel enhancement on FP effectiveness. In the latter area, candidate materiel solutions include armed unmanned ground vehicles (UGVs), unmanned aerial vehicles (UAVs), use of obscurants, ballistic appliques to harden the convoy vehicles, and improved C2 (i.e., enhanced C2 intra-convoy and between the convoy and home base). In these analyses, the primary measure of merit was the average losses that the convoy sustained in the attack.

The primary contributors to this analysis were analytic personnel from MITRE and AMSO. These analysts used the Mana Distillation as their primary tool. To initiate their analyses, they reviewed prior convoy assessments (e.g., RAND's support to the 2001 ASB Summer Study (Reference 24) and the recent counter-mine study (Reference 25)) and Sandia's assessments of convoy ambushes. To calibrate their tools, the analysts first demonstrated that they could derive results that were consistent with RAND's earlier JANUS-based studies, using the Mana Distillation. As a second step, parametric studies were used to identify interesting breakpoints in capability and to stimulate dialogue with the Operations and S&T Panels. Subsequently, specific materiel recommendations by the S&T Panel were assessed to help prioritize future actions.

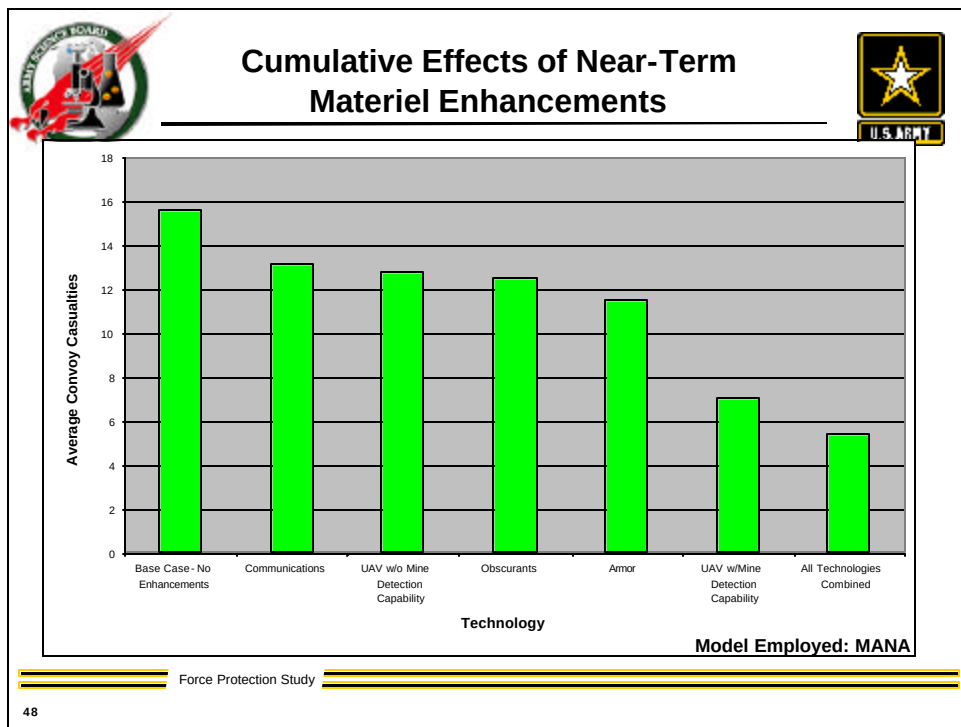


The Mana Distillation, developed by the New Zealand Defence Technology Agency, is an agent-based cellular automaton model, used to generate the scenarios and data analysis for the convoy force protection case. Mana is part of the Project Albert suite of Distillation modeling and analysis tools. Project Albert is a program sponsored by the Marine Corps Warfighting Lab to research new modeling and analysis tools and techniques, which address the phenomena of nonlinearities, intangibles, and adaptive decision making, often not represented or represented poorly by current tools and techniques. For a more detailed description of both Project Albert and the Mana model, refer to Appendix A. The slide depicts a Mana screen shot of the convoy scenario. The base scenario illustrates a convoy of blue trucks with associated escort units in a column formation. The convoy consists of two escort units of 5 HMMWVs each, one in the lead and one in the rear, and a supply unit with 30 trucks. The convoy is traveling in an environment with rolling hill terrain and a partially developed road network. It is assumed that the convoy is en route to a humanitarian assistance site. An ambush has been set up to disrupt the convoy from completing its mission. The ambush party is a dismounted party with 24 members. The ambush party has buried a mine in the road to create a blockade either to stop or to disable the convoy.

Simple terrain features are represented in Mana through color. The gray area represents an obstacle, such as a mountain, which fully impedes movement and line of sight of the convoy vehicles. The yellow areas represent easily trafficked terrain such as roads, and the dark and light green areas represent light and dense brush which partially impede movement and sight. The red plus sign represents the mine in the middle of the road, used to initiate the ambush. The red agents clustered to the right of the gray obstacle are the ambush party, which run out to attack the convoy after the mine detonates. The blue vehicle agents represent the various members of the convoy. The colored flags represent waypoints for either the convoy vehicles or the ambush party. The waypoints represent a set of objective points or a defined patrol route to help direct movement of the agents in a particular direction.



This slide indicates near term technologies identified by the S&T panel to mitigate risk to convoy operations. For further details refer to the S&T panel report on recommended near term technological solutions to FP.

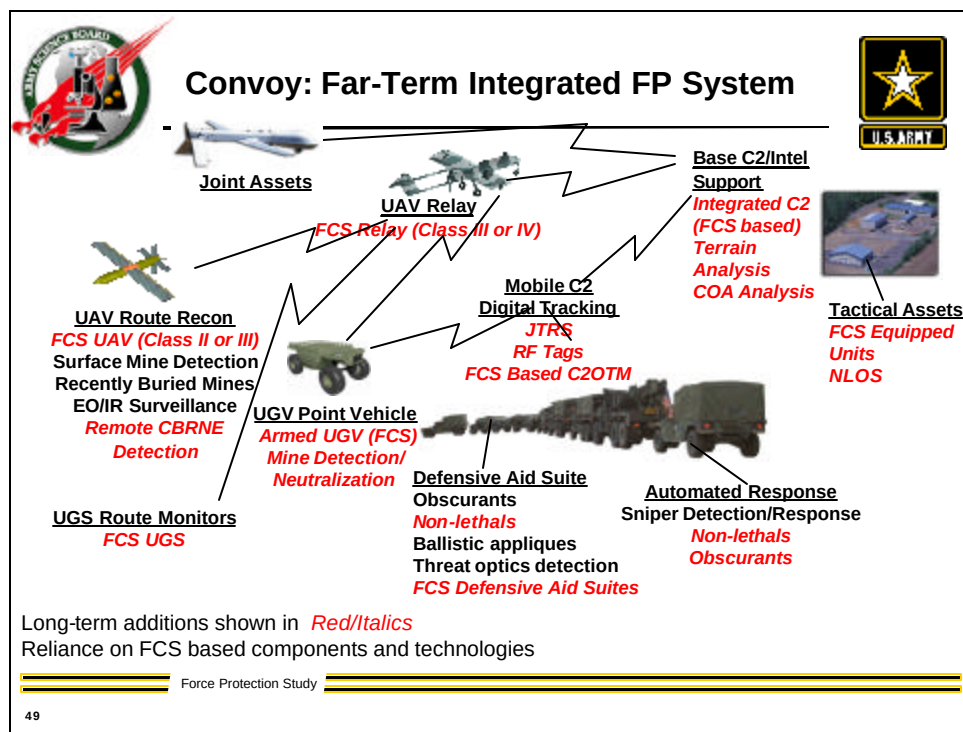


Using the Mana Distillation for the base scenario described in an earlier slide, several technologies were modeled to determine if any, or a combination of all of the technologies (representative of an integrated FP system), would affect the outcome to the convoy ambush. The base scenario models

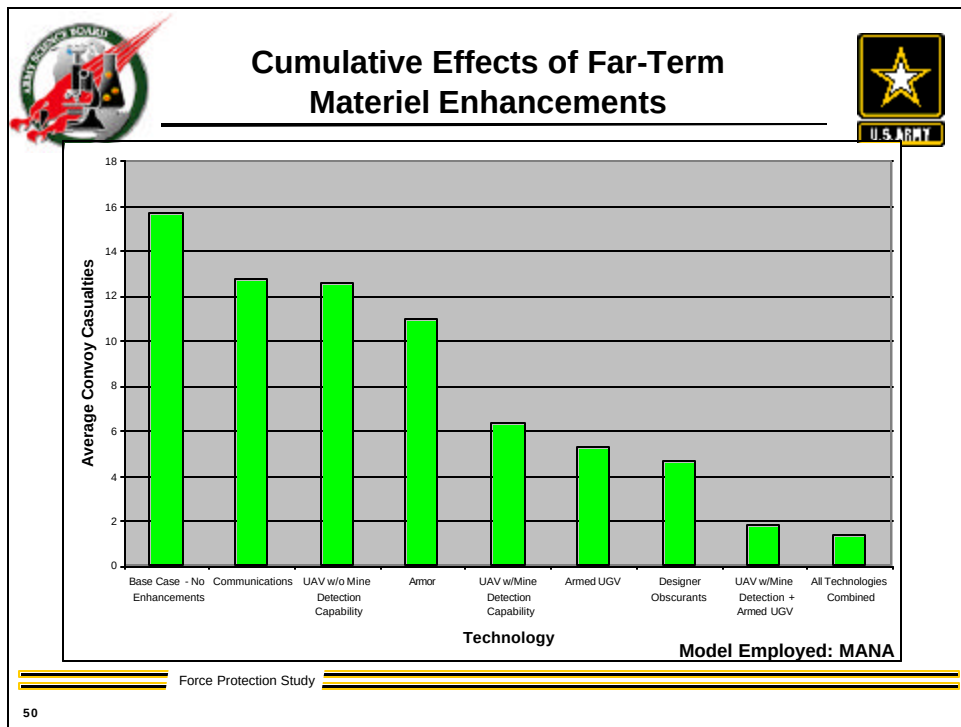
limited, less coordinated communications between members of the convoy, indicative of the fact that not all trucks have radios. Ballistic appliques and obscurants are not enhanced, but are representative of what would normally be organic to the convoy. No UAV capability is assumed.

In general, the convoy analyses focused on variations from this base case to include: better, more coordinated communication between convoy members; the addition of a UAV *without* mine detection capability to enhance situation awareness; the addition of a UAV *with* mine detection capability to improve survivability of the convoy; use of obscurants; armored appliques; addition of an armed UGV for mine detection and neutralization; and the combination of all of the technologies, consistent with the appropriate timeframe.

In the near-term, several technologies were identified that could be implemented quickly and could improve force protection for a convoy. Each was explored independently of the others to determine what improvements could be recognized by implementing individual technologies. As can be seen in the slide, modest improvements (i.e., 15% to 25% reduction in Blue casualties with respect to the base case) were realized for all of the individual technologies, *except* for the addition of a UAV with mine detection capability, which provides approximately a 55% reduction in Blue casualties with respect to the base case. When all technologies are combined to represent an integrated near-term FP system, the greatest decreases in convoy losses were observed. However, in this latter case, the reductions in convoy losses were only modestly better than those achieved by adding a UAV equipped with mine detection capability.



The items in red/italics on the slide indicate far-term technologies identified by the S&T Panel to mitigate risk to convoy operations. For further details on recommended far-term technological solutions to FP, refer to the S&T Panel report.



For the far-term, similar analyses were performed using the Mana Distillation. Technologies were analyzed individually and then in aggregate. The individual technologies include the list on the slide. For the far-term, the performance of each of the technologies was modeled as a substantial enhancement beyond the near-term. Other technologies are included in the far-term that were deemed infeasible to field in the near term (e.g., armed UGV).

The effectiveness of the candidate technologies can be aggregated into three broad categories. In the first category, the technologies provide limited enhancements to convoy survivability beyond the base case (i.e., approximately 20% to 30% reduction in Blue casualties). These technologies include enhanced communications, a UAV without mine detecting capabilities, and improved armor. In the second category, appreciable enhancements to convoy survivability are realized (e.g., approximately 60% to 70% better than the base case). These technologies include a UAV with mine detecting capabilities, an armed UGV, and designer obscurants. Finally, the third category provides very substantial enhancements to convoy survivability (e.g., approximately an 85% to 90% improvement beyond the base case). It consists of combinations of technologies: a UAV enhanced with mine detection capabilities plus an armed UGV in the lead to neutralize mines; and a combination of all of the technologies for the far-term. Note that the combination of all technologies for the far-term provides relatively modest improvement over the UAV/UGV addition.



Case V: Preliminary Observations (1 of 2)



- Lessons Recorded
 - Convoys are highly vulnerable to ambushes, mines
 - There exist a relatively extensive set of mitigating options; hence, a portfolio approach may be needed to identify an affordable, effective mix
 - Enhanced Blue situation awareness appears to have a significant impact on convoy survivability (e.g., a UAV with mine detection capabilities)
- Mitigating Options
 - Family of decision aids to support planning; e.g.,
 - Prediction of likely ambush locations
 - Route planning tools (with alternative routing to avoid ambushes)
 - DOTMLPF variants (note: there is “no silver bullet”; a *mix* of options is needed);
 - Modified TTPs (e.g., use precursor force to sanitize area)
 - Materiel (e.g., robots, with and without weapons; hardening; obscurants)
 - C2 enhancements (e.g., improved Blue force tracking)

Force Protection Study

51

Convoys are very lucrative targets for deadly ambushes and attacks by a variety of mines (e.g., pressure sensitive, command detonated). This observation reflects the results of the analyses performed as well as the day-to-day reality of operations in Iraq. The S&T Panel identified a relatively extensive set of options to mitigate the effects of those attacks. Consequently, a portfolio approach may be needed to identify a mix of those options that is effective and affordable. One key component of that portfolio should be options to enhance Blue situation awareness. Preliminary analyses of those options (e.g., addition of UAVs with mine detection capabilities) reveals that their addition to the mix appears to have a significant impact on convoy survivability.

There are a variety of mitigating options that should be pursued to deal with this high probability threat. First, a family of decision aids should be developed to support the early steps associated with the pre-attack phase. This would include predictive tools to identify likely locations of ambush sites and route planning tools to identify lower risk routing to avoid ambushes. Second, a mix of DOTMLPF options is needed. It is clear from the preliminary assessments that there is “no silver bullet”. Among the options to consider are modified TTPs (e.g., use a precursor force to sanitize likely ambush spots prior to the arrival of the convoy), materiel solutions (e.g., add robotic vehicles to the convoy, with and without weapons; harden the elements of the convoy against ballistic projectiles or fragments; outfit the convoy with obscurants, preferably “designer” obscurants that are relatively transparent to Blue with its aided vision devices and opaque to Red forces); and C2 enhancements (e.g., improve Blue force tracking so that the Commander is constantly aware of the location and status of his logistical convoys).



Case V: Preliminary Observations (2 of 2)



- Analysis Actions
 - Support to operations: logistics commanders need a family of enhanced decision aids; e.g.,
 - Improved route planning tools
 - Course of Action analysis tools to defeat adversary counter-mobility actions
 - Support to assessments
 - Analysts need a suite of tools to support portfolio analyses of mitigating options (e.g., a derivative of MITRE's PALM)

Analytically, there are a number of actions that should be taken to enhance our ability to cope with such an attack. First, steps should be taken to provide logistics commanders with a family of enhanced decision aids. These would include improved route planning tools and COA analysis tools to help defeat adversary counter-mobility actions. Second, to support the assessment community, analysts need a suite of tools to support portfolio analyses of mitigating options. As an example, MITRE has developed and employed the Portfolio Analysis Machine (PALM) (Reference 26) to address a variety of similar portfolio analyses. PALM develops the “efficient” frontier, identifying portfolios (and the elements in each) that provide the most benefit at a specific budget or funding level. It could readily be adapted to identify an efficient mix of investments to enhance convoy survivability.



Case VI: Small Unit Operations (SUO)



- Attack
 - Small Blue force patrolling a market place
 - Selected elements in market place engage Blue with small arms
- Key issues
 - Selection of S&T options to mitigate casualties to Blue forces
 - Value of materiel options (e.g., use of non-lethal weapons, enhanced situation awareness) to minimize collateral losses of neutrals
- Measures of Merit
 - Losses sustained by Blue forces
 - Red killed, injured
 - Neutrals killed, injured
 - Time to traverse market place
- Assessment
 - Performed by MITRE, AMSO
 - Tool: Mana

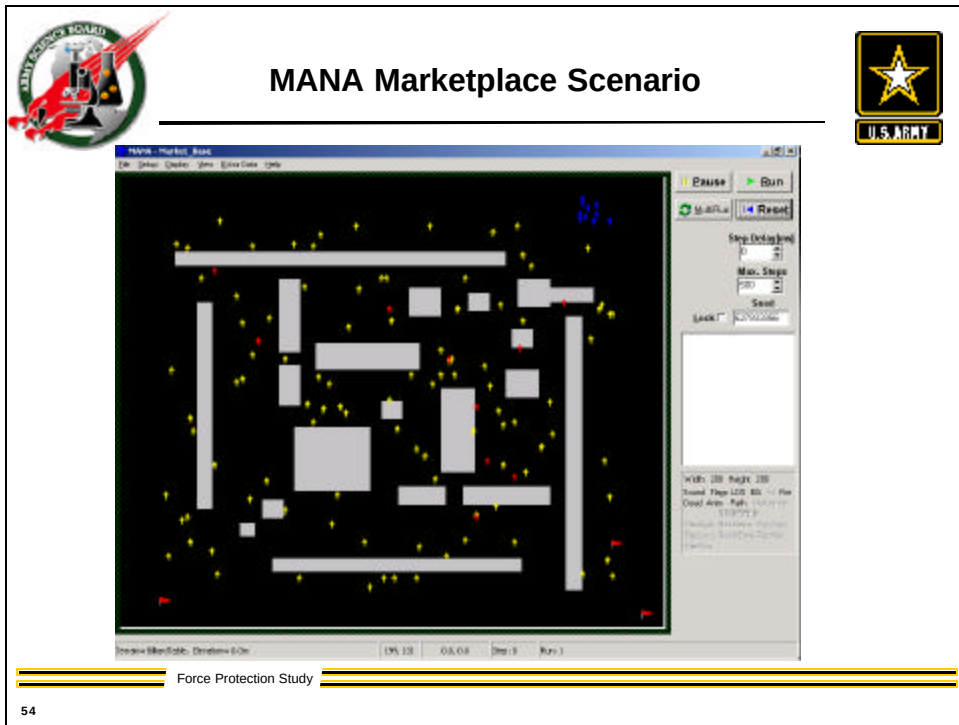
Force Protection Study

53

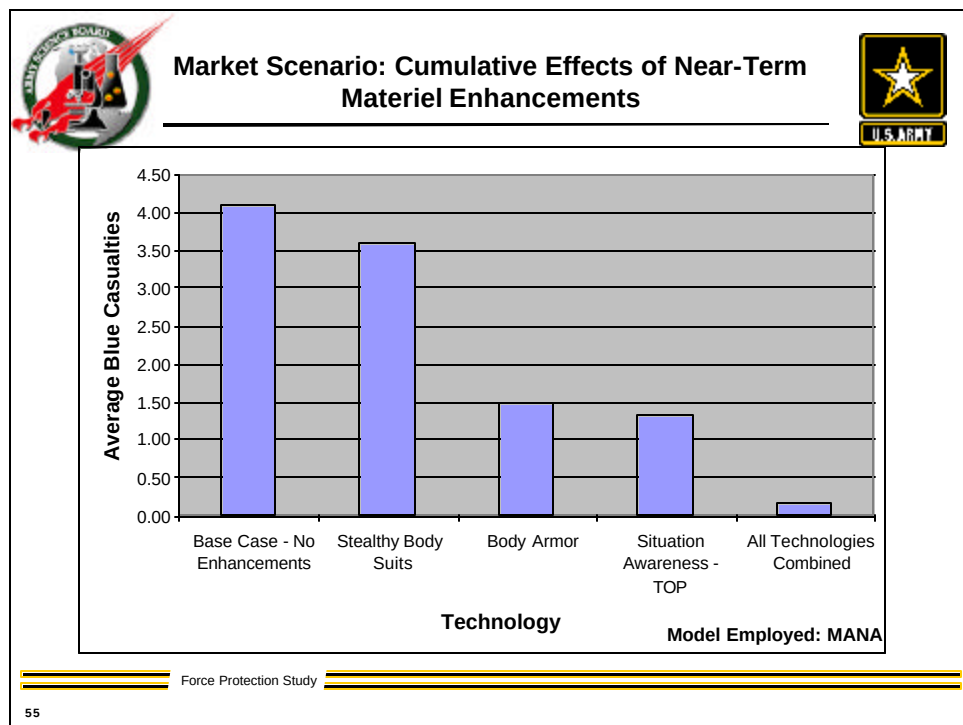
Case VI envisions a small Blue force patrolling a market place containing a large mix of non-combatants. However, a few members of the crowd are hostile and they will opportunistically engage Blue forces with small arms.

A variety of issues were addressed during the course of this analysis. These included the selection of S&T options to mitigate casualties to Blue forces. In addition, there was interest in assessing the value of materiel options (e.g., use of non-lethal weapons, enhanced situation awareness) to minimize potential collateral losses of neutrals. To illuminate those issues, the analyses employed the following measures of merit: losses (kills, injuries) sustained by Blue forces, Red forces, and neutrals. In addition, as a measure of functional performance, estimates were made of the time that Blue required to traverse the market place.

The assessment was performed by a team of MITRE and AMSO analysts using the Mana Distillation.



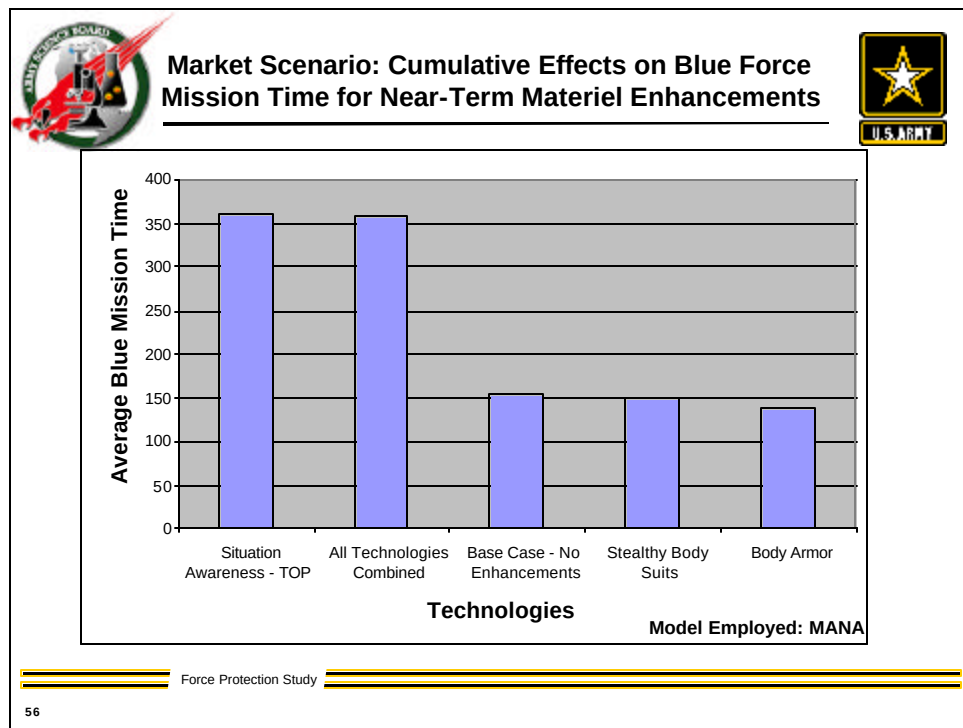
As noted above, small unit operations (SUO) were modeled using the Mana Distillation. In this scenario, a small Blue force of 10 soldiers is patrolling a market place. The patrol route takes them through the heart of the market to an objective point at the other end of the market. The market is crowded with a hundred non-combatants; however 10 Red forces are spread throughout the market place and will engage the Blue force if encountered.



The S&T Panel identified several near- and far-term technologies to enhance FP for individuals and small units.

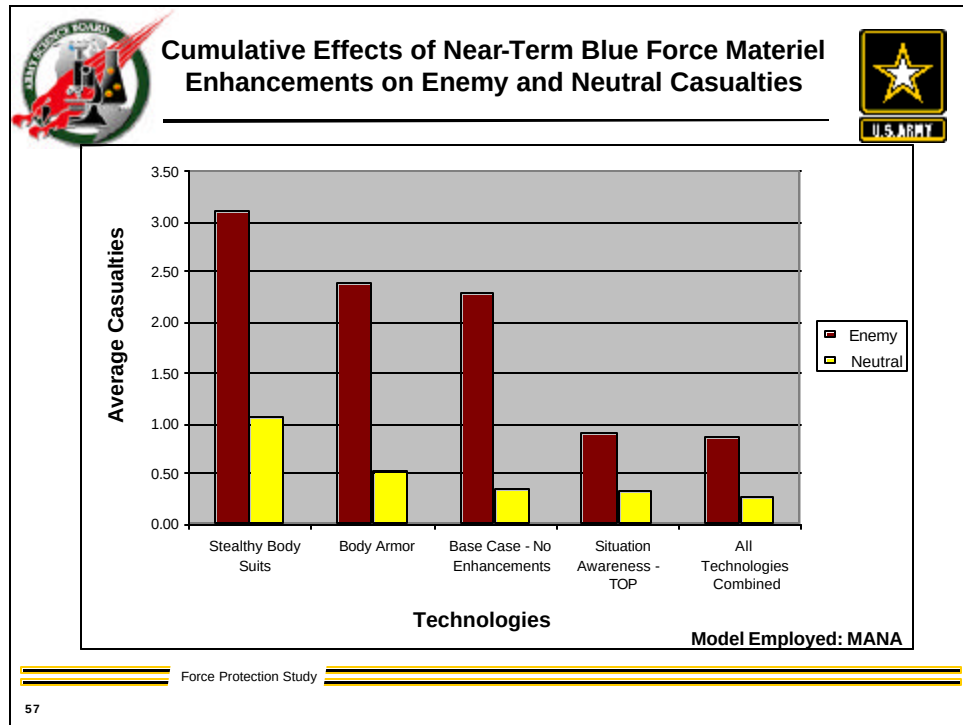
For the near-term timeframe, assessments were conducted for stealthy body suits, body armor, and enhanced situation awareness (via an enhanced Tactical Operational Picture (TOP)). The stealthy body suit provides enhanced concealment for the Blue forces allowing them to blend into the ambient environment (i.e., for the near-term, 25% concealment was assumed). Body armor is modeled through the surrogate of increasing the number of Blue Hits to Kill (from 1 to 2). Situational awareness, representing an increase in the quality, quantity, and timeliness of information passed to the tactical level (through improved sensors and C2), is modeled by increasing the sensor range of the soldiers (from 15 to 30 range boxes in a 200 by 200 grid).

The base case corresponds to an existing small unit without any FP enhancements. The slide depicts the effect of proposed FP technologies on average Blue casualties. It can be seen that adding stealthy body suits provides only marginal enhancements to Blue force survivability (i.e., approximately a 15% improvement). Conversely, adding either body armor or enhanced situation awareness provides substantial improvement (i.e., approximately 65% and 70% improvements, respectively). It is notable that these preliminary assessments suggest that implementing all three of the candidate technologies could reduce Blue casualties dramatically (i.e., on the order of 95% improvement). It must be cautioned, however, that these assessments are very preliminary and are merely suggestive of the benefits that could accrue from these enhancements. Rigorous experiments and analyses are required to develop more credible estimates of effectiveness.



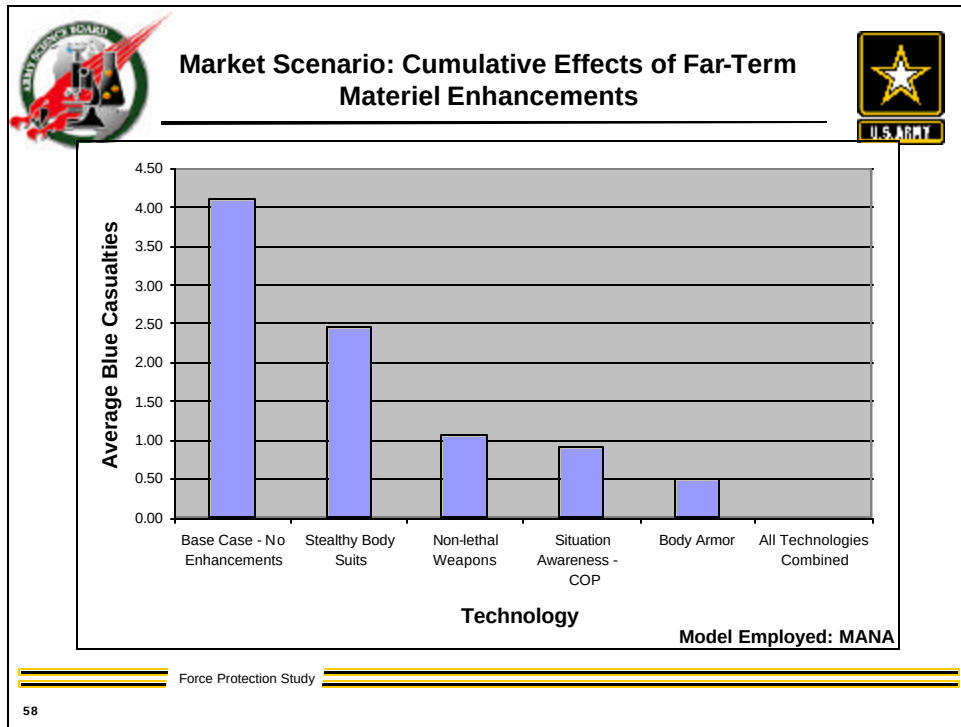
This slide depicts the average time steps for Blue to complete its mission as a function of augmenting the Blue unit with additional FP technologies. It is interesting to observe that when situation awareness was enhanced (either singly or in concert with other technologies), the average time for mission completion was *increased* substantially beyond the comparable average time for the base case (i.e., approximately a 130% increase). The reason for this increase in mission time is that Blue forces use this enhanced situation awareness to select paths through the market place which enable them to minimize their exposure to hostile members of the population and to minimize the exposure of neutrals

to potential violence. This behavior is clearly observable in watching playback runs of the simulation. Conversely, if the Blue unit is equipped with either stealthy body suits or body armor, the average time to complete the mission is comparable to the base case.



This slide depicts enemy and neutral losses as a result of Blue's use of near-term technologies. Two broad trends are in evidence. First, with the addition of stealth body suits and (to a lesser extent) body armor, Red and neutral losses *increase* (i.e., for stealthy body suits, Red and neutral losses beyond the base case are approximately 30% and 250%, respectively; for body armor, the corresponding increases are approximately 5% and 80%). The reason is that either of these technologies make Blue forces less vulnerable to enemy fire but do not enhance Blue's ability to distinguish foe from neutral. Blue is therefore able to increase its engagement of other forces in the market place, leading to increased kills of Red as well as of neutrals.

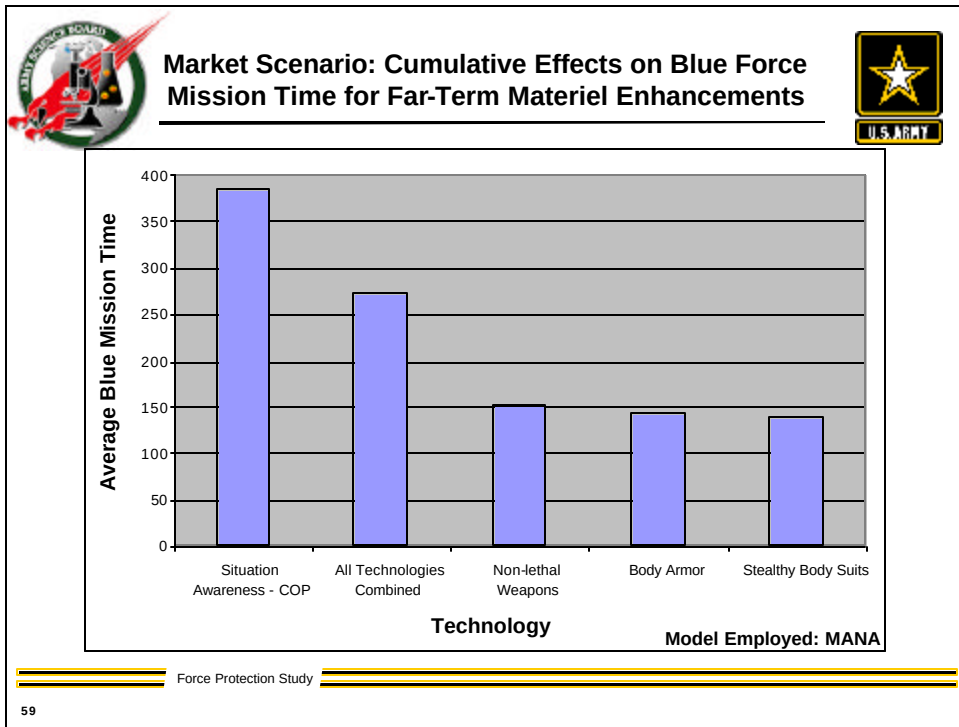
Second, with the addition of enhanced situation awareness (and any mix of technologies including situation awareness), Red and neutral losses *decrease* (e.g., for enhanced situation awareness, Red and neutral losses are approximately 60% and 25% less, respectively, than the comparable base case values). The reason for these decreases is that with enhanced situation awareness, Blue forces are able to select paths that minimize their exposure to Red forces and are better able to distinguish foe from neutral. The cumulative effect is to decrease both the number of Red and neutral forces killed.



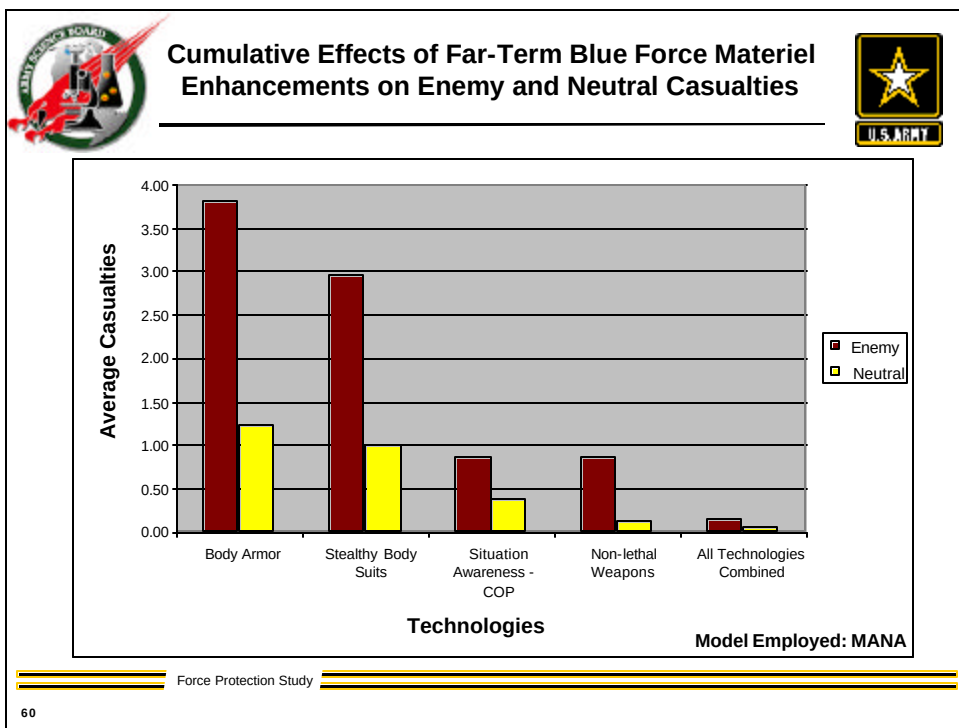
This slide depicts the effect of far-term technology options on Blue force casualties. In this case, stealthy body suits represent uniforms that have an increased capability to blend into the landscape (i.e., 75% concealment was assumed). Situation awareness is enhanced beyond the near-term to represent a more global view of the situation (i.e., a common vice a tactical operational picture, extending to 60 range boxes). Additional technology options include non-lethal weapons as well as enhanced body armor that provides enhanced protection and reduced weight through the use of new materials (e.g., 4 Blue Hits to Kill, representing nanotechnology fibers).

As depicted in the slide, Blue survivability is progressively enhanced by the addition of stealthy body suits, non-lethal weapons, situation awareness, and body armor. This constitutes a slight departure from the near-term assessment where situation awareness provided a slight improvement in average Blue casualties over the addition of body armor. However, given the preliminary nature of these calculations, these differences are not statistically significant.

In addition, when all of the technologies were implemented, simultaneously, for the market place scenario, the simulation revealed that Blue suffered nearly no losses, on average. Clearly, that result must be reassessed using a broader array of credible tools.



The trend depicted on this slide is comparable to the trend seen in the slide assessing the impact of near-term options on average time of Blue to conduct its mission. Again, the addition of enhanced situation awareness makes extended paths visible through the market which enable Blue forces to minimize simultaneously their exposure to hostile members of the population and the exposure of neutrals to potential violence.



The trend in average casualties for Red and neutrals depicted on this slide for far-term options is broadly comparable to the near-term case with a few notable differences. For advanced stealth and body armor, the relative magnitude of Red and neutral casualties are reversed, in comparison to near-term stealth and body armor enhancements. Furthermore, the use of non-lethal weapons gives rise to Red losses that are roughly comparable to those for enhanced situation awareness. Note that non-lethal weapons and enhanced situation awareness result in substantial reductions in collateral damage (e.g., in comparison to stealthy body suits, enhanced situation awareness reduces the average neutral casualties by approximately 60% while non-lethal weapons reduce the average neutral casualties by approximately 90%). Finally, for all technologies combined, both Red and neutral losses are reduced appreciably below corresponding near-term values.



Case VI: Preliminary Observations (1 of 2)



Lessons Recorded

- No single materiel enhancement is preferred for all of the measures of merit (i.e., minimize Blue, neutral casualties; maximize Red casualties)
- For the options that minimize Blue casualties, the more attractive options include
 - Near-term: enhanced Situation Awareness, body armor
 - Far-term: enhanced body armor, improved Situation Awareness, non-lethal weapons
- Options subsuming *all* of the technology options manifest low numbers of casualties for Blue, Red, neutral
- **Mitigating Options**
 - Explore options to enhance the quality of HUMINT to support the identification of friends, foes, and neutrals
 - If confirmed by further study, consider implementing the most cost-effective mix of DOTMLPF options, cited above
 - Pursue options to enhance the training of small Blue units
 - Near term: Enhance training in local culture, history, language; Use USMC CDR to enhance squad proficiency in FP
 - Longer term: Enhance training through the use of emerging ICT products (e.g., Full Spectrum Warrior, Command)

Force Protection Study

61

In these preliminary assessments, measures of merit were considered that subsumed Blue, Red, and neutral losses. For the two timeframes of interest, no single materiel option dominated the others with respect to all of these measures (e.g., in the near-term, options such as enhanced situation awareness led to reduced Blue and neutral casualties, but they also gave rise to reduced Red casualties). If it is assumed that the primary objective is to reduce Blue casualties, then several of the individual options are particularly attractive. These include (in descending order of effectiveness) enhanced situation awareness and body armor, in the near-term, and enhanced body armor, improved situation awareness, and non-lethal weapons, in the far-term. Finally, in both timeframes, combined options subsuming *all* of the technology options identified by the S&T Panel manifest low levels of casualties for Blue, Red, and neutral.

There are a variety of mitigating options that should be pursued to deal with this high probability threat to small Blue forces. First, options should be explored to enhance the quality of HUMINT to support the IFFN process. Second, if the results of these preliminary analyses are confirmed by further study and experimentation, consideration should be given to implementing the most cost-effective mix of DOTMLPF options, cited above. Finally, it is urged that options to enhance the training of small Blue units be pursued. In the near term, this would include enhancements to training in the areas of local culture, history, and language. With respect to the latter, there are cases where locals have tried to warn

small units about impending ambushes, but the Blue forces have failed to understand them. In addition, the USMC has used the CDR to enhance squad proficiency in FP. Since the tool is portable and low cost, consideration should be given to employing it to train small units of the Army. In the longer term, training should be enhanced through the application of several emerging ICT products. These include suitable adaptations of Full Spectrum Warrior and Full Spectrum Command, at the squad and company levels, respectively.



Case VI: Preliminary Observations (2 of 2)

- Analysis Actions
 - Pursue an aggressive research program to improve our understanding of the behavior of people (e.g., individuals, crowds) from different cultures when subjected to differing levels of fear, anger, need (e.g., hunger, sleep deprivation)
 - In conjunction with our allies, inject the results of human behavior research into evolving models
 - Subsequently, refine these models through the disciplined application of the Model-Experiment-Model paradigm

Force Protection Study

62

Analytically, there are a several actions that should be taken to enhance our ability to cope with such situations. First, it is essential that we pursue an aggressive research program to improve our understanding of the behavior of people from different cultures. This entails exploring the behaviors that are manifested in the context of a crowd as well as for individual actions. In addition, these behaviors need to be understood over a broad set of conditions. These include varying levels of fear, anger, and need (e.g., need for food, water, or sleep). Working with our allies, we should inject the results of this human behavior research into our evolving suite of FP models. Subsequently, efforts should be undertaken to refine these models through the disciplined application of the model-experimentation-model paradigm.



Outline of Report



- Introduction
- Assessment of M&S Capabilities for Force Protection
- Analyses to Support the Study
- Summary

Force Protection Study

63

This section summarizes the Panel's observations on M&S for FP and the assessments of the selected cases. In the former area, we identify the major FP M&S needs for the Army's major M&S domains (i.e., ACR, TEMO, and RDA) and the Panel's findings and recommendations. In the latter area, we summarize the preliminary recommendations that emerged from the assessments of the six FP cases. We conclude the report with some final observations on what was accomplished and proposed follow on steps.



Context: M&S Needs



- M&S must play a major FP role in three domains
 - Advanced Concepts & Requirements (ACR)
 - Enhance the ability to evaluate the impact of proposed changes in DOTMLPF on FP effectiveness, efficiency
 - Support the optimization of FP investments (e.g., portfolio analysis)
 - Training, Exercises & Military Operations (TEMO)
 - Support just-in-time training tools for FP participants at all echelons
 - Provide efficient support to FP exercises (e.g., faster, better, cheaper)
 - Provide operational decision aids that are credible, easy to use
 - Research, Development & Acquisition (RDA)
 - Represent human behavior credibly (a research need)
 - Provide infrastructure to support the SMART acquisition of future FP systems-of-systems

Force Protection Study

64

Organizationally, the Army has established three domains for M&S: Advanced Concepts & Requirements (ACR), Training, Exercises & Military Operations (TEMO), and Research, Development & Acquisition (RDA).

In the ACR domain, the panel has concluded that two major FP M&S needs must be satisfied. First, steps must be taken to enhance the ability to evaluate the impact of proposed changes in DOTMLPF on FP effectiveness and efficiency. Second, to support the allocation of resources among candidate FP options, tools must be developed to support the optimization of FP investments (e.g., portfolio analysis tools).

In the TEMO domain, the panel has concluded that three major FP M&S needs must be satisfied. First, tools to support just-in-time training for FP participants are required at all echelons (e.g., from the Commander to the “strategic private”). Second, tools are needed to provide efficient and effective support to FP exercises. These tools should ensure that the preparation, execution, and after action reporting of exercises are performed faster, better, and cheaper. Finally, enhanced FP operational decision aids are needed that are credible and easy to use.

In the RDA domain, the panel has concluded that two major FP M&S needs must be satisfied. First, in the area of research, it is essential that we strengthen our understanding of how to represent human behavior credibly in M&S. This is a vital need if we are to be able to credibly model the FP problems associated with mobile Blue forces. Second, if future FP systems are to be acquired using the SMART paradigm, key infrastructure, M&S, and data bases must be assembled and kept current.



Key M&S Findings



- Overall -- M&S has very wide applicability and utility to FP, but:
 - The FP M&S community is very heterogeneous and fragmented
- ACR -- Selected FP assessment tools exist, but:
 - Are generally difficult to set up and employ (particularly if non-materiel options are to be assessed)
 - Need refinement to represent human behavior more credibly
- TEMO -- Other Services, Agencies have some useful capability, but key voids include:
 - Inadequate support to FP training, particularly for senior echelons
 - Limited support for FP exercise planning, execution, assessment
 - Shortfalls in existing FP decision aids (e.g., plume prediction)
- RDA -- The USAF has a FP Battlelab, but:
 - The USA does not participate directly in the USAF lab
 - Existing USA tools are inadequate to support a SMART acquisition of a joint integrated Force Protection system

Force Protection Study

65

Overall, the Panel concluded that M&S has very wide applicability and utility to FP. However, the FP M&S community is currently very heterogeneous and fragmented. The following findings are M&S domain specific.

In the ACR domain, selected FP assessment tools exist (e.g., JCATS, JANUS) but they are generally difficult to set up and employ, particularly if non-materiel options are to be assessed. In addition, these tools need refinement to represent human behavior more credibly.

In the TEMO domain, other Services and Agencies have some useful capability that the Army could exploit. For example, in FP training, the USMC has a useful tool, the Combat Decision Range, for

training squads in FP. However, there are key training needs, particularly at senior echelons, for which no adequate training tools are available. In the area of exercise planning, execution, and assessment, the US Army Pacific has developed a useful, web-based tool, CHESSS, to support selected needs of the intelligence community. However, there is no comparable capability to satisfy the full range of exercise needs. Finally, there are many examples of useful FP decision aids to support the operational user. However, it is widely recognized that many of these tools are limited (e.g., the quality of plume prediction in HPAC for turbulent atmospheric conditions) and there is concern that these decision aids are not being synthesized into an integrated decision support system.

In the RDA domain, the USAF has established a FP Battlelab. However, the Army does not participate directly in the USAF Battlelab. Finally, existing Army tools are inadequate to support a SMART acquisition of a joint integrated FP system.



Recommended M&S Investments



- Overall:
 - Develop a POAM for FP M&S (Action - DUSAOR)
 - Create a Army-led joint FP FACT (Action – DAMO-ZS)
- ACR: Action – DAMO-AC
 - Develop a flexible tool kit of models and associated data bases for the FP analyst/experimenter
- TEMO: Action - DAMO-TR
 - Develop a family of E&T tools to support the just-in-time FP needs of all echelons
 - Develop automated tools to enhance the efficiency, effectiveness of planning, executing, and evaluating FP exercises
 - Develop an integrated family of decision aids to help the theater commander and his staff conceptualize and formulate FP strategies
- RDA: Action - ASA(ALT)
 - Conduct an aggressive research program on human behavior in partnership with other DoD organizations and inject results into on-going M&S activities (e.g., agent based models, OneSAF)
 - Improve the performance of key FP decision support applications (e.g., plume prediction and course of action formulation for an urban environment)
 - Develop a joint FP M&S testbed to support the SMART, evolutionary acquisition of systems-of-systems that lead to a balanced, defense-in-depth capability

Force Protection Study

66

Overall, a Plan of Action and Milestones (POAM) is needed to identify and prioritize the most critical M&S investments needed to enhance FP and promote cross-community dialogue. DUSAOR should generate this product. Furthermore, an Army-led FP FACT should be established to create a recognized FP M&S Community of Interest. DAMO-ZS should take the lead in creating this FACT. In the ACR domain, steps should be taken to develop a flexible tool kit of models and associated data bases for the FP analyst/experimenter. DAMO-AC should take the lead in planning for and implementing this capability.

In the TEMO domain, three major initiatives are recommended. First, a family of E&T tools should be developed to support the just-in-time FP needs of all echelons. Particular emphasis should be placed on the needs of higher echelons. Second, automated tools should be developed to enhance the efficiency, effectiveness of planning, executing, and evaluating force protection exercises. This initiative should build upon the base established by the US Army Pacific in the CHESSS program. Finally, an integrated family of decision aids should be developed to help the theater commander and his staff conceptualize and formulate force protection strategies. DAMO(TR) should take the lead for each of these initiatives.

In the RDA domain, there is need for an aggressive research program on human behavior. This research should be performed in partnership with other DoD organizations (e.g., DARPA, DMSO, ONR). The results of this research should be injected into key on-going M&S activities (e.g., agent based models, such as MANA, and OneSAF). Second, steps should be taken to improve the performance of key force protection decision support applications. A notable area for improvement is the prediction of plume propagation, particularly in the micro-climate over urban canyons. Finally, a joint force protection M&S testbed should be developed to support the SMART, evolutionary acquisition of systems-of-systems that lead to a balanced, defense-in-depth capability. ASA(ALT) should take the lead for each of these initiatives.



Selected Recommendations: Force Protection Functions



- In order to develop an efficient, effective force protection capability, efforts should be pursued to develop a balanced Defense-in-Depth capability, subsuming
 - Pre-attack options, that
 - Improve current attack prediction capabilities
 - Extend and enhance battlespace monitoring
 - Strengthen efforts to deter, deny an attack (e.g., keep threats at or beyond effective ranges; enhance perimeter and portal defenses; randomize actions)
 - Enhance protection (e.g., hardening)
 - Improve readiness (e.g., enhance training; set appropriate FPCONS; conduct regular, routine exercises)
 - Trans-attack options, that provide enhanced stand-off and early warning, particularly against a range of CBRNE threats
 - Post-attack options, that
 - Mitigate the effects of an attack (e.g., enhance responsiveness of emergency responders)
 - Facilitate the restoration of breached defenses
 - Provide the insight needed to enhance the protection of the force against future threats

Force Protection Study

67

In order to develop an efficient, effective force protection capability, the Panel's preliminary analyses suggest that efforts should be pursued to develop a balanced Defense-in-Depth, FP capability. In the pre-attack phase, this implies that a series of options be pursued that enhance a broad set of sub-functions. These include: improving current attack prediction capabilities; extending and enhancing battlespace monitoring; strengthening efforts to deter, deny an attack (e.g., keep threats at or beyond effective ranges; enhance perimeter and portal defenses; randomize actions); enhancing protection (e.g., selectively hardening key nodes); and improving readiness (e.g., enhance training; set appropriate FPCONS; conduct regular, routine exercises). In the trans-attack phase, options should be pursued that provide enhanced stand-off and early warning, particularly against a range of CBRNE threats. This includes improvements in sensing (e.g., long range detection, classification, and identification of adversary threats), communicating, hardening, and neutralization (lethal, non-lethal). In the post-attack phase, options should be pursued that mitigate the effects of an attack (e.g., enhance responsiveness of emergency responders), facilitate the restoration of breached defenses, and provide the insight needed to enhance the protection of the force against future threats.



Observations



- Opportunities have been identified to enhance the M&S needed to support all of the functions associated with force protection (e.g., ACR, TEMO, RDA)
- Preliminary assessments have been conducted, using a mix of tools, to identify DOTMLPF opportunities to enhance force protection effectiveness and efficiency; these results suggest:
 - The importance of achieving early warning and extended keep out range in defending a fixed installation
 - The potential utility of selected materiel and operational actions to enhance the protection of a convoy (e.g., employing armed UGVs and UAVs; developing and deploying “designer” obscurants)
 - The value of suitable levels of protection (e.g., enhanced body armor), enhanced situation awareness, and non-lethal weapons in reducing casualties while performing small unit operations
- Follow on, rigorous analyses should be performed to confirm and extend these preliminary findings

Force Protection Study

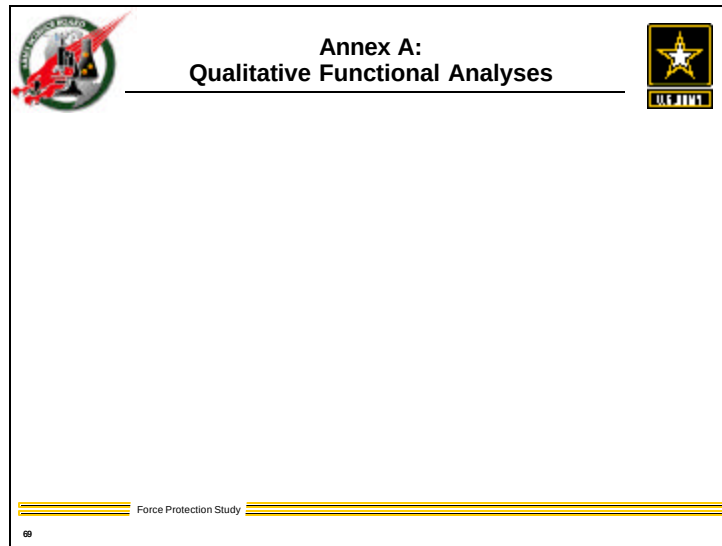
68

In conclusion, the panel has identified a variety of opportunities to enhance the M&S needed to support all of the domains associated with force protection (e.g., ACR, TEMO, RDA). It strongly recommends that the M&S managers of these three domains work in concert to assess and implement the actions proposed by the Panel. That is due to the fact that there are several key M&S needs that cut across those domains. The proposed FP FACT could play a significant role in facilitating the needed communications and coordination.

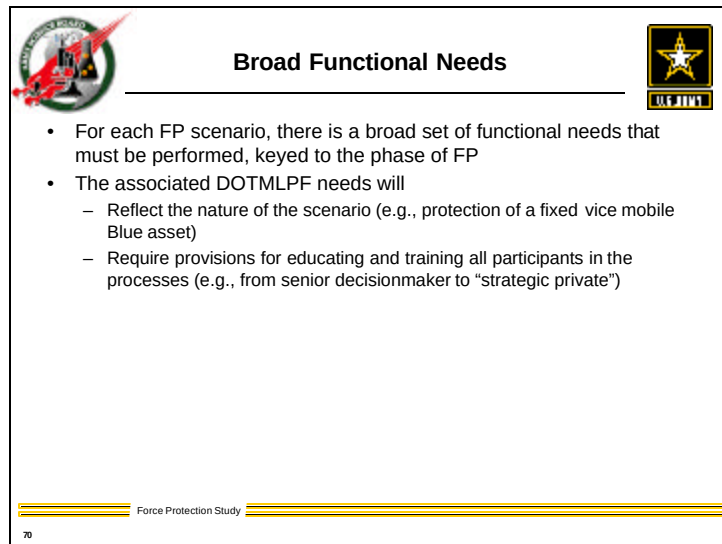
It must be emphasized that the substantive assessments that the panel performed are preliminary in nature. As such, they are suggestive of the DOTMLPF actions that should be taken to enhance FP effectiveness and efficiency. These preliminary results point to three major conclusions:

- The importance of achieving early warning and extended keep out range in defending a fixed installation;
- The potential utility of selected materiel and operational actions to enhance the protection of a convoy (e.g., employing armed UGVs and UAVs; developing and deploying “designer” obscurants)
- The value of suitable levels of protection (e.g., enhanced body armor), enhanced situation awareness, and non-lethal weapons in reducing casualties while performing small unit operations.

The panel recommends strongly that additional, rigorous analyses be performed to confirm and extend these preliminary conclusions.



This Annex identifies the broad functional needs associated with pre-, trans-, and post-attack activities. It characterizes these functional needs for the sub-functions of predict, monitor, deter, deny, prevent, defend, respond, restore, and retaliate. Additional functional requirements have been identified by the Operations Panel and are documented their report.





Functional Needs: Predict



- Establish a framework within which "sense" can be made of observations, inputs
- Predict the nature of potential future attacks (e.g., who, what, how, where, when, likelihood)
- Formulate alternative courses of action (COA), anticipating likely Red reactions, and estimate the risk associated with the alternatives
- Generate appropriate FP plans, consistent with preferred COA
- Identify observables that should be monitored, consistent with the above (e.g., Indications & Warning; precursors of an imminent attack)
- Identify threshold values of observables that merit reaction (e.g., consistent with acceptable PD-PFA tradeoffs)

Force Protection Study

71



Functional Needs: Monitor



- Generate baseline statistics to characterize "normal" behavior for observables such as, inter alia,
 - Traffic flow (as a function of time of day, day of week)
 - Contaminants (in air, water, food)
 - Communications (level of adversary "chatter")
- Generate and maintain a common relevant operational picture of each observable (characterized by "acceptable" levels of completeness, latency, accuracy, precision)
- Detect operationally significant deviations in baseline values, early enough to support effective reaction

Force Protection Study

72



Functional Needs: Deter



- Keep key FP parameters opaque (e.g., nature of security processes)
- Simultaneously, conduct highly visible (but randomized, as appropriate) deterrence actions; e.g.,
 - Frequent patrols, escorts
 - Show of force (e.g., heavily armed patrols)
 - Establishment of appropriate FPCONs
 - Randomized, in-depth searches
 - Exercises of FP plans (to signal high levels of readiness; note: some exercises should be "no-notice")
- Conduct Information Operations (e.g., transmit the message that "We are 10 feet tall!")

Force Protection Study

73



Functional Needs: Deny, Prevent



- Selectively harden potentially vulnerable areas
- Ensure there is no single point of failure (e.g., build in redundancy, robustness, adaptability, fault tolerance)
- Keep potential adversaries at ranges beyond their effectiveness, lethality
- For fixed installations
 - Secure, monitor perimeters
 - Limit access through portals (balancing ease of access for Blue vice detection and apprehension of Red)
- For mobile units, avoid areas that are likely candidates for ambush positions

Force Protection Study

74



Functional Needs: Defend



- Detect, neutralize threats (e.g., adversaries, contaminants) beyond appropriate "keep out" ranges, if feasible (e.g., bring counter-fire to bear on Red indirect fire weapons)
- Predict evolution of the attack (e.g., spread of a plume of contaminants) to help formulate COAs
- Take actions to protect people, materiel at risk; e.g.,
 - Ensure safety of high value targets
 - Evacuate people from regions of risk, if warning time is sufficient
 - Alert people to protect themselves (e.g., put on appropriate MOPP gear)
 - Take protective actions for materiel, if time allows (e.g., deploy protective foam on buildings)
- If feasible, confound the adversary through cover, concealment, and deception (CC&D) actions

Force Protection Study

75



Functional Needs: Respond, Restore



- Mobilize, coordinate, control resources to mitigate problems created by the attack; e.g.,
 - Contact, coordinate emergency responders to deal with the consequences of the attack (e.g., police, firemen, emergency medical responders, teams to locate and rescue personnel trapped in rubble)
 - Decontaminate (as needed)
- Reconfigure defenses (as needed)
- Identify lessons learned to guide restoration of defenses
- Revise plans, DOTMLPF to reflect lessons learned

Force Protection Study

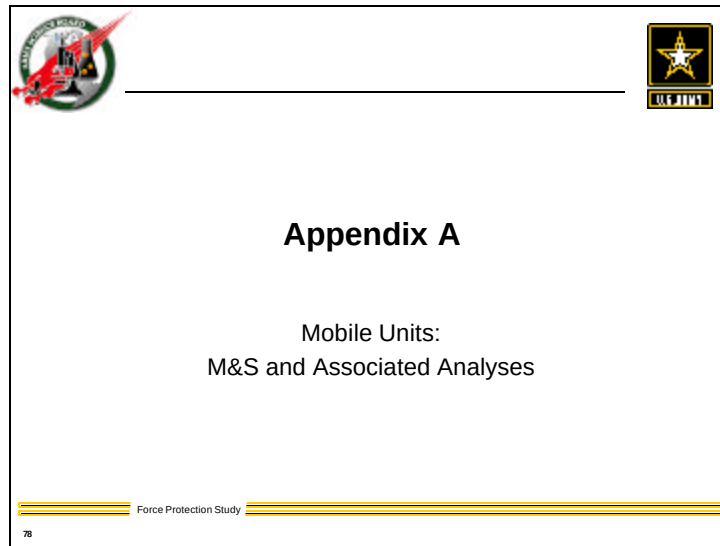
76



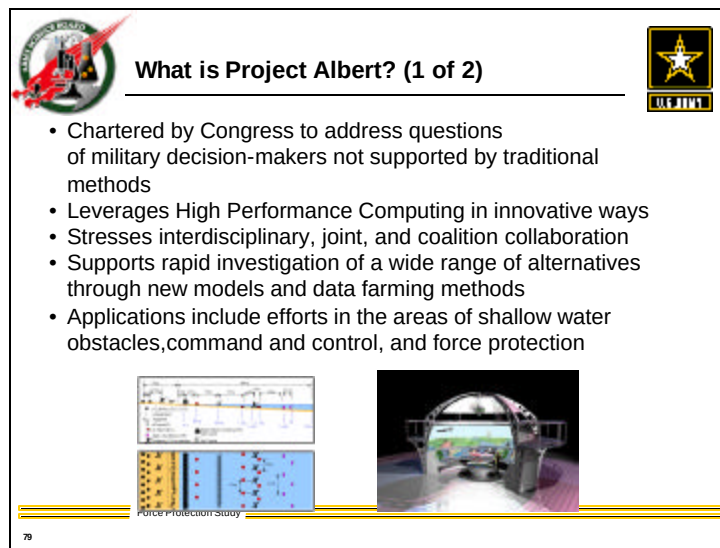
Functional Needs: Retaliate



- Short term
 - If feasible and desirable, plan and implement military actions to punish Red for the attack (note: the retaliatory team will generally involve different units than the target attacked; e.g., SOF)
- Longer term
 - Undertake punitive, effects-based operations focused on assets of value to the adversary (e.g., diplomatic, political, social, economic)



This appendix describes the tools that were employed in the analyses of FP for mobile units (e.g., convoys, small unit operations). It also provides preliminary analytic results that identify promising concepts of operations and technologies to enhance the protection of these mobile units.



Project Albert is a program sponsored by the Marine Corps Warfighting Lab, funded by special authorization from Congress. The charter from Congress is to address questions posed by military decision-makers that cannot be supported by traditional operations analysis methods. The ultimate goal of Project Albert is to introduce advanced operational analysis and research techniques to the study of military science and to apply these concepts in a modeling and simulation environment. The specific focus of Project Albert has been to explore important phenomena inadequately represented by current techniques. These phenomena include nonlinearities, intangibles, and adaptive decision-making. Project Albert uses new models, modeling techniques and tools, multidisciplinary teams, and the scientific method to explore questions. The approach utilizes the meta-technique *Data Farming* to look at 21st Century questions from the perspective of the whole—and lots of data points are needed to explore this “whole”. This meta-technique has been made possible by a convolution of advancements as the 21st Century begins. These include:

Advances in agent-based models, which have the promise of capturing some of the adaptability and other key factors inherent in conflict;

Advances in computing power that enable us to increase our volume of data;

Advances in our ability to organize, analyze, and visualize scientific data;

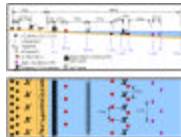
Advances in concepts on how to integrate across the spectrum of operations research techniques.



What is Project Albert? (2 of 2)



- Chartered by Congress to address questions of military decision-makers not supported by traditional methods
- Leverages High Performance Computing in innovative ways
- Stresses interdisciplinary, joint, and coalition collaboration
- Supports rapid investigation of a wide range of alternatives through new models and data farming methods
- Applications include efforts in the areas of shallow water obstacles, command and control, and force protection



Force Protection Study

80

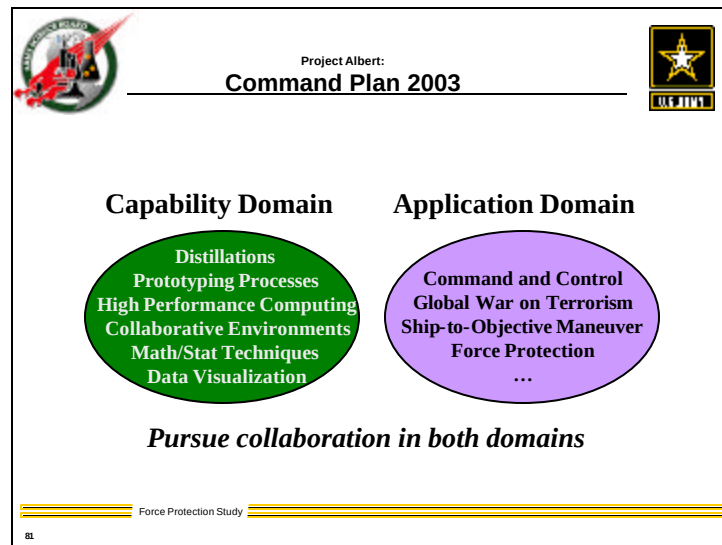
A *Distillation* is a simulation that abstracts a scenario to address directly the essence of a military decision-maker's questions. Distillations are intended to be intuitive, transparent, and transportable. Distillations should be agile: quickly developed, quickly understood, and quickly run.

Data Farming is the process of executing replicates and variations of distillations, examining the results using various analysis, visualization, and perceptualization techniques, and then iteratively adjusting the distillation and its variations.

Data Farming requires the use and development of *High Performance Computing* environments in order to execute the large number of distillations, process and manage the large volume of resultant data, and provide interfaces for users.

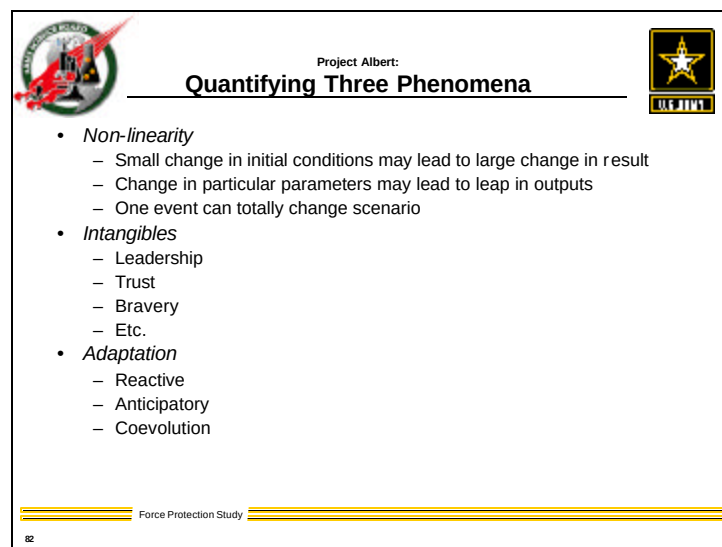
Data Farming also requires development of new methods of *Data Perceptualization*, analysis, and data mining in order to examine and understand the resultant volumes of data.

The long term objective is to support decision makers by combining insights into questions produced by distillation modeling and analysis techniques with current techniques of modeling and analysis to try and capture important phenomena not represented by current techniques and thus provide a more complete picture of the situation. The end goal is the integration of various methods of analysis including: wargames, deterministic models, simulations, and distillations into an iterative data farming process.



Project Albert is currently pursuing efforts in two domains: the capability domain and the application domain. The capability domain includes definition and development of the distillation models, a scenario library, the supercomputing environment, and statistical and visualization techniques to examine multi-dimensional data - designing and developing the infrastructure and all of its associated components to allow exploration of real world questions.

The Marine Corps Warfighting Lab has categorized four application areas to explore for the current year. The four areas encompass command and control, the global war on terrorism, ship-to-objective maneuver, and force protection. These four areas are broad in nature and cover a multitude of questions.



In order to present a richer picture of a situation for a decision-maker, a main thrust of the program is to attempt to quantify three phenomena not addressed by other techniques. These phenomena include nonlinearities, which are sensitivities to initial conditions that can drastically impact the outcome of a situation; intangibles, which are aspects such as morale, leadership, discipline, trust - attributes which can also play an important role in the outcome of conflict. The third phenomenon is adaptation. Adaptation to natural events can be reactive; adaptation can be anticipatory, and a more advanced form

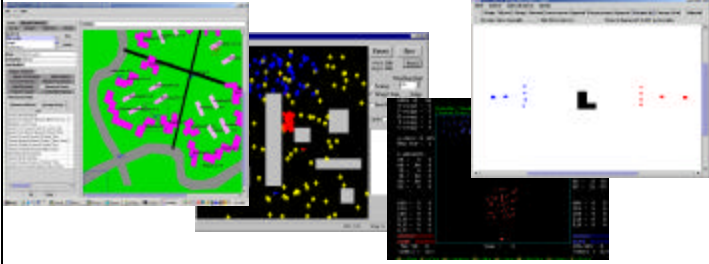
of anticipatory adaptation is through coevolutionary decision making processes ("I think, he thinks, I think he thinks, I think he thinks I think").



Project Albert: Distillations



- Distillation – Model/simulation that is intuitive, transparent, transportable, and farmable...
- A bottom up distillation of the essence of a question
- An experiment with controls and repeatability; A prototype of a situation
- Quick implementation - less than a few hours – eventually... minutes



Force Protection Study

83

Distillations have the potential to allow rapid exploration of appropriate questions. Distillations are simple models/simulations that are intuitive (behaviors make sense), transparent (behaviors are traceable to parameter settings), transportable (small/simple enough to implement across multiple platforms), and farmable (able to integrate into the high performance computing environment and run many times).

Distillations filter out enough detail or reduce a situation to its basic components in order to capture the essence of a problem. Distillations have the potential to provide an intuitive look at a situation. They do not necessarily provide concrete answers, but they can provide glimpses of whether or not what intuition suggests might happen, really can happen at all, thus providing a better discussion mechanism for decision-makers.



Distillations Are Abstractions



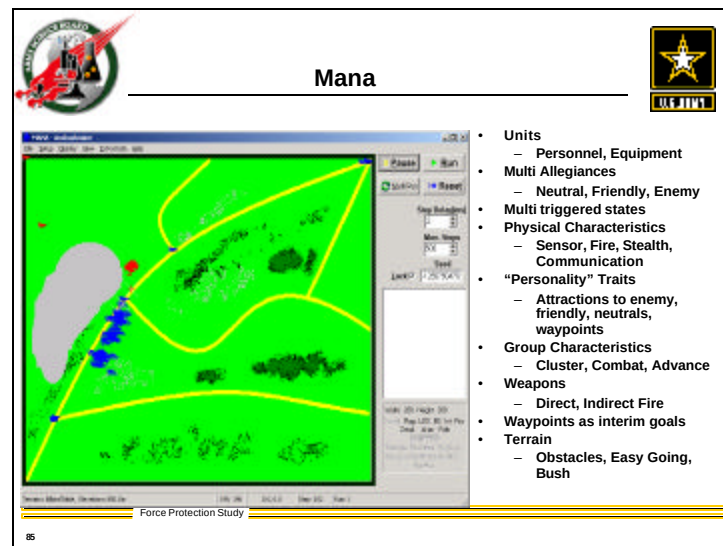
- “Bullets” can represent interchanges of various types
 - Food
 - Negative messages
- Location, proximity may represent relative aspects of other relational parameter
- Obstacles can represent walls, floors, borders, and other obstructions of non-geoterrain/combat interchanges
- Example: Communication level can act as “proxy” for trust (e.g., Do you use or ignore information provided?)

Force Protection Study

84

Distillations are abstractions of real world situations. Distillations reduce the detail associated with complex situations down to their basic components. For instance, within distillations, weapons can

represent other things, such as food, political broadcasts, etc., which influence behaviors, but in a different way than injuring or killing an agent. Obstacles can represent walls, floors, borders, features other than terrain impediments. Communication levels can act as a proxy for trust by the measure of whether or not an agent ignores or uses the information it is given.



The Mana model has been used to generate the initial scenarios and data for the convoy and small unit questions. Mana is a cellular automaton model developed by the New Zealand Defense Technology Agency used to explore military questions. The Mana Distillation is part of the Project Albert suite of tools. The basic, key features of the Mana model include the following: units can be defined in terms of either personnel or equipment characteristics. The model has multiple sides, based upon allegiance – friendly, neutral, or enemy. Basic physical characteristics can be defined for each unit – such as sensor range, firing range, stealth, and communication links, as well as weapons definition. Agent grouping characteristics can be defined, such as a cluster parameter, or “unit cohesion”, which is an attraction to friendly agents until a user-defined numerical threshold has been achieved before agents will move; an advance parameter which is another user-defined threshold that agents must meet before moving toward the goal; and a combat parameter, which is a user-defined numerical advantage for agents before they will move on the enemy. Agents’ movement propensities are determined by attractions toward or away from other agents, whether friendly, neutral, or enemy, and towards or away from waypoints and terrain types. A key feature of Mana is triggered events which can cause agent behavior changes. Every agent has a base state, or default behavior state with default ranges; however, users can define other behavioral characteristics based upon certain events, and these triggers can be individual or perpetuated for the whole squad. For instance, an agent or a squad can change from the default when shot at by other agents, upon reaching a waypoint, if injured, or when enemy contact is made. Terrain is represented very simply, and based upon color. Definable terrain features include obstacles (which can impede movement, sight, and firing) and easily traversed terrain (e.g., roads or paths, and dense and light brush).



Convoy Force Protection



- Project Albert invited to participate in the Army Science Board Summer study
- Focus on Convoy Operations
- Force Protection is a focal category in the Command Plan laid out for Project Albert by BGEN Panter of the Marine Corps Warfighting Lab

Force Protection Study

86

Late in the Spring, Project Albert was invited to participate in this FP study. The goal was to use any of the Project Albert models which may be able to provide some illustrative insights into the scenario areas covered by the study.

The main focus of Project Albert modeling is on convoy operations, although the small unit question has also been explored.

The command plan laid out for Project Albert by the Marine Corps Warfighting Lab includes a focus area on Force Protection. Thus participation in the summer study was viewed as being mutually beneficial for all parties.



Starting Point



- Previous study by RAND on convoy operations
- Study was reducible enough to "distill" essence of problem using MANA
- Basic terrain and force distributions from RAND study were used to create farmable distillations

Force Protection Study

87

To lend credibility to using distillations to examine these questions, initial analyses were conducted based upon a previous study by RAND (Reference 24). The basic terrain and force distributions from the RAND study were used to initiate this analysis. Consistent results were found between the RAND study and the Project Albert Distillation study.



Base Scenario



- Involves Blue convoy of 10 HMMWVs and 30 trucks on a Humanitarian Aid mission
- Red ambush party consists of 24 members
- Red hides behind a visual obstruction to ambush Blue
- Terrain contains rolling hills and a road system



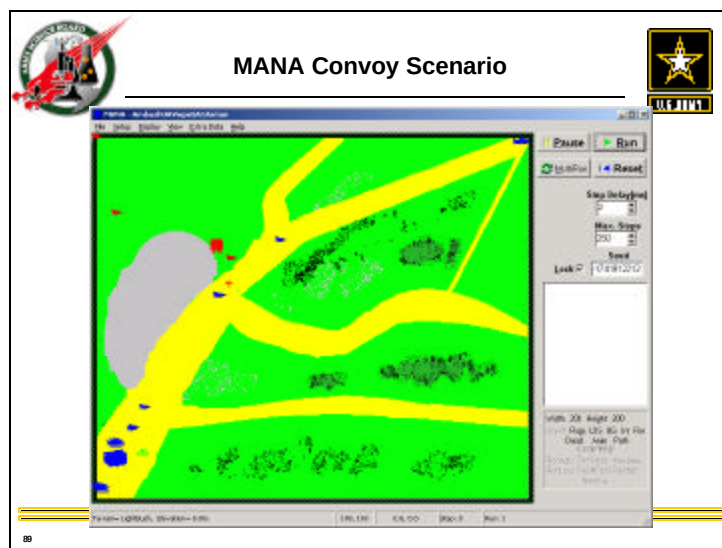
Force Protection Study



88

The base convoy scenario includes 10 HMMWV escort vehicles for 30 convoy trucks en route to a humanitarian aid site.

An ambush party of size 24 hides behind a visual obstruction to engage the convoy and has buried a land mine in the middle of the road to surprise, disrupt, and/or disable the convoy.



The slide depicts a Mana screen shot of the convoy scenario. The base scenario shown here and described in an earlier slide consists of a convoy of Blue trucks with associated escort units in a column formation. The convoy consists of two escort units of 5 HMMWVs each, one in the lead and one in the rear, and a supply unit with 30 trucks traveling in between. The convoy is traveling in an environment with rolling hill terrain and a somewhat developed road network. The convoy is en route to a humanitarian assistance site. An ambush has been set up to disrupt the convoy from completing its mission. The ambush party is a dismounted group with 24 members. The ambush party has buried a mine in the road to create a blockade either to stop or to disable the convoy.

Simple terrain features are represented through color. The gray area represents an obstacle, such as a mountain, which fully impedes movement and line of sight of the convoy vehicles. The yellow areas represent easy going terrain such as roads, and the dark and light green areas represent light and dense brush which partially impede movement speed and sight. The “red plus” sign represents the mine in

Excursions

- Variations explored:
 - Tactics - Vehicle Dispersion (2 formations)
 - Protection
 - Armor
 - UGV use
 - Designer Smoke

Force Protection Study

Tactics

- Two different vehicle formations were used as templates for the different excursions from the base
 - 5 HMMWVs – 30 Trucks – 5 HMMWVs
 - 4H – 30T – 4H with 1H on each flank

Force Protection Study

01

The two convoy formations included in the initial analysis are two examples of the kinds of tactics that can be modeled using Mana. The first formation represents a linear column formation with front and back HMMWV escorts for the convoy trucks. The escorts are split in equal numbers between front and

back. The trucks are grouped together in the middle of the formation. The second formation represents a flanked column, in which there are front, back, and two side HMMWV escorts for the trucks grouped in the middle of the formation. The same number of vehicles were used in both cases; just the arrangement of the vehicles is changed.



Armor



- Enhancement to convoy to improve survivability
- Modeled in Mana by using increased number of hits required to kill Blue as a proxy

Force Protection Study

92

Armor was modeled in Mana using a surrogate parameter – Blue hits to kill. This value represents the number of hits each Blue agent must sustain before it can be killed. The first hit puts a Blue agent into the injured state and subsequent hits are counted until this threshold is met. Once the threshold is met, a Blue agent is classified as killed.

Armor was included as part of the original RAND study and was thought to enhance convoy survivability – e.g., use of kevlar blankets. The same concept was modeled initially to check for consistency of results between the Mana Distillation and the RAND study.



UGV



- Without weapon: Draw out enemy
- With weapon: Take out mine and possibly draw out enemy

Force Protection Study

93

Use of a UGV was modeled to investigate what protection might be provided by a robotic vehicle, as well as situation awareness. Initially, the use of a UGV was modeled in two ways. First, it was modeled as an unarmed vehicle to draw out the enemy as a decoy, thereby foiling their element of

surprise. Second, the UGV was given a weapon that was equivalent to the capability of the HMWWV escorts. In the latter case, the armed UGV was able to destroy any detected mines or draw out the ambush party prior to the convoy arriving at the scene.



Smoke



- Designer Smoke reduces the enemy's ability to see while not affecting the force using the smoke
- Modeled through surrogates of increased Blue stealth and decreased Red sensor range in MANA

Force Protection Study

94

Designer smoke, an obscurant that reduces the enemy's ability to see without affecting the force using the obscurant*, was postulated to enhance Blue survivability through cover and concealment. This technology was also modeled initially to determine its impact on convoy protection/survivability.

* This assumes that Blue forces are equipped with aided vision equipment whose performance is not adversely effected by the designer smoke.



Initial Data Runs



- Two Convoy Formations
 - Armor
 - Without UGV
 - With UGV Unarmed & Armed
 - Blue Smoke Screen
 - Without UGV
 - With UGV Unarmed & Armed

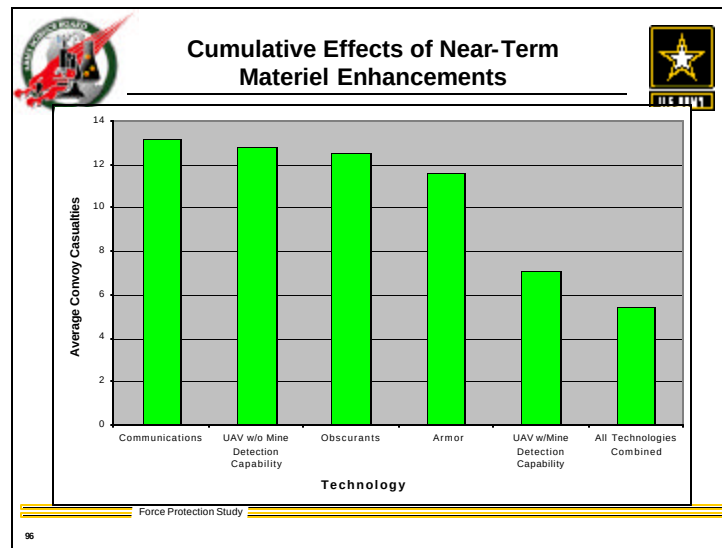
Force Protection Study

95

Using the Mana Distillation, initial parametric analyses were conducted on convoy operations to demonstrate the type of illustrative results the model could provide. The intent was to use initial results as a discussion mechanism among the Operations Panel, the Analysis and Modeling Panel, and the S&T Panel to refine their requirements for further analysis.

Initial results were gathered for the excursions described above. The technologies were explored independently and in combination to determine their maximum impact on convoy survivability. All

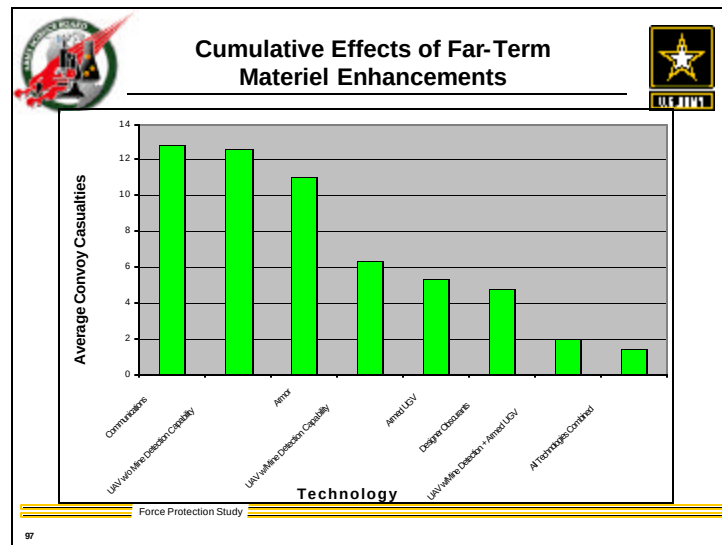
results should be considered as illustrative. However, it is maintained that the results are adequate to determine sensitivities in outcomes due to changes in parameter settings, demonstrate whether or not a parameter is important to the outcome of a scenario, or whether or not there is some point where the benefit of increasing the parameter plateaus and it is no longer affecting the outcome. If the more important parameters or boundaries of the parameters can be established, this could provide a point of departure for higher fidelity simulations to perform more rigorous assessments.



Using the Mana Distillation described above, several variations from the baseline were modeled to determine whether any proposed technology, or combinations of the technologies (representative of an integrated FP system), would affect the outcome of the convoy ambush. The base scenario models limited, less coordinated communications between members of the convoy, indicative of the fact that not all trucks have radios. Ballistic appliques and obscurants are not enhanced, but representative of what would normally be organic to the convoy. No UAV capability is assumed.

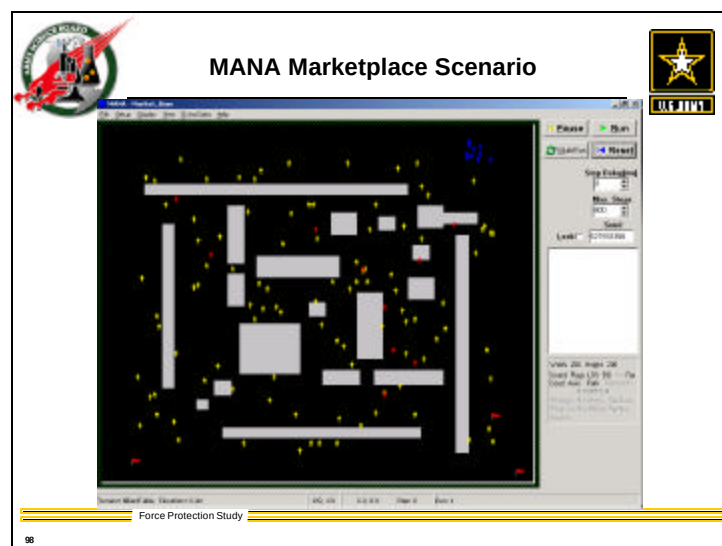
The convoy analyses focus on variations from this base case to include: better, more coordinated communications among convoy members; the addition of a UAV without mine detection capability to enhance situation awareness; the addition of a UAV with mine detection capability to improve survivability of the convoy; the use of obscurants; armored appliques; the addition of an armed UGV for mine detection and neutralization; and the combination of all of the technologies in the near- and far-term.

In the near-term, several technologies were identified that could be implemented quickly and could improve force protection for a convoy. The near-term technologies considered are depicted in this slide. Each was explored independently of the others to determine what improvements could be achieved by implementing individual technologies. Marginal improvements were found with individual technologies, except for the addition of a UAV with mine detection capability, which manifested the greatest decrease in convoy losses. When all technologies were combined to represent an integrated near-term FP system, the greatest decrease in Blue losses was observed. However, the improvement in Blue survivability for this latter case was relatively modest in comparison with the level achieved by adding a UAV enhanced with mine detection capability.

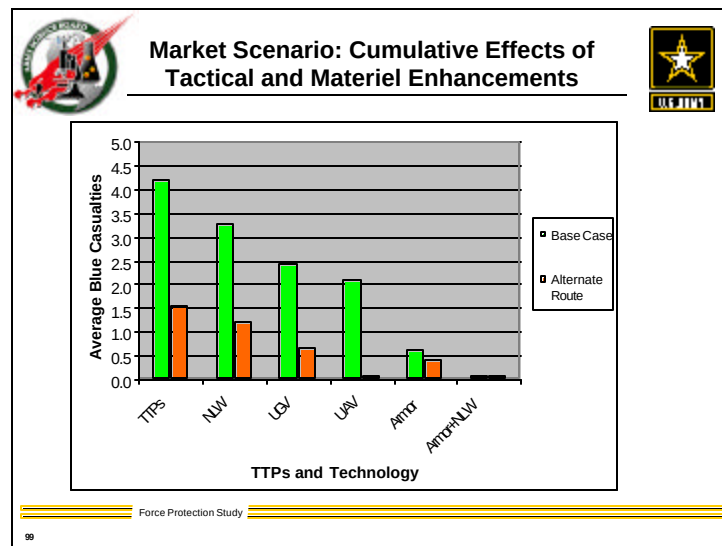


For the far-term, similar analyses were performed using the Mana Distillation. Technologies were analyzed individually and then in aggregate. The individual technologies include the list on the slide. For the far-term, the performance of each of the technologies was modeled as a substantial enhancement beyond the near-term. Other technologies are included in the far-term that were deemed infeasible to field in the near term.

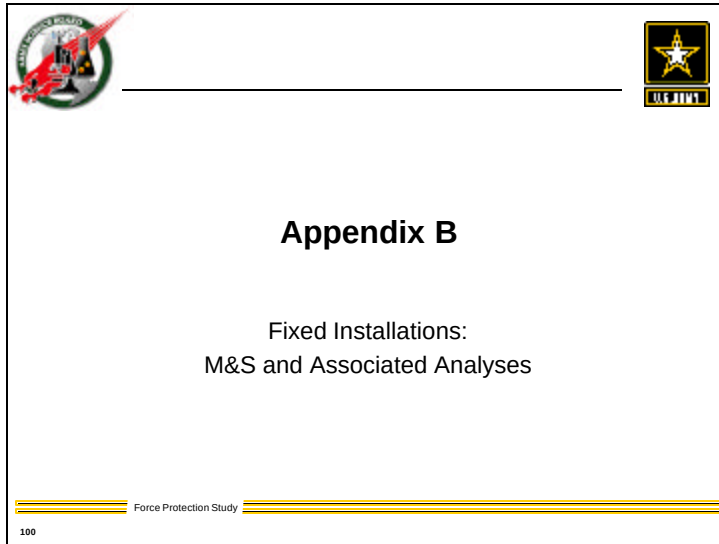
The effectiveness of the candidate technologies can be aggregated into three broad categories. In the first category, the technologies provide very marginal enhancements to convoy survivability. These technologies include enhanced communications, a UAV without mine detecting capabilities, and improved armor. In the second category, appreciable enhancements to convoy survivability are realized (e.g., approximately 50% to 65% better than category 1). These technologies include a UAV with mine detecting capabilities, an armed UGV, and designer obscurants. Finally, the third category provides very substantial enhancements to convoy survivability (e.g., approximately an 85% improvement beyond category 1). It consists of combinations of technologies: a UAV enhanced with mine detection capabilities plus an armed UGV in the lead to neutralize mines; and a combination of all of the technologies for the far-term. Note that the combination of all technologies for the far-term provides relatively modest improvement over the UAV/UGV addition.



Small unit operations (SUO) were also modeled using the Mana Distillation. In this scenario, a small blue force is patrolling a market place. The patrol route takes them through the heart of the market to an objective point at the other end of the market. The market is crowded with neutrals, however a few hostiles are spread throughout the area and will engage the blue force if encountered.



Initial analyses focused on modified procedures and technologies which might improve the Blue force's protection against an attack while on patrol. Options initially explored included changes in TTPs, such as using an alternate route if engaged by the hostiles within the crowd. It was hypothesized that using an alternate route would mitigate not only Blue losses but also collateral damage/losses. Use of non-lethal weapons as a suppressant were also explored to mitigate Blue losses and collateral damage. Furthermore, enhanced body armor, use of UGVs to explore ahead of the patrol, and use of a UAV to provide better situation awareness were investigated. Preliminary results indicate that the choice of TTP reduces Blue losses, as well as the combined use of body armor and non-lethal weapons. However, these results are illustrative and were used to guide further analyses. Subsequently, near- and far-term technologies identified by the S&T Panel were examined to help prioritize these technologies. Those results are summarized in the main body of this report.



The staff at Sandia National Laboratories has developed and applied a variety of tools to support the assessment of force protection for fixed installations. This appendix describes briefly their broad methodology and the tools that they have developed and applied to the problem. Emphasis is placed on the tools that they employed in support of the Analysis & Modeling Panel's deliberations.



Hazard Assessment and Mission Enhancement of Resources (HAMER)



- Problem
 - Commanders have no systems approach, based on *risk* and consequence, to assist them in making force protection decisions
- Objective
 - Provide commanders a prototype tool, that employs a *systems approach*, to make *informed, prioritized, force protection decisions*

Force Protection Study

101

Hazard Assessment and Mission Enhancement of Resources (HAMER) is a force protection software tool developed by Sandia National Laboratories. The HAMER prototype was completed in the Fall 1991. HAMER allows a military installation commander to make more informed risk management decisions based on mission, consequences, threat spectrum, vulnerabilities, constraints and available resources. The goal of the HAMER initiative was to demonstrate that by using this risk analysis tool a commander can make more informed force protection decisions. Within the HAMER prototype software the user proceeds through a logical sequence of events to determine the relative risk for potential targets identified on an installation. It helps the user determine the most critical targets, threat to these targets, consequences of successful attacks on the targets and the effectiveness of the protection system. HAMER provides the capability to develop a baseline scenario and then to perform what-if scenarios to reduce the risk. The HAMER program also has the capability to perform a top-level blast analysis (Reference 27).



Risk Equation



- Process for risk and resource management using a suite of tools and information
- Based on the risk equation:

System Risk → $R = P_A * [1 - P_E] * C$

Probability of Attack

P_A

Probability of Adversary Success (P_{AS})

P_I

Probability of Interruption

P_N

Probability of Neutralization

Consequences

C

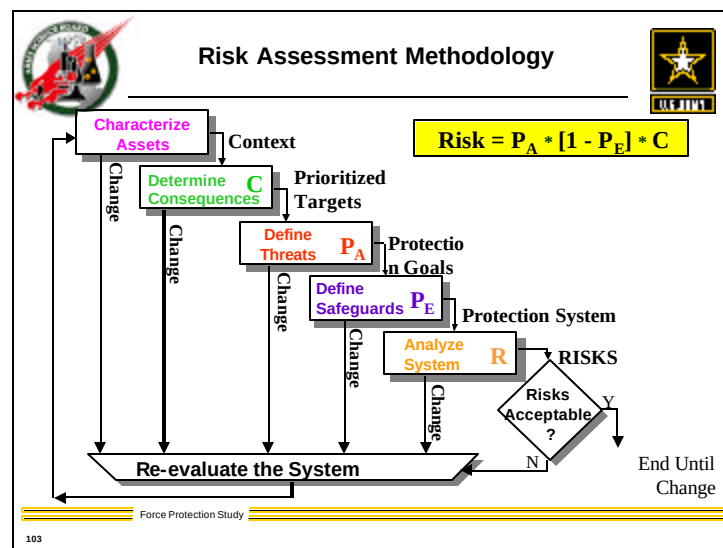
- Integrates many components into a single, consistent, approach for determining risk and making decisions

Force Protection Study

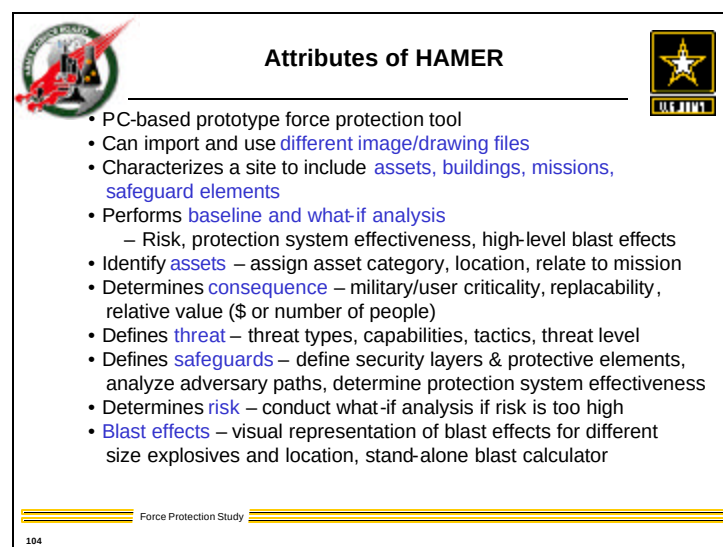
102

HAMER and other vulnerability assessment (VAs) and risk assessment methodologies (RAMs) developed at Sandia have the risk equation represented in the slide as the basis for the approach. The determination of risk ranges from qualitative to a more quantitative results depending on the approach and requirements.

The risk equation considers the threat, protection system effectiveness (i.e., adversary success) and consequences. The assessment of P_A involves the identification and characterization of potential threats and may also include consideration of the likelihood of adversary attack, target attractiveness, and other features which affect P_A . An analysis of P_A could assume that the adversary attack would take place and thus the probability of attack would be assumed to one. This would be a conditional risk. Criteria for consequences of identified undesired events may be loss of lives or injuries, damage to facilities/buildings, mission impact or other areas determined by the user. For HAMER consequences considers mission impact, replacability, and value (i.e., number of people affected or cost impact). The probability of adversary success is the compliment of protection system effectiveness, P_E . Two areas contribute to P_E : probability of interruption, P_I , which determines the effectiveness of the protection system to detect, assess, delay, and respond to an adversary attack, and probability of neutralization, P_N , which determines the ability of protective forces to engage and successfully defeat an adversary force once they are interrupted.



This slide depicts the basic RAM process and the steps necessary to determine a risk value. The process provides continual interactions among some of the steps and the ability to re-evaluate the risk if the risk is determined to be too high or changes occur which could affect risk.





Results from HAMER



Graphical – Site layout, blast effects

Tabular – Summary risk results



Asset Risk Components

BL 1

Total # of Assets: 97

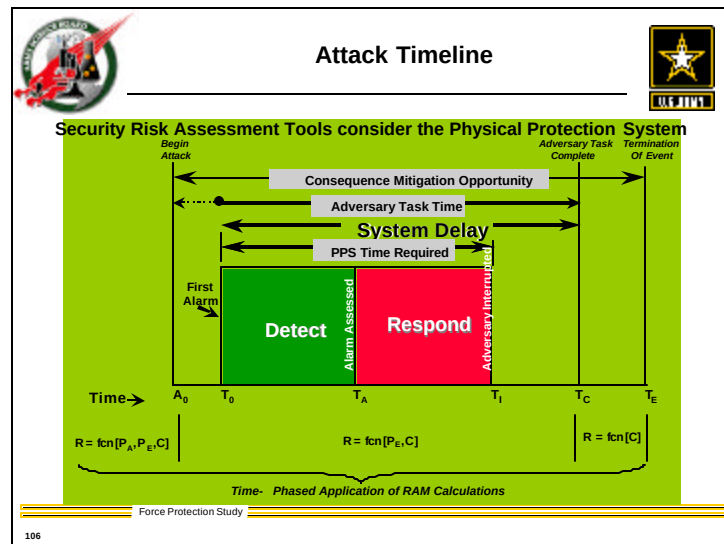
Sorted by Risk

	C	T	V	R
1st Military – Terminal	Red	Orange	Orange	Orange
2nd Military – Terminal	Red	Orange	Orange	Orange
3rd Hqs – Terminal	Red	Orange	Orange	Orange
4th Hqs – Terminal	Red	Orange	Orange	Orange
ADA Hqs – Terminal	Red	Orange	Orange	Orange
ADA Hqs – Terminal	Red	Orange	Orange	Orange
ADA Hqs – Control	Red	Orange	Orange	Orange
ADA Hqs – Control	Red	Orange	Orange	Orange
ADA Hqs – Unmanned Warfare	Red	Orange	Orange	Orange
ADA Hqs – Control	Red	Orange	Orange	Orange
ADA Hqs – Unmanned Warfare	Red	Orange	Orange	Orange

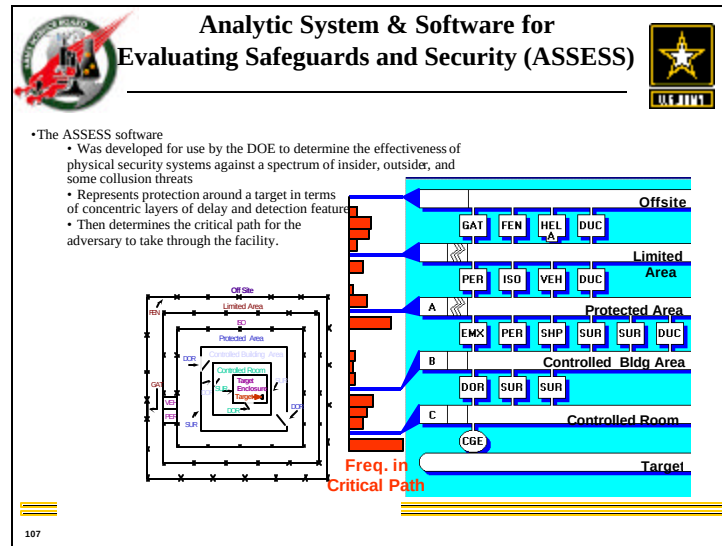
Slide 1 of 10

Key Very Low Low Medium High Very High

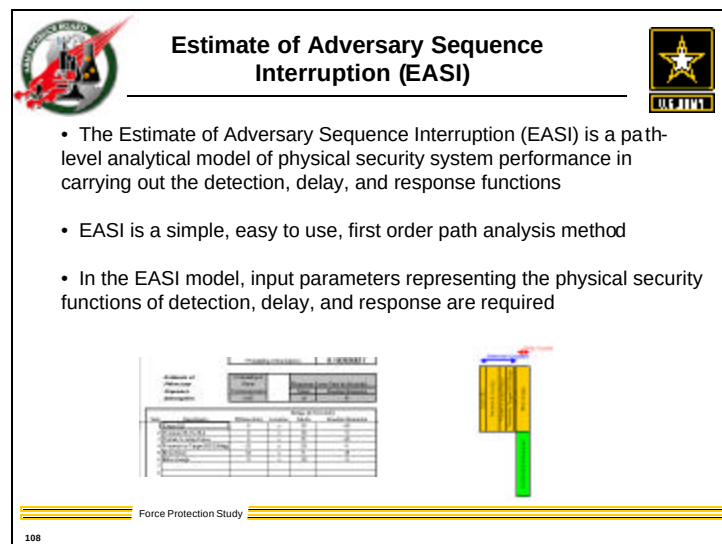
The slide shows the graphical results for an installation from a vehicle bomb. The color of the buildings reflects the level of damage to the buildings for the selected explosive size. In HAMER the user can let the program determine the location where the most damage would occur to a specific target or select the location of the vehicle bomb explosion. The chart is one of the overview charts and represents the overall risk and the results for the three components of risk (C – consequence, T – threat, V – probability of adversary success/system effectiveness). The results are color coded from very low to very high.



This slide represents the relationship and key points for the physical protection system (PPS). It includes consideration of both physical security and safety/mitigation measures. The PPS considers detection of the adversary attack, assessment, delay of the adversary, and notification and response of security forces and/or safety/mitigation systems. In this slide the response forces successfully interrupt the adversary before they reach the target.



ASSESS is a software tool developed initially for use in evaluating DOE nuclear facilities. It has subsequently been applied to many other types of facilities. It includes outsider adversary, insider adversary, and neutralization modules. In the slide, a facility is graphically represented by the adversary sequence diagram (ASD) on the right. The ASD represents the physical and protection layers and the protective elements between these layers. For each of these protective elements a delay time and detection probability can be assigned from a data base. ASSESS then performs an adversary path analysis and identifies the worst-case paths to the target. HAMER incorporates the principles of ASSESS and conducts a path analysis using a similar data base of detection and delay values. This data base was developed by Sandia based on many years of performance testing.



This slide show a simple single-path tool used over the years to determine the probability of interruption. The user defines the adversary path/steps from offsite to the target. Values for detection and delay are input for each step and a simple calculation is performed to determine the probability of interruption. HAMER uses the EASI approach in evaluating all of the possible paths to the target.



Security Effectiveness Assessment (SEA)



- The goal of an SEA is to conduct a systematic evaluation in which a performance criteria approach is used to measure the effectiveness of physical security systems employed
 - Across a broad spectrum of targets
 - Against a wide range of potential threats
- SEAs have been used to evaluate DoD (i.e., USAF) installations
- Steps in the SEA include
 - Facility Characterization
 - Target Screening and Identification
 - Consequence Analysis
 - Threat Identification
 - Physical Security System Characterization
 - Analysis Results

Force Protection Study

109

The security effectiveness assessment (SEA) is a vulnerability assessment approach that has been used at many DoD installations/facilities. The basic SEA approach is very similar to HAMER. The SEA approach is currently implemented manually.

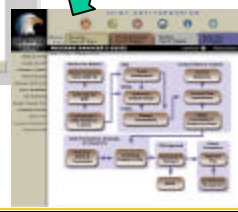


Joint Antiterrorism/Force Protection (JAT/FP) JAT Guide





Purpose: provide installation commanders with improved antiterrorism program management by helping plan, train, exercise, and review an Installation Antiterrorism Program IAW DoDI 2000.16 standards.



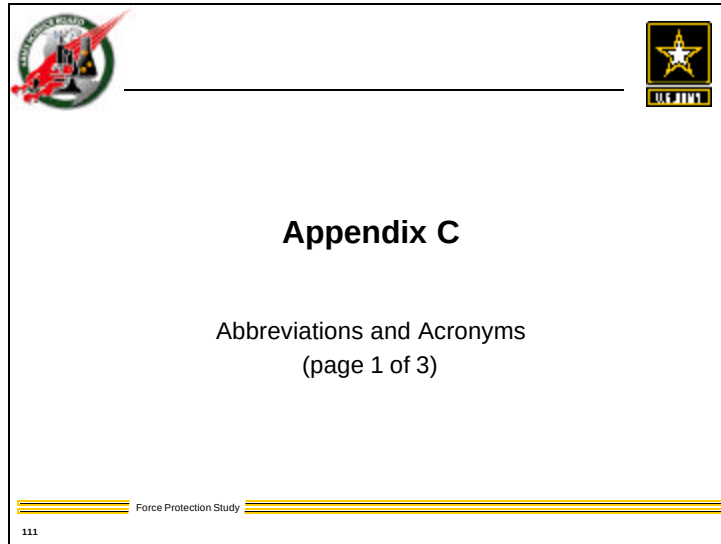
Lead: US Army COE, Engineer R&D Center
Sponsor: Joint Staff, J-3
DDAT/FP The product is an AT Program Management Guide (JAT Guide)

The program objective is to develop/provide/maintain process, tools, and templates in an operational framework for AT technology transfer

Force Protection Study

110

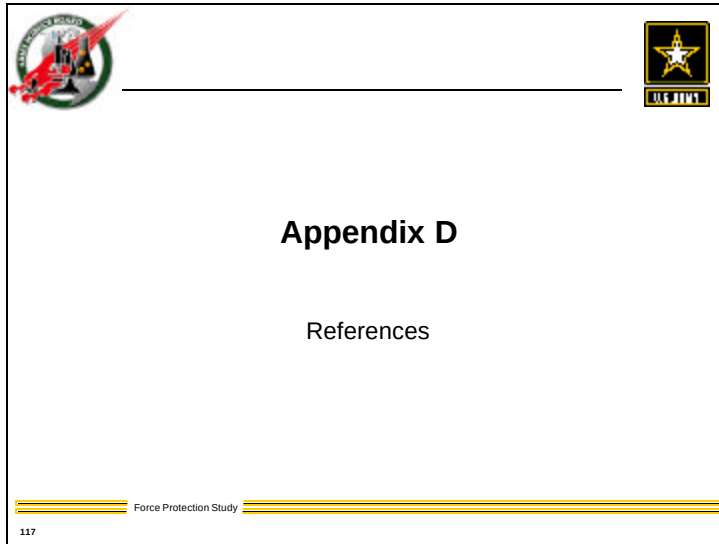
This slide is included to reference work currently being done within DoD to help installations improve their anti-terrorism and force protection programs.



Term	Definition
ACR	Advanced Concepts & Requirements
ADIDSS	Advanced DARPA Integrated Decision Support System
AEW	Airborne Early Warning
AFCCC	Air Force Combat Climatology Center
AMSO	Army Modeling and Simulation Office
AOR	Area of Responsibility
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics, & Technology
ATEC	Army Test and Evaluation Command
C2	Command & Control
C2OTM	C2 On the Move
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear and High Explosives
CC&D	Cover, Concealment, and Deception
CDR	Combat Decision Range
CGF	Computer Generated Force
CHESSS	Counterintelligence and Human Intelligence Exercise Scripting Support System
CI	Counterintelligence
COAs	Courses of Action
COTS	Commercial Off The Shelf
DAMO (AC, TR, ZS)	Organizations in the Department of the Army
DARPA	Defense Advanced Research Projects Agency
DISA	Defence Information Systems Agency
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities
DTRA	Defense Threat Reduction Agency
TD	Technology Development
DUSAOR	Deputy Undersecretary of the Army (Operations Research)
E&T	Education and Training
ESRI	GIS and Mapping Software Company
FACT	Focus Area Collaborative Team
FARP	Forward Arming and Refueling Point

FCS	Future Combat Systems
FFRDC	Federally Funded Research & Development Center
FLIR	Forward Looking Infrared
FOB	Forward Operating Base
FP	Force Protection
FPB	Force Protection Battlelab
FPCONs	Force Protection Conditions
GIS	Geographic Information Systems
GPUs	Graphic Processing Units
HAMER	Hazard Assessment and Mission Enhancement of Resources
HLS ACTD	Homeland Security Advanced Concept Technology Demonstrations
HPAC	Hazard Prediction and Assessment Capability
HUMINT	Human Intelligence
ICT	Institute for Creative Technologies
IFFN	Identification Friend, Foe, or Neutral
JANUS	Name of a constructive simulation
JCATS	Joint Conflict and Tactical Simulation
JEM	Joint Effects Model
JTRS	Joint Tactical Radio System
JVB	Joint Virtual Battlespace
LCT-50	The level at which 50% of the exposed population will be affected
M&S	Modeling & Simulation
MANA	Name of an agent based model
MATREX	Modeling Architecture for Technology and Research Experimentation
MOB	Main Operating Base
MOPP	Mission Oriented Protective Posture
MOUT	Military Operations in Urban Terrain
MPARS	Mission Planning and Rehearsal System
NDI	Non Developmental Item
NLOS	Non Line of Sight
NLW	Nonlethal Weapons
NRC	National Research Council
OACSIM	Office of the Assistant Chief of Staff for Installation Management
One SAF	One Semi-Automated Forces
ONR	Office of Naval Research
PALM	Portfolio Analysis Machine
PD-PFA	Probability of Detection-Probability of False Alarm
PEO	Program Executive Officer
POAM	Plan of Action and Milestones
POL	Petroleum, Oil, and Lubricants
RDA	Research, Development & Acquisition
RDE	Research, Development & Engineering
RDECOM	Research, Development & Engineering Command
S&T	Science & Technology
SASO	Security and Stability Operations
SENSE	Synthetic Environments for National Security Estimates (a model developed by IDA)
SMART	Simulation and Modeling for Acquisition, Requirements, and Training
SOFPARS	Special Operations Forces Planning and Rehearsal System

SOSIL	System of Systems Integration Laboratory
SPAWAR	Space and Naval Warfare System Command
STRI	Simulation, Training, and Instrumentation
SUO	Small Unit Operations
TEMO	Training, Exercises & Military Operations
TLAC	Think Like a Commander
TRAC	TRADOC Analysis Center
TRADOC	Training and Doctrine Command
TTPs	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicle
UGVs	Unmanned Ground Vehicles
VERTS	Virtual Emergency Response System
WMD	Weapons of Mass Destruction



1. Combat Decision Range (CDR). See http://www.mcwl.quantico.usmc.mil/fact_sheets/fs/cdr_h.pdf
2. Full Spectrum Warrior. See http://www.ict.usc.edu/disp.php?bd=proj_games_fsw
3. Think Like a Commander (TLAC). See / http://www.ict.usc.edu/disp.php?bd=proj_clas
4. Eagle Defender. See <http://www.mrassociates.com/Eagle.htm>.
5. VERTS. See http://www.mt2-kmi.com/Archives/7_8_MT2/7_8_QA.cfm
6. Counterintelligence and Human Intelligence Exercise Scripting Support System (CHESSE) User Manual, US Pacific Command, May 2003.
7. Hazard Assessment and Mission Enhancement of Resources (HAMER). See <http://www.dtic.mil/ndia/security2/jaeger.pdf>
8. Mana. See <http://www.mcwl.quantico.usmc.mil/divisions/albert/research/index.asp>
9. Hazard Prediction and Assessment Capability (HPAC). See http://www.dtra.mil/td/acecenter/td_hpac_fact.html
10. National Research Council (NRC) Study. "Tracking and Predicting the Atmospheric Dispersion of Hazardous Material Releases: Implications for Homeland Security"; see <http://www.nap.edu/books/0309089263/html/57.html>
11. Joint Effects Model (JEM). See <http://www.sbccom.army.mil/busops/follas-jem.ppt>
12. ESRI's Arcview GIS. See <http://www.informs-cs.org/wsc01papers/089.PDF>
13. Mission Planning and Rehearsal System (MPARS). See <http://www.onesaf.org/MPARS%20and%20MDMP.ppt>
14. Lanchester convoy analysis. See <http://diana.gl.nps.navy.mil/~washburn/Files/Lanchester.pdf>
15. Advanced DARPA Integrated Decision Support System (ADIDSS), Briefing to ASB Analysis & Modeling Panel, Sandia National Labs, 12 June 2003
16. The Genetic Algorithms Archive. See www.aic.nrl.navy.mil/galist/
17. MOUT Focus Area Collaborative Team (FACT). See <http://www.tradoc.army.mil/dcssa/Briefings/Fall%20cocsep02/MOUT%20FACT%20Paper.doc>
18. Installation Transformation Wargame. See <http://www.hq.usace.army.mil/cepa/pubs/dec02/story11.htm>
19. IDA's SENSE. See <http://www.ida.org/DIVISIONS/sfrd/S.E.N.S.E./pages/background.html>
20. OneSAF. See OneSAF <http://www.onesaf.org/>
21. Graphics Processing Units (GPUs), See <http://wwwx.cs.unc.edu/~harrism/gpgpu/index.shtml>
22. Captain J. M. Pierre, "Convoy Live Fire: Training the Support Platoon to Defend Itself in Ambushes". See <http://call.army.mil/products/trngqtr/tq4-01/pierre.htm>

23. "Public Health Consequence Management Strategies and Urban Defense and Response Architectures" Defense of Cities Against Biological Weapons Attack Study, Washington Institute, McLean, VA, May 2003.
24. ASB 2001 Summer Study. "The Objective Force Soldier/Soldier Team", July 2001
25. FIST Countermine Phase I Report, Sandia National Labs. July 2002
26. Brian K. Schmidt, T. N. Shimi, "C4ISR Investment Planning with the Portfolio Analysis Machine (PALM)", MITRE Technical Report, MTR 00B0000057V01, December 2000
27. SAND Report 2003-0085, "HAMER Report (Hazard Assessment and Mission Enhancement of Resources); Part I: Program and Prototype Review; Part II: Tools for Force Protection", March 2003. [Note: This is a limited distribution SAND Report; interested individuals should contact the lead author and HAMER POC: Cal Jaeger, cdjaege@sandia.gov].



Interface Panel Report

Force Protection Study

Interface Panel Report

Forward

The Panel's Report was prepared during the period December 2002 through July 2003. Early on, the Panel recognized the important role that Civil-Military Operations (CMO) could serve to enhance force protection throughout the "phases" of a campaign, e.g., by supporting HUMINT and situational understanding, and drawing upon civilian support and enhancing goodwill, while lowering the threat level through the stabilization of civil society (and its security apparatus). This Report discusses at some length these force protection benefits of CMO and sets out recommendations to make CMO even more effective.

Operation Iraqi Freedom (OIF) added new emphasis to the Panel's approach by illustrating the unique force protection and CMO challenges that exist in the aftermath of large-scale combat operations. This Report uses the term "Phase IV operations" to refer to those kinds of operations, which occur in the period after the conclusion of major combat operations (Phase III), but before the emergence of a stable and secure environment in which civilians (governmental and non-governmental) are able to engage in reconstruction. The term Phase IV operations is based on Joint Service doctrine and is consistent with Army doctrine.¹

The Panel observes that OIF planning did not effectively anticipate the difficult Phase IV tasks the Army would face following the conclusion of major combat operations (Phase III). The Report includes specific recommendations that flow from the belief that force protection in Phase IV is dependent on planning and actions that begin in Phase I. Only with these kinds of planning and actions will the Army be well-positioned to build the stable environment necessary to transition more of the security burden to civilian authorities — non-military, US Government and indigenous authorities — who will be engaged in reconstruction activities. It is that stabilization and transition that will most relieve the enormous force protection burden the Army otherwise must shoulder.

I. Terms of Reference, Study Focus and Organization of the Report

The TOR focused the "Interface Panel" in the following manner:

Address problems and opportunities associated with international operations, including commercial, governmental, non-governmental and infrastructure environments in which the Army must operate and accomplish force protection.

¹ See FM 3-0 Chapter 9. In addition, Phase IV operations can also occur in other circumstances, including, for example, when Army forces are deployed where there is failed state.

The TOR presented the Panel with an expansive landscape in which to consider the opportunities and risks associated with Army interactions with non-Army organizations that affect force protection.

With respect to force protection, there are a large number of scenarios and environments, involving a limitless number of third parties (commercial, governmental, non-governmental). For the reasons set out immediately below, the Panel believed it most valuable to focus its efforts on those environments and operations that present exceptional force protection “problems and opportunities.”

1. By its language, the above-cited portion of the TOR is limited to international operations, although other portions of the TOR include CONUS. Accordingly, the Panel narrowed its focus to OCONUS operations.
2. The number of external parties with whom the Army interfaces OCONUS is large and varied; the interfaces occur typically along functional lines at the staff level, e.g., law enforcement to law enforcement, intel to intel, Civil Affairs units to local government agencies and NGOs. In OCONUS operations, units not engaged in major combat operations (e.g., involved with rear area security, peacekeeping) interface formally and informally with civilians. These interfaces are Civil-Military Operations (CMO) -- largely the formal province of Civil Affairs forces. The Panel explores these CMO and force protection in Section II of this Report.²
3. In Section III of the report, the Panel focuses on “post-conflict” stability operations³ or Phase IV operations, and the importance of the underlying planning process.
4. Finally, the use of civilian contractors emerged as a cross-cutting risk area. The unique impact of the interface with commercial entities and local workers is addressed in Section IV of the Report.

² The Panel understands that the JIACG (Joint Interagency Coordination Group) concept is being implemented at many of the Combatant Commands, including CENTCOM (in Operation Iraqi Freedom (OIF)). The impetus for the JIACG was Khobar Towers, which was the subject of the Downing Report. That report recommended improvements to the quality of USG communications and coordination within a theater of operations, with the “country team.” The report also recommended improved interagency campaign planning and execution. The Panel did not re-examine the JIACG concept, which has been evaluated and tested by JFCOM.

Likewise, the Panel did not revisit the Downing Report’s examination of the problem posed by too frequent rotation of intelligence and counterintelligence personnel, and its impact on both collection and force protection. Nor did we revisit the Downing Report’s examination of the interface with local security forces concerning base protection.

³ FM 3-0 (para 9-18) describes Stability Operations as follows: “Army forces may conduct stability operations before hostilities, in crises during hostilities, and after hostilities. Before hostilities, stability operations focus on deterring or preempting conflict. In a crisis, they may resolve a potential conflict or prevent escalation. During hostilities, they can help keep armed conflict from spreading and assist and encourage partners. Following hostilities, stability operations can provide a secure environment that allows civil authorities to reassume control.”

II. Effective Civil-Military Operations and Force Protection

The Panel was asked to address interfaces and force protection problems and opportunities. At bottom, it is difficult to quantify or even *prove* the effects of specific Army interactions with local populations and institutions upon force protection. On the other hand, it appears intuitively obvious and there is ample anecdotal evidence that force protection is enhanced by good working relationships with local communities in the Area of Operation (AO). But that enhancement is a second order effect. Interfaces do not provide force protection, but they can support force protection in several ways. Interactions with local communities that build trust or demonstrate the Army's good intentions should generally reduce hostility, dampen incitements to violence, promote cooperation, ease information collection, and promote coordination of action. Here are two contrasting anecdotes:

An armed Army patrol was proceeding through a Muslim community approaching a Mosque where a meeting was being held. The gathered group saw the patrol approaching, became concerned and increasingly agitated. Not wishing to incite an incident, having no reason compelling reason to become defensive or offensive, the patrol leader commanded the patrol to lower their weapons and point them at the ground while continuing to proceed. Once the crowd saw the lowered weapons, tensions eased without a confrontation. Did this peaceful encounter contribute to some local residents starting to question some of the stereotypes about American intentions? Probably.

A negative example is equally instructive. A commander's "predilection for punitive forays in response to even minor incidents like theft did cow many (local leaders), but he also undermined many alliances and relationships painstakingly established by local commanders. Instead of quieting small disturbances, (the commander's) expeditions often created larger problems by driving pacified or neutral villages into joining more rebellious ones, and made it more difficult for his subordinates to gain local trust."⁴

How units and the individual soldiers in units interact with local populations can clearly help shape the threat environment and the force protection requirements. The experience of Afghanistan, Bosnia, Kosovo, and Iraq has provided an extensive body of literature that has examined these operations and interactions. This Report draws force protection implications from those experiences.

The Value of Robust Interactions with the Local Public and Civil Organizations

⁴ Crane and Terrill, RECONSTRUCTING IRAQ: CHALLENGES AND MISSIONS FOR MILITARY FORCES IN A POST-CONFLICT SCENARIO, Strategic Studies Institute, U.S. Army War College (January and February, 2003) pp. 12-13 (hereinafter "Crane and Terrill").

The threshold conclusion of this Report, albeit intuitively obvious, is an important starting point: Robust interactions with the local populations, civilian and non-governmental organizations can support mission accomplishment and support force protection. However, force protection concerns can invite a “bunker mentality,” as there is short-term safety behind the wire. In the long run keeping the Army from robust interactions with local populations for force protection purposes is illusory. Instead of seeing interactions as only a threat, robust interactions with local communities can build linkages that can buttress the commander’s force protection capability and lower the threat level.

The Report of the Commission on Post-Conflict Reconstruction (published by the Center for Strategic and International Studies (CSIS) and the Association of the U.S. Army (AUSA)) observed: “While security is essential, it will never be one hundred percent guaranteed and the perfect must not become the enemy of the good.”⁵ It is simply not possible to accomplish the missions being encountered by the Army today if the establishment of local stability is left to local populations that do not have a functioning security capacity. The longer it takes to accomplish stability, the longer the Army’s forces are exposed to a hostile threat environment with its danger of continuing casualties.

Overly restrictive force protection measures can interfere with mission accomplishment and can be counter-productive. One thorough examination of operations in Bosnia and Kosovo concluded: “Measures such as the four-vehicle convoy rule, the wearing of full battle dress, and restrictions on leaving the immediate area of operation did not permit the teams to operate to their fullest potential.”⁶ These measures can have the counter-intended result of interfering with force protection insofar as they impede gathering “insights into intentions and the general “pulse” of the operational environment.”⁷ Moreover, overly restrictive force protection rules can actually impede the conduct of the civil affairs functions by making it difficult for the US forces to interact with NGOs and other civilian organizations operating outside the wire.⁸

This may translate into powerful perceptions of US forces. The press has commented on the contrasting ways in which US forces and other nation’s forces address force protection and how they are perceived by indigenous populations in post-conflict, peacekeeping and other similar deployments. For example, in a London Sunday

⁵ *Play to Win, Final Report of the bi-partisan Commission on Post-Conflict Reconstruction* (January 2003), p. 6 (hereinafter referred to as the CSIS-AUSA Report).

⁶ Wentz, “Lessons from Bosnia: The IFOR Experience” (1997) p. 69 (hereinafter “IFOR”).

⁷ *Ibid* p. 69.

⁸ *Ibid* p. 135. “[F]orce protection regulations hampered CIMIC personnel’s ability to perform their CIMIC mission effectively. When CIMIC personnel were able to muster the needed four vehicles to leave the base, they arrived at an NGO site with a heavier military presence than some NGOs desired. As a related issue, the appearance of the need for great security when outside the protected confines of Tuzla Main worked counter to the efforts of CIMIC personnel to create an impression among the local population that the internal situation had improved. Finally, with the inaccessibility of the Tuzla CIMIC to the NGOs and the restrictive procedures limiting the CIMIC staff’s ability to visit the NGOs, the requirement to communicate indirectly had increased.”

Telegraph article, the differing approach taken by the British and US soldiers in Iraq was contrasted as follows:

[The British] have abandoned their helmets in favor of their more people-friendly berets, have taken off their body armor and mingle with the locals. They have helped to set up a local police force and a council to get the city's infrastructure running smoothly.

The Americans are, admittedly, bound by much less flexible rules. Their Force Protection Doctrine decrees that all soldiers must wear helmets and body armor in a war zone at all times and that gunfire must be met with response. * * * The British have learned in the past 30 years that good information on the enemy was their best protection and that putting soldiers at risk to get it was justified.⁹

Flack vests, helmets, and weapons can intimidate civilians and, as a result, interfere with civil-military affairs. There may be valid reasons why in the same theater of operations US forces might be more wary; perhaps the threat to US forces (as the lead nation and a choice target) may be greater. But, the point is “not necessarily whether or not troops deploy subject to enhanced force protection measures ... but that the military and political leadership understand the effects of such measures on the perceptions of the local population”¹⁰ as well as the effect on HUMINT collection, improving situational understanding, engendering good will, and enhancing civil security. The key is to interface with the population and its leaders -- little is accomplished (and little progress is made toward mission accomplishment) unless this is done.

The Role of Local Civil Security and Force Protection

In stability operations there are two fundamentally different ways to provide force protection. The first, and best understood, are classic defensive and offensive military operations designed to protect Blue forces and impede or destroy Red forces. However, there is a second way to address force protection requirements: Lower the threat level by improving the capacity of local civilian authorities.

The Commission on Post-Conflict Reconstruction noted that “efforts to design and reconstruct or reform local security institutions, including both military and police, must begin early in the peace process.”¹¹ The Army must embrace this responsibility, as early as possible, because it is the only institution capable of operating in dangerous threat environments and securing order. This responsibility is manpower intensive.

In Phase IV operations, building the indigenous local security can be an economy of force measure because it creates the potential use of non-Army forces to reduce the threat

⁹ See also, Wentz IFOR p. 210.

¹⁰ Ibid p. 212.

¹¹ CSIS-AUSA Report p. 7.

level. As the capacity of local authorities to maintain a stable, secure environment grows, local security assets can complement US force protection activities (e.g., information sharing/validation, guarding infrastructure) and ultimately reduce the burden borne by US forces.

The Commander has a variety of means to help build the civil security capacity to lower the level of threat and complements the Army's own force protection measures. Military Police are one. Another major tool is the use of Civil Affairs resources that:

Provide Combatant Commanders the ability to engage the civil component within the operational environment ... to mitigate and defeat threats to or by civil society and assist in establishing the capability for deterring or defeating those threats in the future.¹²

The Panel's conclusion is that rapidly establishing a viable public security capability is one of the commander's best courses of action for reducing force protection requirements and expediting the transition of non-military tasks to civil organizations. Based on comprehensive reviews of the Kosovo and Bosnia missions, one scholar portrayed this civilian security capacity as a three-legged stool consisting of police, courts, and prisons.¹³



This scholar also observed: "Generally, progress in one area of the security triad is ineffective without timely improvements in all areas. Additionally, improvements by the

¹² TTP for Civil Affairs, 3-05.40, Chapter 1, page 1-1. The Army's Civil Affairs capacity has a series of responsibilities in these environments that typically involve: Governance and Civil Administration; Rule of Law/Public Safety; Public Education; Health Infrastructure; and Economy.

¹³ Wentz, "Kosovo: The KFOR Experience" p. 259 (2002) (hereinafter "Wentz KFOR"). In this Report, the Panel uses the term police in the broad context to include all non-military public security forces such as border police, and national and local police forces.

civil administration in one area do not necessarily result in diminished responsibilities for the military.”¹⁴

It is important to recognize that as indigenous civil capacity to predict, monitor, deter, and deny threats increases, the Army’s ability to accomplish the underlying mission increases. Robust civil security capacity can complement US force protection by: (i) facilitating information sharing and validation, (ii) increasing the security presence and effectiveness, and (iii) ultimately assuming responsibility for security. In essence, the sooner a robust local infrastructure is established (or re-built) the sooner the transition to civilian authorities occurs, and the sooner the size of the Army’s forces devoted to security and stabilization can be reduced (along with the associated force protection burden).

Civil-Military Operations can be enhanced, and its force protection value increased, in several ways. The Panel offers a series of recommendations, which are discussed below.

1. Training and Education

A variety of studies have identified a weakness in the preparation of officers and NCOs to interact successfully with groups and individuals with whom these soldiers must interface in foreign deployments. One area is negotiation skills.

Officers and NCOs will be in close contact with combatant and noncombatant groups in situations where decentralized diplomacy and on-the-spot negotiating skills can defuse a volatile situation, possibly saving American, allied, and noncombatant lives. We cannot place the lives of those officers and NCOs at risk by failing to prepare them for the challenges of negotiating under adverse conditions with individuals from other cultures. We have to find ways to adapt our formal training of officers and NCOs to develop the skills they will need to succeed in such situations.¹⁵

* * *

In peace operations such as Kosovo, required skills include patience, the confidence to delegate authority and take risks, and the ability to engage with people outside the military, including representatives of nongovernmental and international organizations and the media. The army needs to develop a set of general principles that enhances all levels of officer education, including reference to geopolitics, cultural awareness, foreign languages, and interpersonal skills.¹⁶

Similarly, the US Institute for Peace suggests that learning to interface with local authorities should be included in the curriculum of senior service colleges:

¹⁴ *Ibid.*

¹⁵ Stofft, William A. and Guertner, Gary L. "Ethnic Conflict: the Perils of Military Intervention." *Parameters* 35 (Spring 1995): 30-42. (<http://carlisle-www.army.mil/usawc/Parameters/1995/stofft.htm>)

¹⁶ Howard Olsen and John Davis, Training U.S. Army Officers for Peace Operations: Lessons from Bosnia (<http://www.usip.org/oc/sr/sr991029/sr991029.html>) (hereinafter “USIP Bosnia Lessons”).

Most general officers interviewed for this study singled out senior service college institutions as the place where leadership training for peace operations must be conducted and the place that needs the most curriculum development. A greater emphasis on peace operations and on geopolitical and cultural awareness is needed at these institutions.¹⁷

While CMO doctrine will be important to address these matters, the Balkans experiences suggest that negotiating skills, cultural awareness, and geopolitical understanding are more important than highly developed doctrine: “Soldiers often forget doctrine, but they less often forget the training that shapes their instincts in the field.”¹⁸

Recommended Action:

Curriculum development at the senior service colleges should include greater consideration of geopolitics, cultural awareness, foreign languages, negotiation and interpersonal skills necessary for peacekeeping and reconstruction deployments, as well as simulations and robust exercises for Phase IV/stability operations.¹⁹

2. Communications Capacity

In addition to physically interacting with local populations, it is essential to communicate in the most robust manner. The Civil-Military Operations Center (CMOC) is the nerve-center of communications and coordination between the US military and civilian organizations providing relief and other assistance. The CMOC maximizes ability of all the parties to coordinate. It can be a physical place and on the web, thus eliminating the need for all the participants to be in the same place at the same time.

In Bosnia, the CMOC (aka the CIMIC) was behind the wire, while most of the NGOs operated in town.

With access to the base by non-IFOR personnel strictly limited, the effectiveness of the CIMIC Center as a tool for coordinating NGO and military activity was greatly reduced.²⁰

The humanitarian relief organizations tend to have limited communications and information system capabilities, especially in the theater of operation. Typically, they will use the in-country telecommunications infrastructure to the extent possible but many also have their own HF and/or VHF radios. These radios,

¹⁷ Ibid.

¹⁸ Wentz KFOR pp. 501-04.

¹⁹ The Panel concurs in the parallel recommendation of the Operations Panel concerning the importance of parallel training for company grade officers and NCOs, to support their ability to diffuse confrontations with local citizens.

²⁰ Wentz IFOR p. 135

however, may or may not be interoperable with the military systems they come in contact with during peace operations.²¹

Recommended Actions:

The Army should procure and distribute as soon as possible compatible communications radios, telephone, and computer systems to the Military Police, local police, Military Intelligence and local intelligence assets, Military medical services and local medical services and all other US civil-military liaison personnel and their local counterparts.

The Civil Military Operations Center (CMOC) should be made a TOE element at the Civil Affairs Battalion level and above.

III. Phase IV Operations – A Force Protection Planning and Execution Challenge

Regardless of however the Army addresses the general CMO issues discussed in Section II, there are unique force protection challenges in Phase IV operations.

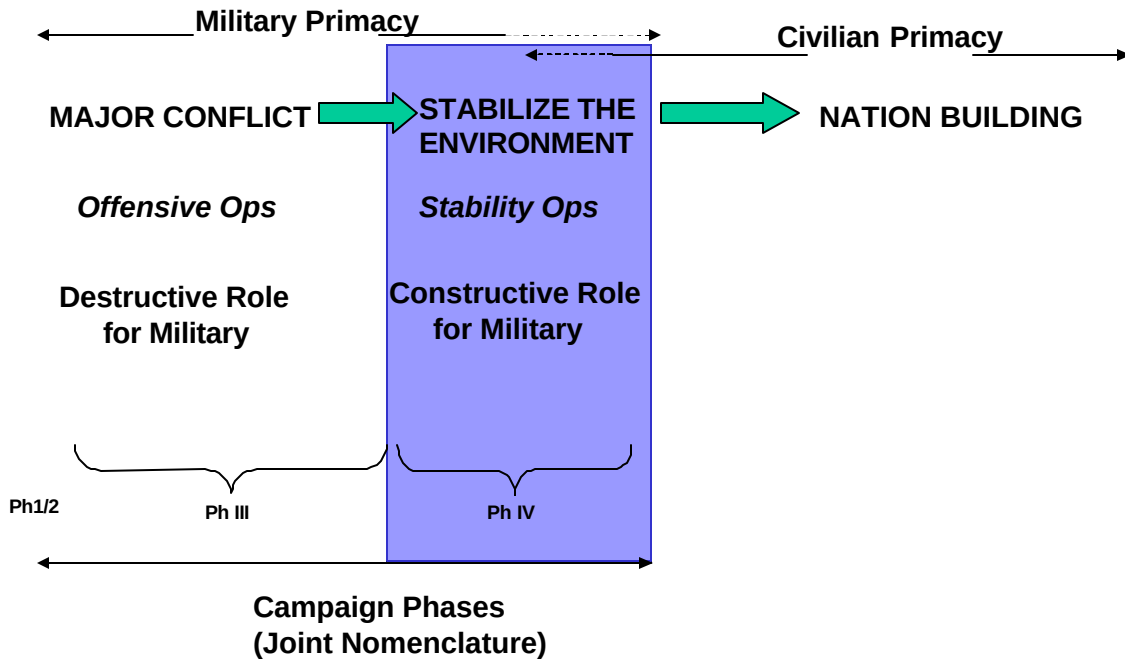
During Phase IV operations, the military role should recede. That is not to say that there is no civilian role beforehand or that there is no military role afterwards; it is simply that there is a transition from military to civilian responsibility for a safe and secure environment. During this transition period, there will be a phasing from primarily military responsibility to primarily civilian responsibility. This overlap must be coordinated and de-conflicted through the inter-agency process and the in-country Joint Inter-Agency Control Group (JIACG). Moreover, during this Phase IV period stability operations can be ongoing while combat operations continue elsewhere.²²

Below is a roadmap representing this space, and the relationship between the military operations (Phases I-IV) and the transition to civilian responsibility.

²¹ Wentz IFOR p. 419

²² "When conducting full spectrum operations, commanders combine and sequence offensive, defensive, stability, and support operations to accomplish the mission. The JFC and the Army component commander for a particular mission determine the emphasis Army forces place on each type of operation. Throughout the campaign, offensive, defensive, stability, and support missions occur simultaneously Operations designed to accomplish more than one strategic purpose may be executed simultaneously, sequentially, or both. For example, within a combatant commander's Area Of Responsibility (AOR), one force may be executing large-scale offensive operations while another is conducting stability operations. Within the combat zone, Army forces may conduct stability operations and support operations as well as combat operations." (FM 3-0, Operations, 14 Jun 03, para 1-49, pg. 1-16.)

Focus of Interface Panel: Stability Operations-Phase IV



There are many historical examples (e.g., Germany, Japan, Iraq, and Afghanistan) where the Army's involvement did not end upon enemy capitulation from direct combat. Instead, achieving a durable solution (i.e., a safe and secure environment for the conduct of reconstruction and humanitarian assistance in the absence of US conventional forces),²³ required a substantial investment of resources in the conduct of Phase IV operations. Indeed, Phase IV operations have become an integral component of every major military campaign in the last decade.

The transitory nature of these operations (phasing from combat operations to civilian control) presents the commander with a difficult force protection challenge. For example, in a large nation, such as Iraq, the end of large-scale combat operations does not necessarily mean the end of all combat operations. Pockets of resistance, including resistance by an enemy that may have attempted to blend back into local populations, can continue in parts of Iraq for a period of time. This environment is not stable. Stability does not increase or decrease in a uniform or linear fashion. Islands or pockets of instability can appear, disappear and then reappear. The threat level may ebb and flow in an unpredictable fashion.

The commander's expectations about the level of threat and the capacity of the local civilian government to deter or defeat those threats may not match the reality he ultimately faces on the ground. Operations that follow major combat activities need to be matched to the environment created by the Phase I-III activities. It is, of course, exceedingly rare that the commander knows before a war what the military and civil landscape will be after Phase III. It is natural to be optimistic; this was the case in Iraq. In virtually all cases, it is still unlikely that expectations, whatever they might be, will be met. Dealing with this "gap" between assumed and actual "civil capacity" can be a major risk that must be addressed more fully in the initial inter-agency and Army planning processes. The special importance of bridging this gap is discussed below, and the need to plan and execute throughout the campaign with Phase IV's "bridge" objectives firmly in mind.

The Critical Force Protection Importance of the Phase IV Transition: Dangerous but Essential to Navigate Successfully and Rapidly

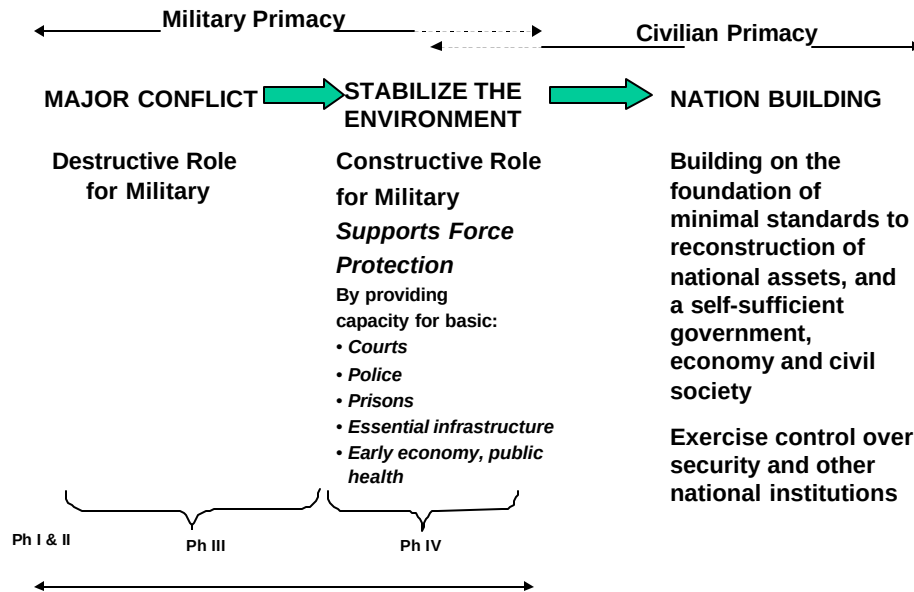
There is a dangerous gap between the end of war ... and the establishment of a stable foreign nation capable of providing essential services. The gap is "instability" in which victory on the battlefield can be lost to upheaval, violence and disintegrating social structures. Military operations must continue to prevent anarchy and to support short-term and long-term recovery. ... [One] mission of

²³ Here one must differentiate force presence in furtherance of subsequently or separately established, mutual security agreements or treaties such as NATO, from forces needed to accomplish a Phase IV mission. Army forces that have remained in Germany and Korea for 50 years are no longer engaged in Phase IV activities.

the U.S. military is to [be] the bridge to stability as the civilian agencies bring their development programs online.²⁴

Expanding upon the “map” of the Phase IV space, one can visualize the kinds of tasks that would be undertaken by the Army during Phase IV operations and the relationship between those tasks and those that will be undertaken by civilian authorities.²⁵

Map of Key Roles For Phase IV Operations

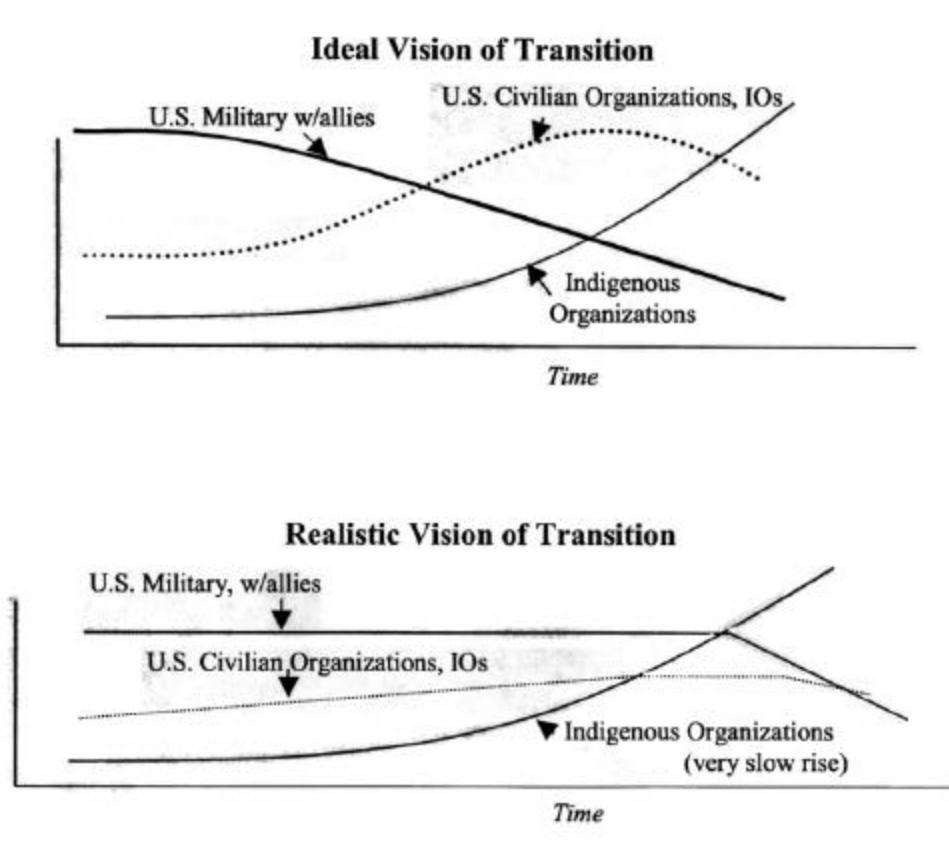


²⁴ Bingham, Rubini and Cleary, “U.S. Army Civil Affairs—The Army’s ‘Ounce of Prevention’” (Land Warfare paper No. 41, March 2003), p. 8 and p. 20.

²⁵ Some stability tasks will always be required of the military in Phase IV operations and are uniquely the province of the military. For example, the military is uniquely capable to provide initial security and de-confliction, processing detainees/refugees. Other tasks will vary in their scope and level of effort depending on the status of the infrastructure and the civilian capacity existing following the conclusion of major combat operations

Crane and Terrill set out a matrix consisting of 135 essential tasks grouped into 21 mission categories arrayed across four phases of transition for Iraq: Security, Stabilize, Build Institutions, and Handover/Redeploy, the essence of which is summarized pp. 42-54.

An early 2003 report issued by the Army War College's Strategic Studies Institute, anticipating the Iraq post-conflict task, describes two visions of the timing of this transition from military primacy early in Phase IV leading to civilian primacy after Phase IV.²⁶



During this Phase IV transition period, the Army is engaged across substantive lines of effort including:

- Security and De-confliction (Demobilization, Disarmament, Reintegration and Reconciliation of soldiers; de-mining; training of police and conflict resolution)
- Limited, early infrastructure restoration (including economic development and public health) and other steps to help restore a sense of normalcy
- Early, political development activities (civil-military affairs, election planning, civic education)

Successful completion of Phase IV (i.e., building a secure, stable environment) is a prerequisite to the nation building by civilians. In other words: “*Security is the sine qua non of post-conflict reconstruction.* Though every case is different, there is one constant – if security needs are not met, both peace in a given country and the intervention intended

²⁶ Crane and Terrill p. 45.

to promote it are doomed to fail.”²⁷ A recent assessment of the Operation Iraqi Freedom concluded that the US, unfortunately, did not properly plan for the execution of the steps needed to make the transition from Phase III to Phase IV and then to civilian nation building: “[T]he need to see conflict termination and the **transition** to nation building as a critical military mission is one of the most important single lessons of the Iraq War.”²⁸

The Compelling Need for an Effective Army Plan for Phase IV Operations

A military campaign can only be successful if Phase IV is a success. Planning and execution for Phase IV must begin in Phase I. General Gordon Sullivan, former Army Chief of Staff and currently President of the AUSA, observed:

Civil Affairs is a vital part of our Army, and its soldiers bridge the dangerous gap between the end of war and the establishment of a stable foreign government capable of providing essential services. If we are to win the peace as decisively as we win the war, Civil Affairs must be a player **in the planning and execution of Army operations from beginning to end.**²⁹

This end-to-end planning is necessary for the Army to bridge the gap between the end of direct combat operations (and the subsequent inherent instability) and the stability necessary for meaningful reconstruction led by US civilian agencies, such as the Department of State and USAID. Getting this right is incredibly important; the consequences of getting it wrong can be monumentally tragic. The Panel notes that with proper planning, modeling and simulation at all levels (strategic, operational and tactical) the chances of success greatly improve.

Fundamentally, “[w]arfighting and peace operations require different skills and capabilities,”³⁰ yet the training, simulations, exercises and plans focus on the former and less on the latter. The Army has not, in the context of the total campaign plan, systematically included Phase IV operations and developed the planning and evaluation infrastructure necessary to determine what is needed and how those needs should be met.³¹ **Simply put, what is required is to apply to Phase IV the same planning rigor the Army has historically devoted to Phases I, II and III.**

²⁷ PLAY TO WIN, *Final Report of the bi-partisan Commission on Post-Conflict Reconstruction* (January 2003) p. 6.

²⁸ Anthony H. Cordesman, *The Lessons of the Iraq War: Main Report Tenth Working Prepublication Draft* (July 2, 2003) p. 312 (emphasis added).

²⁹ AUSA Land Warfare Paper #41, March 2003, p. v. (emphasis added).

³⁰ *Ibid* p. 440.

³¹ The Institute for Land Warfare report notes that “[p]rogress has been made to include Civil Affairs as part of the planning process up and down the ‘trace’ and building CA annexes into regional combatant commander operations plans and contingency plans.” (p. 23). But much more is required, including, but not limited to, a permanent liaison among (i) the technical experts in civilian agencies and contractors who support them, (ii) the warfighters and (iii) Civil Affairs forces.

This will require not merely examination of Phase IV needs, but a plan that spans all Phases of the campaign. Phase IV requirements and plans must be part of the planning in Phase I. Moreover, that integrated planning process must recognize that traditional Phase IV tasks will start to be executed in Phase I, as the battlefield is prepared not only for major combat, but also for the security and stabilization operations that will follow.

Moreover, the Phase I-III plans must be updated and reflected in the Phase IV planning process. The consequences of combat decisions on the Phase IV environment can and should be evaluated. For example, targeting decisions in the early phases should be made with a clear appreciation of the impact of the destruction on Phase IV operations. Key infrastructure (e.g., prisons and communications infrastructure), if destroyed, will need to be rebuilt, and the destruction will shape civilian attitudes. That does not mean that the target list should be altered – for if Phases I-III are not successful, Phase IV concerns are rendered moot. But it does mean that the choices made must be understood for their impact, so that Phase IV planning can be effective. The campaign is a continuum through Phase IV; the campaign does not cease with the end of Phase III.

This approach would be a fundamental shift that will result in changes both to the planning process and the concept of what is required to achieve post-conflict success. Eventually, this planning process should result in revisions to Army doctrine, policy, budgets, technology, education and training, simulations, and exercises so that the Army has a more effective capability to conduct Phase IV operations rapidly and with success, and speed the transition from military to civilian control/capacity.

Recommended Actions:

The G3, TRADOC, and the Army Component Commanders, should take appropriate steps to assure that campaign plans:

- Reflect the national security goals for Phase IV operations and provide the requisite capabilities, including a properly resourced Civil Affairs force structure.

- Are derived from the use of modeling, simulations and related tools that tie together all phases of the campaign operations (Phases I-IV).

The Broader National Security Question

The Nation is increasingly focused on the importance of “playing to win” post-conflict. The January 2003 report of the Commission on Post-Conflict Reconstruction, jointly headed by the Center for Strategic and International Studies (CSIS) and the Association of the US Army (AUSA), sets out a clear and persuasive case that the United States Government, under the direction of the President through the adoption of a new National Security Presidential Directive (NSPD) (now in draft), needs to develop a comprehensive and robust planning process in order to assure effective post-conflict reconstruction.³²

Indeed, the CSIS-AUSA Report specifically concluded that “a coherent international strategy based on internal and external parties’ interests is crucial.”³³ The Report recommends that “the current *ad hoc* USG strategy and planning process for addressing post-conflict reconstruction situations (needs to be replaced) with a standing comprehensive interagency process” at the strategic and operational levels.³⁴ Implicitly, this process would be run concurrently and collaboratively with national level planning for the combat phase. In the absence of such clarity, there will be continuing confusion over who has what responsibilities after major combat operations end.

Similarly, the Department of Defense, through the Office of Force Transformation has commissioned the National Defense University to develop a series of products designed to guide future DoD force structures to address the military’s role in post-conflict reconstruction planning and operations. This restructuring may evolve in many different ways, but it will also have substantial implications for the Army and its Civil Affairs forces.

There has been much rhetorical discussion concerning the role of the military and “nation building.”³⁵ This Report’s focus is on force protection and the security that evolves from the transition to civilian authorities. As the CSIS-AUSA Commission observed:

Although the military may play a crucial role when it comes to security needs in certain cases, a host of civilian actors has a comparative advantage in addressing many of post-conflict reconstruction’s wide range of needs. Non-governmental organizations, the private sector, international organizations, multilateral development banks, and civilian agencies of multiple donor governments all have a crucial role to play in addressing governance and participation, justice and

³² CSIS-AUSA Report p. 10.

³³ *Ibid* p. 6.

³⁴ *Ibid* p. 10.

³⁵ Illustrative is the National Security Advisor Condoleezza Rice’s observation: “‘There’s nothing wrong with nation building, but not when it’s done by the American military.’” *Ibid* p. 9 and n.6, quoting “Foundation for a Nation,” *Washington Post*, October 29, 2001, p. A17.

reconciliation, and economic and social needs. Some of these groups even have an important role to play on security issues.³⁶

In January 2003, the Strategic Studies Institute at the US Army War College examined post-conflict scenarios for Iraq and similarly concluded:

In Iraq it will ... be important to lessen military involvement as expeditiously as possible, so interagency planners must be sure that governmental, non-governmental, and international civilian organizations are ready to perform assigned tasks when required.³⁷

The Panel submits that now is the right time for the Army (as the Nation's land force involved with post-conflict operations) to participate, if not lead, a fundamental review of what it takes to win the peace: (i) how the strategic and operational level planning process should be done; (ii) how Army forces should be structured for Phase IV operations³⁸; (iii) how the DoD should be restructured to support Phase IV operations; and (iv) how the DoD should complement the USG's larger post-conflict commitments.

This review should result in a crucially important series of decisions for the Nation. Consideration should be given to elevating the review to be part of the Quadrennial Defense Review, which sets out four key goals for US forces. With respect to Phase IV operations, a fifth goal, which is set out in italics below, might be considered:

- Assuring allies and friends of the United States' steadiness of purpose and its capability to fulfill its security commitments;
- Dissuading adversaries from undertaking programs or operations that could threaten U.S. interests or those of our allies and friends;
- Deterring aggression and coercion by deploying forward the capacity to swiftly defeat attacks and impose severe penalties for aggression on an adversary's military capability and supporting infrastructure;
- Decisively defeating any adversary if deterrence fails
- *Supporting the restoration of the basic capacity of indigenous institutions to maintain the safe and secure environment necessary for reconstruction*

Recommended Action:

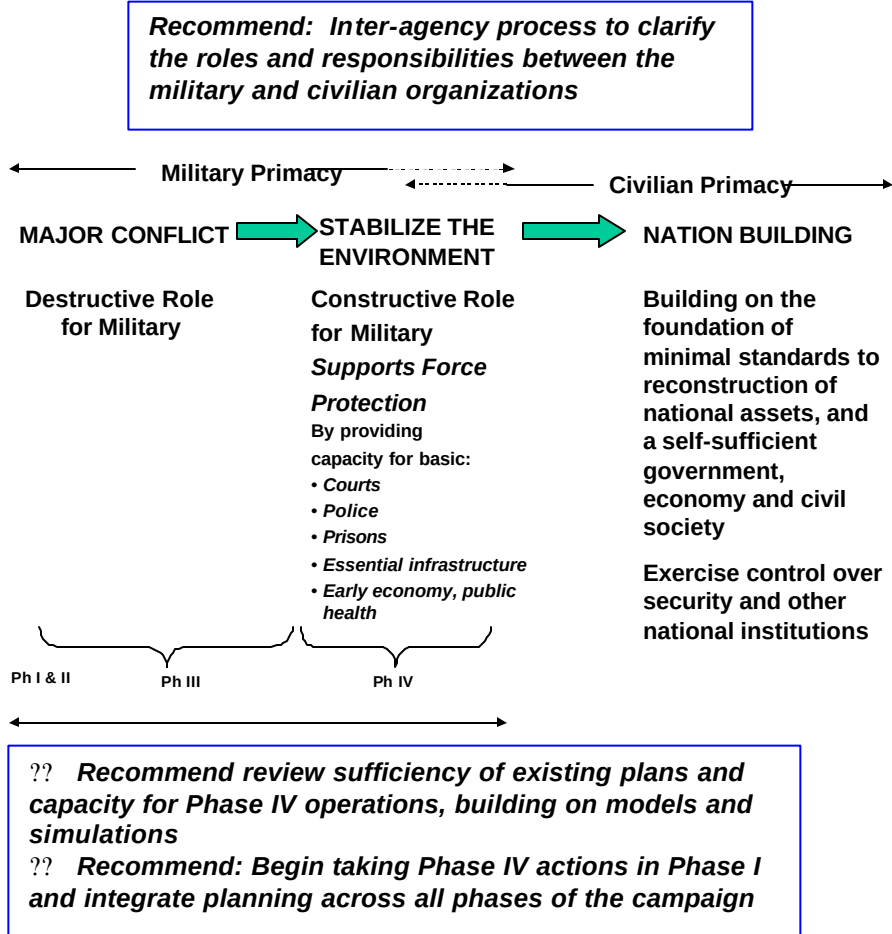
The Army and DoD should support efforts to replace the current, national level, *ad hoc* strategy and planning process for addressing Phase IV and reconstruction operations, to a standing comprehensive inter-agency process, in which the Army would have primary role, as recommended by the Commission on Post-Conflict Reconstruction.

³⁶ *Ibid* p. 9.

³⁷ Crane and Terrill, p. 17.

³⁸ This would building on the Army's planning as suggested in our recommendation on page 17, above.

Map of Key Recommendations For Phase IV Operations



IV. Contractors

The panel examined an additional force protection issue; one associated with the Army's reliance on contractors on the battlefield. Few operations proceed without contractor support. In considering force protection matters with the Army-contractor interface, the Panel identified three matters meriting attention:

- Whether the commander has an obligation to provide force protection to contractor personnel.
- The risk that contractor employees (especially indigenous employees) present to force protection.
- The problems arising from reliance on local interpreters.

Each of these matters is separately discussed.

Force Protection for Contractors

As a matter of background, the type of services provided by contractors to deployed forces is extremely broad.³⁹ Within a base camp, an indigenous work force is likely to provide services such as food preparation, laundry, waste management, water production, security guards, mail distribution, construction and facilities maintenance. Outside the base camp, an indigenous work force is likely to provide other services to include linguist support and road maintenance. Additionally, Phase IV operations are likely to be supported by US contractors and their employees who are not indigenous. Examples include skilled technical employees who perform weapon systems maintenance, C3I systems maintenance, and intelligence analysis. Other non-indigenous employees would probably include employees of the contractor that originally managed the construction of the base camp who remained to supervise improvements.

The number of contractor employees that support Phase IV operations typically is relatively high. For example, the General Accounting Office estimates that, in Bosnia, there are two support contractors for every deployed soldier.⁴⁰ Because various federal contracting activities award these contracts, the local commander usually does not have complete information on all of the support contractor employees within the vicinity. For example, there have been instances where the base camp commander had no advance notice of the arrival of contractor employees yet the contracting activity had obligated the base camp commander to support the contractor with real property facilities.⁴¹

³⁹ See, e.g., P.W. Singer, *Corporate Warriors: The Rise Of The Privatized Military Industry* (Cornell University Press 2003).

⁴⁰ GAO Report "Military Operations: Contractors Provide Vital Services To Deployed Forces But Are Not Adequately Addressed In DoD Plans" GAO-03-695 (June 2003) p. 8, n. 5.

⁴¹ *Ibid* p. 33.

The first of the matters listed above is whether the commander has an obligation to provide force protection to contractor personnel. Official guidance is less than a model of clarity:

- One source suggests there is no responsibility to provide protection unless expressly stated in the contract. Joint Publication 4-0, Chapter V, Section 13 (“Force protection responsibility for DoD contractor employees is a contractor responsibility, unless valid contract terms place that responsibility with another party.”)
- Another source suggests there is an obligation to provide protection but limits the obligation to “U.S. contract personnel.” AR 715-9, *Contractors Accompanying The Force* (“All U.S. Army-sponsored contractor employees in the Area of Operations shall be designated to a military unit to maintain administrative oversight and accountability. The Theater Support Command, the Logistics Support Element, or other official delegate ... is responsible for providing ... force protection for U.S. contractor personnel.”)
- Still another source states that the Army will provide protection to U.S. contractors “on a reimbursable basis.” FM 100-10-2, *Contracting Support On The Battlefield*. See appended ltr from Ass’t Sec. of Army dated Dec. 12, 1997 (“When U.S. contractors are deployed from their home stations, in support of Army operations/weapon systems, the Army will provide or make available, on a reimbursable basis, force protection”)
- Finally, one source states that the Army has a “moral responsibility” to provide protection to its support contractors. AMC-P 715-18 *Contractors and Contractors Supporting Military Operations*, Chapter 10 (“The Army has a moral responsibility, over and above specific contractual requirements to provide a secure working environment for contractor personnel.”)

Regardless of whether there is any contractual, legal, or moral responsibility to protect contractor employees, the bottom line is that if contractor employees perceive a significant threat to their safety and the threat has not been reasonably mitigated by the commander providing force protection, these individuals are likely to flee or procure their own protection. If they flee, it is doubtful if the unit will obtain the services set forth in the contract. The commander is likely to find it unacceptable to have armed protection forces under the control of contractors and not under the commander’s direct command. Therefore, as a practical matter, the commander has little choice but to provide force protection to contractor personnel.

Recommended Action: TRADOC should promulgate doctrine that the commander has responsibility to provide protection to contractor employees. The protection should be commensurate with the protection the commander would extend to DoD civilian personnel.

Force Protection Risks Posed By Local Workers

The second matter listed above involves the fact that an indigenous contractor employee who works at a base camp is well-situated to harm the force in a multitude of ways, such as contaminating food or water supplies. Another risk is that a contractor employee is gathering intelligence concerning US Forces and their activities. Typically, vetting of local workers is the responsibility of US contractors who employ them and not the Army. Generally, the Army has not provided oversight to assurance that contractors are performing adequate background checks on their employees.

Among the best ways to mitigate this risk is to (1) thoroughly screen contractor employees and (2) limit the access of indigenous contractor employees to vicinities in which their work is required. One useful force protection tool is to implement a theater-wide digitized database (including current photographs) of all contractor employees. For example, if an indigenous employee has gained access to several base camps, this could be an indicator that the employee is gathering intelligence.

Recommended Actions:

1. The contracts with prime contractors and their subcontractors should require the prime contractor to submit the contractor's operating procedure for performing background investigations on potential employees who will be given access to base camps. The operating plan must be approved by the Provost Marshal for the base camp. The Provost Marshal should also serve as the contracting officer's quality assurance representative to make periodic inspections to assure the vendor is complying with the operating procedure.
2. The Army should install an on-line database of all non-DoD civilians who are given access to base camps. All support contractor employees should be issued badges with photographs that contain bar code or other "swipe" technology that allows a record to be made when a contractor employee enters or exits the base camp. The Provost Marshal for each base camp should be given responsibility for establishing and maintaining the database.
3. The Army should perform a market survey of radio frequency identification (RFID) systems to monitor the location of indigenous employees within base camps. Upon selecting a qualified vendor, the Army should have a contractual instrument (such as a GSA schedule contract) available to acquire the necessary hardware and support to implement an RFID system with base camps.

Reliance on Local Interpreters

In terms of force protection, interpreter services is one of the most critical services that the Army requires. The accurate exchange of information with local officials and citizens is essential during Phase IV. As a norm, there is a lack of qualified interpreters.⁴²

In Bosnia, a recurring problem with interpreters was that frequently they injected their ethnic bias into the translation. Another common problem has been that the skill level among local interpreters varies significantly.

The Army has deployed Babylon systems to Afghanistan and Iraq. The Babylon system is a handheld device that soldiers can use for two-way, natural language speech translation. Currently, Babylon has limited dialog of a few hundred common phrases. Hence, Babylon lacks the capacity to be effective for the detailed conversations that Civil Affairs personnel should be having with local civic leaders. Although Babylon undoubtedly will continue to improve, for at least the next several years, it is likely the Army will still need the services of qualified interpreters.

In light of the frequent shortage of competent interpreters, one partial solution might be for soldiers to access interpreters through a radio or cell phone. The radio/cell phone could be passed back and forth between the soldier and the local citizen as the interpreter relates what had been previously spoken by the other party. This is not a new concept. The procedure has been used by some police departments in the United States with acceptable results.

More recently, commercial firms have implemented the service for business transactions. The market leader appears to be Language Line Services (LLS). LLS serviced over six million translation calls in 2002. LLS offers interpreter services in approximately 140 languages. Spanish is the most frequently requested language. LLS's service can be acquired almost instantaneously through the use of a credit card.

Dr. Jurgen Sottung, a program manager for the Defense Language Institute's Foreign Language Institute recently conducted an experiment with telephonic interpreter services. In conjunction with Exercise Vigilant Shield '03 in Oahu, Hawaii, a Vietnamese speaker with no proficiency in English served as a role player. The exercise took the form of a "walk-in" to the Military Counter Intelligence office. Neither the Vietnamese player nor the American counterpart had received any training on telephonic interpreting. The American soldier was provided with a cellular phone for contacting a Foreign Language Center (FLC) to obtain the services of an interpreter. In his report on the experiment, Dr. Sottung observed: "All participants seemed to be generally satisfied with the call-a-linguist capability provided by the FLC, citing it as easy to use and effective."⁴³

⁴² Crane and Terrill p. 17.

⁴³ Concern that interpreters injected their local bias into their interpreting was previously identified as a problem in Bosnia. There does not appear to be an ideal solution. It should be noted that the more removed the interpreter is from the controversy, the less likely the bias. Hence, bias is probably less likely to exist in

Recommendation

1. The Army Acquisition Executive should promulgate guidance to contracting officers suggesting means to implement better advanced planning and quality control in the procurement of interpreter services.
2. To the extent feasible, Defense Language Proficiency Tests (or other comparable tests) should be used to assess the verbal skill level of the interpreters who are hired by vendors to support the Army.
3. TRADOC, as the parent Command of DLI, should make an assessment whether the use of telephonic interpreting services is a viable means of meeting a significant portion of the Army's needs during Civil-Military operations.

Conclusion

This Report is part of a larger study of force protection. It is the Panel's firm conclusion that successful civil-military operations are essential to protecting the force and accomplishing the mission. This is especially true in Phase IV operations, like those now occurring in Iraq.

The Interface Panel began its work before Operation Iraqi Freedom commenced and concludes its work while US forces and its coalition partners still seek to establish the security that is a necessary predicate for the creation of an enduringly peaceful and stable Iraqi society. The Interface Panel submits that the US Army has a unique capability to marshal the resources required to provide the stability and security necessary for civilians (the US Government civilian agencies, NGOs and other organizations, and ultimately indigenous Iraqi authorities) to build that nation. It is the Panel's hope that it has made a contribution to the discussion of how best to plan and organize civil-military operations to produce that necessary security.

telephonic interpretation services. Hence, hypothetically, if a local commander in Bosnia suspected his local interpreter was injecting bias, he could "seek a second opinion" by using the services of London Language Line in the United Kingdom.

Interface Panel Membership

Alan Schwartz, Chair

Jerry Gabig

LTC Ferdinand Irizarry, Government Advisor

Dick Ladd

Interviews and Resources

The Panel reviewed a variety of studies, regulations, field manuals and other written material, and the Panel references this in the notes to the Report. In addition, the Panel interviewed (in person or by telephone) a number of individuals, identified below, who provided the Panel with additional perspective and insight.

1. Lt. Col. Michael Benjamin, USA, Chair, Contract & Fiscal Law Department, U.S. Army Judge Advocate General School
2. Mr. Charles Frechette, Joint Forces Command
3. LTC Ferdinand Irizarry, Director, Special Operations Proponency, USAJFKSWCS (AOJK-SP)
4. Colonel Frank Groud, USA, Deputy Chief, Operational Applications Division, Defense Threat Agency
5. Jerry McGinn, RAND
6. James McKnight, Kellogg Brown & Root
7. Dr. Elizabeth Stanley-Mitchell, Georgetown University (former Military Intelligence Officer in Macedonia and Bosnia)
8. Carl Peckinpough, General Counsel, DynCorp.
9. Mr. Ron Reichelderfer, Joint Forces Command
10. David Ricci, Director of Contracting, Defense Contract Management Agency
11. Daniel Serwer, Director Peace Operations and Balkans Initiative, US Institute for Peace
12. Dr. Jurgen Setting, Program Manager, Defense Language Institute
13. Major Gregg Sharp, USA, Professor, Contract & Fiscal Law Department, U.S. Army Judge Advocate General School
14. Colonel Michael Simone, USA, Commandant, Defense Language Institute
15. Peter W. Singer, John M. Olin Post-Doctoral Fellow, [Foreign Policy Studies](#), The Brookings Institution
16. Lt. General Jerry Sinn, USA, Assistant Secretary of the Army (FM)
17. Major Lynda Snyder, USA, Civil Affairs, Vicenza, Italy
18. Professor Tom Sweeney, Army War College
19. Colonel William Webb USA (Ret), Chief Operating Officer, Time Domain Corporation
20. Larry K. Wentz, Professor, George Mason University (former Brigade Commander in Bosnia)
21. Colonel Jeffrey Willey, USA, ASB Executive Secretary (former operational contracting team commander in Kosovo)

APPENDIX A

TERMS OF REFERENCE



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



09 DEC 2002

REPLY TO
ATTENTION OF

Dr. Joe Braddock
Chair, Army Science Board
2511 Jefferson Davis Highway, Suite 11500
Arlington, Virginia 22202

Dear Dr. Braddock:

I request the Army Science Board (ASB) conduct a study to examine "Force Protection Technologies for the 2010-2020 Timeframe." The study should address, but is not limited to, the Terms of Reference (TOR) described below. The ASB members and consultants appointed to this study should consider the TOR as guidelines and may expand the study to issues considered important to the study. Modifications to the TOR must be addressed with you.

Background: The increased likelihood of non-conventional threat action against U.S. Forces provides cause for focusing and improving Army capabilities for Force Protection, to include operations, intelligence, training, consequence management, related science, technology, and modernization. These apply to both Joint and Army capabilities based in and employed outside the United States. Therefore, advanced technologies for protection against non-conventional threats to our forces, bases, and their infrastructure in CONUS and OCONUS environments are required.

TOR:

a. Review prior force protection studies. Sources for these studies include Army, Department of Defense, other organizations that conduct national security studies, and, potentially, NATO allies and Israel. This review should be combined with a current assessment of threats and vulnerabilities and any useful projections. Form a threat/vulnerability continuum and net assessments of the current assessed threats versus current capabilities and assess intelligence requirements to support the force protection mission against non-conventional threats.

b. The study should address potential force protection issues during and after OCONUS deployment. Force protection shall include deterrence, defense and consequence management. Consider mission and operational scenarios to include: Peacekeeping, peace enforcement, humanitarian missions, support to tactical operations, and other similar missions in which the Army may engage into the foreseeable future. Special consideration should be given to the challenges of force protection in an urban environment. The study should treat



the above in the context of needed joint capabilities, operations, and training for the Total Army.

c. The study should address advanced technologies for the 2010-2020 timeframe to support the various previously defined force protection missions. This should be contrasted with a baseline of available and near-term technology. Among the topics to be addressed should be: Command, Control, and Information; Robotics and Automation; Sensors; Physical Protection Systems; and Lethal/Non-lethal Systems.

d. Use analysis and models to evaluate potential contributions of force protection technologies in specific operational contexts where appropriate. Investigate necessary simulation and modeling capabilities needed to support analysis of force protection options. Use these and other models to assess the impact of force protection technologies on the total cost of force protection, with respect to potential reductions in manpower requirements, versus current manpower-intensive methods.

e. Address problems and opportunities associated with international operations, including commercial, governmental and non-governmental, and infrastructure environments in which the Army must operate and accomplish force protection.

Study Sponsorship: I will be the primary sponsor. I recommend you contact the following organizations and request their additional sponsorship: The United States Army Training and Doctrine Command, the United States Army Materiel Command, Office of the Chief of Army Reserves, Director, Army National Guard, the Army G-2, the Army G-3, and the Army G-4.

Study Duration: Please initiate the study in December 2002, provide interim progress reports in February and May 2003, and report out during July 2003.

Sincerely,


Claude M. Bolton, Jr.

Assistant Secretary of the Army
(Acquisition, Logistics and Technology)

APPENDIX B

PARTICIPANTS LIST

PARTICIPANTS LIST

**ARMY SCIENCE BOARD
2003 SUMMER STUDY**

Force Protection Technologies for the 2010-2020 Timeframe

Study Co-Chairs

Dr. Marygail K. Brauner
RAND

Mr. Gilbert V. Herrera
Sandia National Laboratories

Mr. Frank Kendall
Private Consultant

Senior Study Staff Assistant
LTC Alvin Klee
The Objective Force Task Force

ASB Panel Members

The Review of Prior Studies Panel

Panel Chair
Dr. Roberta-diane J. Perna
MezzoGiorno Consulting

Dr. Lynn Gref
Jet Propulsion Laboratory

Mr. John Reese
Private Consultant

The Vulnerability and Threat Assessment / Intel Requirements Panel

Panel Chair
Dr. Anthony K. Hyder
University of Notre Dame

Mr. Milt Finger
Lawrence Livermore National Laboratory

Dr. Roberta-diane J. Perna
MezzoGiorno Consulting

Dr. Elizabeth Stanley-Mitchell
Georgetown University

Dr. Michael D. Krause
Orion International Technologies

Staff Assistant
LTC John Fitzpatrick
MI, USAR

The Operations Panel

Panel Chair

GEN David M. Maddox (USA, Ret.)
DMM Consulting

Dr. Seth Bonder

The Bonder Group

Mr. Herb Gallagher

Computer Sciences Corporation

VADM William J. Hancock (USN, Ret.)

Hancock Associates, Inc.

LTG Charles P. Otstott (USA, Ret.)

Private Consultant

LTG Randall Rigby (USA, Ret.)

Private Consultant

Staff Assistant

Ms. Cheryl Ward

Office of the Deputy Chief of Staff G-3

The Technology Solutions Panel

Panel Co-Chair

Dr. Peter Swan

Southwest Analytic Network

Panel Co-Chair

Dr. Edward C. Brady

Strategic Perspectives, Inc.

Mr. Gary Glaser

LDCL, L.L.C.

Dr. Mark A. Hofmann

COLMAR-L.L.C.

Dr. Don Kelly

AdvanTECH Partners

Dr. Ira Kohlberg

Kohlberg Associates, Inc.

Dr. Steven E. Kornguth

Institute for Advanced Technology

Dr. Peter Lee

Carnegie Mellon University

Ms. Ginger Lew

Telecommunications Development Fund

Dr. Richard Montgomery

Private Consultant

Dr. Prasanna Mulgaonkar

Intel Corporation

Mr. John Reese

Private Consultant

Technology Solutions Panel – Government Advisors

Dr. Reed L. Mosher

Geotechnical and Structures Laboratory

Mr. Mike Toscano

Office of the Under Secretary of Defense for
Acquisition, Technology and Logistics

Dr. Jack Wade

White Sands Missile Range

Mr. Randy Woodson

Office of the Deputy Chief of Staff G-2

Dr. Al Grum

Army Research Laboratory

Mr. Paul Tilson

National Reconnaissance Office

Mr. Thomas Pagán

U.S. Army Space and Missile Defense
Command

Staff Assistant

Mr. Jim Wisniewski

Office of the Assistant Secretary of the Army for
Acquisition, Logistics and Technology

The Analysis and Modeling Panel

Panel Chair

Dr. Stuart H. Starr

The MITRE Corporation

Dr. Ira Kohlberg

Kohlberg Associates, Inc.

Analysis and Modeling Panel Government Advisors

Dr. Michael Macedonia

Program Executive Office for Simulation,
Training and Instrumentation

MAJ Theodore Dugone

U.S. Army Modeling & Simulation Office

Corporate Advisor

Ms. Sarah K. Johnson

The MITRE Corporation

Corporate Advisor

Mr. Dan Rondeau

Sandia National Laboratories

The Interfaces with Local Governments, Commerce and Infrastructure Panel

Panel Chair

Mr. Alan R. Schwartz

PolicyFutures LLC

Mr. Jerome S. Gabig

Q-Track Corporation

Mr. Richard Ladd

Robison International, Inc.

Government Advisor

LTC Ferdinand Irizarry

Special Operations Proponency Office

Cadet Support

CDT Heather Ritchey
U.S. Military Academy at West Point

CDT Adam Tritsch
University of Kansas

Study Sponsors

GEN Paul J. Kern
CG, U.S. Army Materiel Command

GEN Kevin P. Byrnes
CG, U.S. Army Training and Doctrine
Command

LTG Robert Noonan
Deputy Chief of Staff G-2

LTG Charles S. Mahan Jr.
Deputy Chief of Staff G-4

LTG Roger Schultz
Director, Army National Guard

LTG Richard Helmly
Chief of the Army Reserve

LTG Richard Cody
Deputy Chief of Staff G-3

Red Team

Red Team Chair

Dr. Michael Wartell
Indiana University – Purdue University at Fort
Wayne

Dr. Amy Alving
DARPA

Mr. John W. McDonald
SAIC

Dr. Joan Woodard
Sandia National Laboratories

APPENDIX C

ACRONYMS

ACR	Advanced Concepts & Requirements
ACTD	Advanced Concept Technology Demonstration
ADIDSS	Advanced DARPA Integrated Decision Support System
AEW	Airborne Early Warning
AFB	Air Force Base
AFCCC	Air Force Combat Climatology Center
AJCN	Adaptive Joint C4ISR Node
AMC	Army Material Command
AMSO	Army Modeling and Simulation Office
AOR	Area of Responsibility
APC	Armored Personnel Carrier
ARL	Army Research Laboratory
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics, & Technology
ASAP	As soon as possible
ASB	Army Science Board
ASEO	Army Systems Engineering Office
ATD	Advanced Technology Demonstration
ATEC	Army Test and Evaluation Command
B	Biological
BBN	U.S. commercial firm, maker of a counter-sniper system
BW	Biological Warfare
C	Chemical
C/B	Chemical/Biological
C2	Command and Control
C2OTM	Command and Control on the Move
C4ISR	Command, Control, Communications, Computers, Information, Surveillance and Reconnaissance
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CC&D	Cover, Concealment, and Deception
CDR	Commander; Combat Decision Range; Critical Design Review
CECOM	Communications-Electronics Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center
CGF	Computer Generated Force
CHESSS	Counterintelligence and Human Intelligence Exercise Scripting Support System
CI	Counterintelligence
CIA	Central Intelligence Agency
CMO	Civil-Military Operations
COAs	Courses of Action
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operational Picture

COTS	Commercial-off-the-Shelf
CS/CSS	Combat Support / Combat Service Support
CSA	Chief of Staff, Army
CW	Chemical Warfare
DA	Department of the Army
DAMO (AC, TR, ZS)	Department of the Army Military Operations organizations
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DMP	Decision Making Processes
DMSP	Defense Meteorological Satellite Program
DoD	Department of Defense
DOE	Department of Energy
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities
DROZD/ARENA	Russian Active Protection System
DRS	Decision Related Structures
DSS	Decision Support System
DTRA	Defense Threat Reduction Agency
DUSA-OR	Deputy Under Secretary of the Army for Operations Research
E&T	Education and Training
ECBC	Edgewood Chemical Biological Center
EO	Electro-Optical
EO/IR	Electro-Optic / InfraRed
ERDC	Engineering Research and Development Center
ESRI	GIS and Mapping Software Company
EW	Electronic Warfare
FACT	Focus Area Collaborative Team
FARP	Forward Arming and Refueling Point
FCS	Future Combat System(s)
FFRDC	Federally Funded Research & Development Center
FLIR	Forward Looking Infrared
FOB	Forward Operating Base
FOCUS	Freespace Optical / Near-Optical Communications System
FP	Force Protection
FPAT	Force Protection Assistance Team (U.S. Army)
FPB	Force Protection Battlelab
FPCONs	Force Protection Conditions
FPED	Force Protection Equipment Demonstration
FW	Fixed Wing
G-3	Deputy Chief of Staff for Operations
GIG	Global Information Grid
GIS	Geographic Information Systems
GOTS	Government-off-the-Shelf

GPR	Ground Penetrating Radar
GPS	Global Positioning System
GPUs	Graphic Processing Units
HAMER	Hazard Assessment and Mission Enhancement of Resources
HE	High Explosive
HLS ACTD	Homeland Security Advanced Concept Technology Demonstrations
HPAC	Hazard Prediction and Assessment Capability
HUMINT	Human Intelligence
HVT	High Value Target
HX	High Explosive
IBDSS	Integrated Base Defense Security System
ICT	Integrated Concept Team; Institute for Creative Technologies
IED	Improvised Explosive Device
IFFN	Identification Friend, Foe, or Neutral
IMMARSAT	International Maritime Satellite
INSCOM	Intelligence and Security Command
IPB	Intelligence Preparation of the Battlefield
IR	Infrared
IRT	Independent Review Team
IT	Information Technology
IW	Information Warfare
JANUS	an interactive, event-driven wargaming simulation
JCATS	Joint Conflict and Tactical Simulation
JCS J-3	Joint Chiefs of Staff Operations Directorate
JCS JAT	Joint Chiefs of Staff Joint Anti-Terrorism
JEM	Joint Effects Model
JFCOM	Joint Forces Command
JIC	Joint Intelligence Center
JIVA	Joint Intelligence Vertical Architecture
JLENS	Joint Land Attack Cruise Missile Defense Elevated Netted Sensor
JPEO-CBD	Joint Program Executive Office – Chemical and Biological Defense
JPO	Joint Program Office
JRTC	Joint Readiness Training Center
JSAF	Joint Semi-Automated Forces
JSOC	Joint Special Operations Command
JTRS	Joint Tactical Radio System
JVB	Joint Virtual Battlespace
l/w	Lumens/watt
LCT-50	The level at which 50% of the exposed population will be affected
LED	Light Emitting Diode
LIDAR	Laser Radar / Light Detection and Ranging
LoJack	Car anti-hijack system
LOS	Line of Sight
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LTA	Lighter Than Air

M&S	Modeling and Simulation
MANA	Name of an agent based model
MANPADS	Man-Portable Air Defense System
MATREX	Modeling Architecture for Technology and Research Experimentation
MCTL	Military Critical Technologies List
MDARS(E)	ARL Robot
MG	Machine Gun
MISIC	Missile and Space Intelligence Center
MOB	Main Operating Base
MOPP	Mission Oriented Protective Posture
MOSAIC	Multi-Functional On-The-Move (OTM) Secure Adaptive Integrated Communications
MOUT	Military Operations in Urban Terrain
MPARS	Mission Planning and Rehearsal System
NAIC	National Air Intelligence Center
NCISA	Network Centric Integrated Systems Approach
NDI	Non-Developmental Items
NGIC	National Ground Intelligence Center
NIH	National Institutes of Health
NLOS	Non-Line-of-Sight
NLW	Nonlethal Weapons
NOAA	National Oceanic and Atmospheric Administration
NRC	National Research Council
NVGs	Night Vision Goggles
NVL	Night Vision Laboratory
OACSIM	Office of the Assistant Chief of Staff for Installation Management
OCONUS	Outside the Continental United States
OFTF	Objective Force Task Force
One SAF	One Semi-Automated Forces
ONR	Office of Naval Research
OSD	Office of the Secretary of Defense
PALM	Portfolio Analysis Machine
PD-PFA	Probability of Detection-Probability of False Alarm
PEO	Program Executive Office (/Officer)
PEO IEWSS	Program Executive Office Intelligence, Electronic Warfare and Surveillance
PILAR	French anti-sniper system
PM-PSE	Program Manager – Physical Security Equipment
POAM	Plan of Action and Milestones
POL	Petroleum, Oil, and Lubricants
PSEAG	Physical Security Equipment Action Group
R&D	Research and Development
RAW	Rapid Analytical Wargaming
RDA	Research, Development & Acquisition
RDE	Research, Development & Engineering

RDECOM	Research, Development and Engineering Command
RF	Radio Frequency
RPG	Rocket Propelled Grenade
S&T	Science and Technology
SA	Situational Awareness
SA/SU	Situational Awareness / Situational Understanding
SASO	Security and Stability Operations
SATCOM	Satellite Communications
SENSE	Synthetic Environments for National Security Estimates (a model developed by IDA)
SMART	Simulation and Modeling for Acquisition, Requirements, and Training
SOFPARS	Special Operations Forces Planning and Rehearsal System
SOSI	System of Systems Integration
SOSIL	System of Systems Integration Laboratory
SPAWAR	Space and Naval Warfare System Command
STRI	Simulation, Training, and Instrumentation
SUO	Small Unit Operations
TD	Technology Development
TDA	Table of Distribution & Allowance(s)
TEMO	Training, Exercises & Military Operations
TETRA	TErrestrial TRunked RADio – Public mobile radio technology
TLAC	Think Like a Commander
TOE	Table of Organization & Equipment
TOR	Terms of Reference
TRAC	TRADOC Analysis Center
TRADOC	Training and Doctrine Command
TSWG	Technical Support Working Group
TSWG	Training and Simulation Working Group
TTPs	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicle
UGS	Unattended Ground sensors
UGV	Unmanned Ground Vehicle
USANVL	U.S. Army Night Vision Laboratories
USNRL	U.S. Naval Research Laboratory
UT	University of Texas (in this context)
UXO	Unexploded Ordnance
VERTS	Virtual Emergency Response System
VIDE	Vehicular Improvised Explosive Device
WAE	Wargaming the Asymmetric Environment – a DARPA program
WMD	Weapons of Mass Destruction

APPENDIX D

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
Administrative Assistant to the Secretary of the Army, Pentagon, Room 3E733, Washington, DC 20310-0105	1
General Counsel, OSA, Pentagon, Room 2E722, Washington, DC 20310-0104	1
Assistant Secretary of the Army (Civil Works), Pentagon, Room 2E570, Washington, DC 20310-0108	1
Assistant Secretary of the Army (Financial Management and Comptroller), Pentagon, Room 3E606, Washington, DC 20310-0109	1
Assistant Secretary of the Army (Installations and Environment), Pentagon, Room 2E614, Washington, DC 20310-0110	1
Assistant Secretary of the Army (Manpower and Reserve Affairs), Pentagon, Room 2E594, Washington, DC 20310-0111	1
Assistant Secretary of the Army (Acquisition, Logistics and Technology), Pentagon, Room 2E672, Washington, DC 20310-0103	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
Inspector General, Pentagon, Room 1E736, Washington, DC 20310-1700	1
Chief of Legislative Liaison, Pentagon, Room 2C631, Washington, DC 20310-1600	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
Assistant Vice Chief of Staff, 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
The Surgeon General, HQDA, Skyline Place Building No. 5, Falls Church, VA 22041-3258	1
Chief, National Guard Bureau, Pentagon, Room 2E394, Washington, DC 20310-2500	1
Chief, Army Reserve, Pentagon, Room 3E390, Washington, DC 20310-2400	1
Chief, U.S. Army Center of Military History, 103 Third Avenue, Ft. McNair, DC 20319-5058	1

Addressee	Copies
Chief of Engineers, HQDA, Pulaski Building, 20 Massachusetts Ave., NW, Washington, DC 20314-1000	1
Commander, U.S. Army Corps of Engineers, HQDA, Pulaski Building, 20 Massachusetts Ave., NW, Washington, DC 20314-1000	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
Commander, US Army Test and Evaluation Command (USATEC), 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
Deputy Commander for Space, U.S. Army Space Command, 1670 N. Newport Rd., Colorado Springs, CO 80916-2749	1
U.S. Army Space Command Forward, ATTN: MOSC-ZC, 1670 N. Newport Rd., Suite 211, Colorado Springs, CO 80916	1
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
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 Industrial Operations Command, ATTN: IOC-AMSIO-CG, Rock Island, IL 61299-6000	1
Commander, U.S. Army Aviation and Missile Command, ATTN: AMSMI-CG, Redstone Arsenal, AL 35898	2
Commander, U.S. Army Security Assistance Command, ATTN: AMSAC, Alexandria, VA 22333-0001	1
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

Addressee	Copies
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 Edgewood Research, Development and Engineering Center, ATTN: SCBRD-TD, Aberdeen Proving Ground, MD 21010-5423	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 Test, Measurement, and Diagnostic Equipment Activity, ATTN: AMXTM, Redstone Arsenal, AL 35898-5400	1
Commander, USAWSMR Electronic Proving Ground, ATTN: Intelligence Office, Ft. Huachuca, AZ 85613-7110	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/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 Engineer Center and Ft. Leonard Wood/Commandant, U.S. Army Engineer School, Ft. Leonard Wood, MO 65473-5000	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 Chemical and Military Police Centers and Ft. McClellan/Commandant, U.S. Army Military Police School, Ft. McClellan, AL 36205-5000	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

Addressee	Copies
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
Director, Space and Missile Defense Battle Lab, P.O. Box 1500, Huntsville, AL 35807-3801	
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
Program Executive Officer, Joint Program Office for Biological Defense, 5201 Leesburg Pike, Suite 1200, Skyline #3, Falls Church, VA 22041-3203	1
Program Manager, Comanche Program Office, Bldg. 5681, Redstone Arsenal, AL 35898	1
Program Manager for Chemical DeMilitarization, ATTN: SFAE-CD-Z, Aberdeen Proving Ground, MD 21010-5401	1
Superintendent, U.S. Army Military Academy, West Point, NY 10996	1
<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

Addressee	Copies
<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
Under Secretary of Defense for Policy, Pentagon, Room 4E808, Washington, DC 20301	1
Under Secretary of Defense (Comptroller/Chief Financial Officer), Pentagon, Room 3E822, Washington, DC 20301	1
Assistant Secretary of Defense (Command, Control, Communications and Intelligence), Pentagon, Room 3E172, Washington, DC 20301	1
Assistant Secretary of Defense for Economic Security, Pentagon, Room 3E808, 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 Acquisition Reform, Pentagon, Room 3E1034, 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, Operational Test and Evaluation, Pentagon, Room 3E318, Washington, DC 20301-1700	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, Ballistic Missile Defense Organization, Pentagon, Room 1E1081, Washington, DC 20301-7100	1
Director, Defense Information Systems Agency, 701 S. Courthouse Rd., Arlington, VA 22204-2199	1
Director, Defense Intelligence Agency, Pentagon, Room 3E258, Washington, DC 20301-7400	1
Director, Defense Intelligence Agency Missile and Space Intelligence Center, Building 4505, Redstone Arsenal, AL 35898-5500	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
Director, Defense Threat Reduction Agency, 6801 Telegraph Rd., Alexandria, VA 22310-3398	1
Director, Defense Threat Reduction Agency, 45045 Aviation Dr., Dulles, VA 20166-7517	1
Director, Defense Security Assistance Agency, 1111 Jefferson Davis Highway, Suite 303, Arlington, VA 22202	1
Director, National Security Agency, 9800 Savage Rd., Ft. Meade, MD 20755	1
Director, On-Site Inspection Agency, 201 W. Service Rd., Dulles International Airport, P.O. Box 17498, Washington, DC 20041-0498	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

Addressee**Copies****OTHER**

Defense Technical Information Center, ATTN: DTIC-OCP, 8725 John J. Kingman Rd., Suite 0944, Ft. Belvoir, VA 22060-6218	1
Director, Central Intelligence Agency, Washington, DC 20505	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
Library of Congress, Anglo-American Acq., Room LM-B42, Government Documents Section, Federal Advisory Committee Desk, Attn: Richard Yarnall, 101 Independence Avenue SE, Washington D.C. 20540	8

