Smart sensor networks and information management for the Future Combat Systems (FCS)

Louis C. Marquet, James A. Ratches, John Niemela
Communications-Electronics Command
Research, Development & Engineering Center
Fort Monmouth, NJ

ABSTRACT

The vanguard US Army Science & Technology program for the transformation to a medium weight force is the Future Combat Systems (FCS). Critical to the effectiveness of this force is overarching knowledge of the distribution and intent of all the forces on the battlefield. Smart sensor networks and information management are key enablers for the FCS system of systems strategic goals. The role of sensors and information management in enabling FCS victory is described as well as the network centric warfare that will be the cornerstone of the battlefield in the near future. The US Army Communication-Electronics Command's development of sensors and information management assets is also reviewed as they influence the envisioned FCS.

1. FUTURE COMBAT SYSTEMS

Under the direction of the Chief of Staff, the US Army is undertaking a major transformation. This transformation is from a heavy weapons platform orientation to a lighter, much more deployable force that can react quickly to any military contingency any where in the world. This lighter force must at the same time be survivable, lethal, responsive, agile, versatile and sustainable. The ultimate envisioned force is the called the Objective Force. A three axes transformation process is in place by the Army to transform itself to this Objective Force. These axes are (1) the modernization of the existing force components, (2) the standing up of an interim medium force and (3) Science & Technology thrust to enable the full capabilities of the final Objective Force. The vanguard of the S&T effort is a ground combat force structure called the Future Combat Systems (FCS). The S&T efforts focused on FCS and the Objective Force will enable initial sensor and information warfare concepts previously discussed for the Army After Next[1]

Integrated smart sensor networks strongly influence the FCS concept. Sensors are crucial to the survivability of a medium weight force as high quality situation awareness is the key to avoiding unintentional close combat and supports beyond line of sight targeting. The combination of distributed sensors and the network to interconnect them is a prime contributor to situation awareness. Lethality of a medium weight force is also dependent on sensors enabling indirect fire for precision targeting beyond line of sight ranges as well as providing accurate combat identification at extended ranges. The mobility of the Objective Force is influenced by sensors which provide total battlespace awareness that avoids encounters with a heavy force and gives detailed local situation awareness for specific maneuvers.

Information management is critical to FCS by providing agility, versatility and sustainability for FCS as part of the Objective Force. Agility is provided the commander by knowledge and responsive decision aids which are key to dominant maneuver and can provide him with a knowledge base that presents viable alternatives for decisive action while on the move. Rapidly configurable command and control for a force structure to operate on any point of the operational spectrum is another information management feature that provides force versatility. Sustainability of the Objective Force is enabled by information management through permitting a small logistics footprint and replenishment demand based on comprehensive understanding of requirements and available assets. The integration of the entire process of deployment, reach back and maintenance for precision logistics will contribute significantly to the sustainment of the Objective Force.

The FCS is a system of systems (SoS) that can perform any mission required of today's Army. It must by able to handle high intensity conflicts, low intensity, police actions and peacekeeping. FCS is composed of individual soldier platforms, combat vehicles, aviation, weapons, sensors and communication networks. The trade off between the individual system and the SoS is a critical design consideration for FCS. The optimal total integration of intelligence, surveillance, reconnaissance, command, control, close combat, combat services support, air defense, medical and logistics assets at the force level will yield sub-optimal designs for some of the components. However, the key to victory by FCS will be generation of combat

Battlespace Digitization and Network-Centric Warfare, Raja Suresh, Editor,
Proceedings of SPIE Vol. 4396 (2001) © 2001 SPIE · 0277-786X/01/$15.00

knowledge from ubiquitous sensors and information management. The sensors will enable an "unblinking eye"[2] over the entire battlefield and the information management system will send the right information to the commander or individual soldier who needs it in the optimal format.

2. INFORMATION SUPERIORITY

The key to battlefield success for the FCS force will be information superiority. Sensors and information management can provide the means to achieve synchronized battlespace operations and control through establishment of information superiority. Information superiority will be the path to overarching combat power that will enable the FCS to be deployable, versatile, lethal, agile, sustainable, survivable, and responsive. This is such an important concept that one could say that information superiority was a strategic objective for FCS and will determine the outcome of the battle. The need for information superiority will be pervasive and critically important to every soldier, commander and platform.

The potential threats to the US Army will also realize the need for information dominance on the battlefield. Consequently, information network centric warfare will become a major factor in combat operations. The FCS force will be connected together with an information network that integrates sensor information, stored data bases (e.g. terrain maps), direct and indirect fire weapons, and all-pervasive communications. The network must be secure from threat intrusion and capable of degrading gracefully from attrition of assets. It is important to understand that the network centric warfare that will be fought on the next battlefield will be at the information level. Information is just one step in the sensor/information cognitive hierarchy. Sensor data and data bases, such as digital terrain maps and threat tactical doctrine, are intelligently processed to generate information. Information must be oriented and analyzed through the commander's cognitive powers to form knowledge. Knowledge of the complete battlefield situation can be used to make decisions and plan by the exercise of command judgment. Through judgment based on knowledge and understanding of the battlespace is realized and action taken, such as executing the battle plan, seizing the initiative or exploiting a success. The ultimate goal of this hierarchical process is battlefield wisdom. Figure 1 is a graphical representation of this concept.

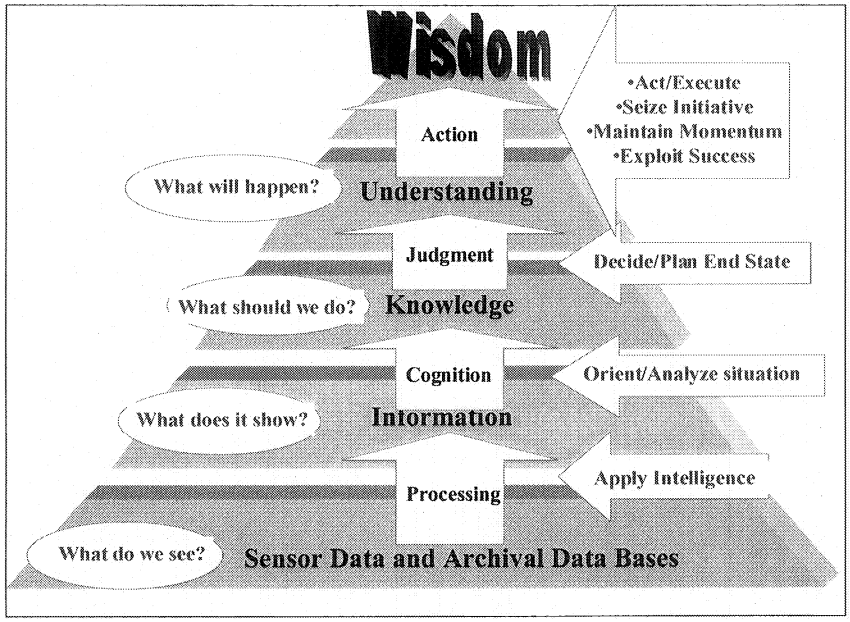

Figure 1. Sensor/information cognitive hierarchy

The principal challenge of the next battlefield is to digest and process the relevant sensor data and information to generate knowledge and deliver the necessary understanding to the battlefield decision maker in a timely and comprehensible fashion so as to enable truly informed decisions. To paraphrase Baumard[3], the sensing data is only 20% of understanding the battlefield, the other 80% is how the data and information are reduced to knowledge. Integral to this concept is the communications infrastructure which is a subject of its own but not of this paper.

3. SENSOR & INFORMATION MANAGEMENT GOALS

3.1 Networked sensor goals

The battlefield goals for networked smart sensors are complete situation awareness and timely beyond line of sight targeting. This objective is referred to as layer surveillance and is shown in Figure 2. The problem for sensors is to find targets in complex terrain and avoid ambush or encountering a heavy force. The FCS force will not be capable of defeating a heavy force in a close combat. Threat forces will have to be detected beyond line of sight and killed with indirect fires. Consequently, the networked array of sensors is layered. The outer layer is global surveillance and contains satellite sensors, JSTARS, Global Hawk and Predator unmanned air vehicles (UAVs). This layer receives tasking from national command, theater, corps and division. The next layer contains brigade sensor assets, such as the Tactical UAV, Comanche and possibly another larger UAV potentially under development by DARPA.

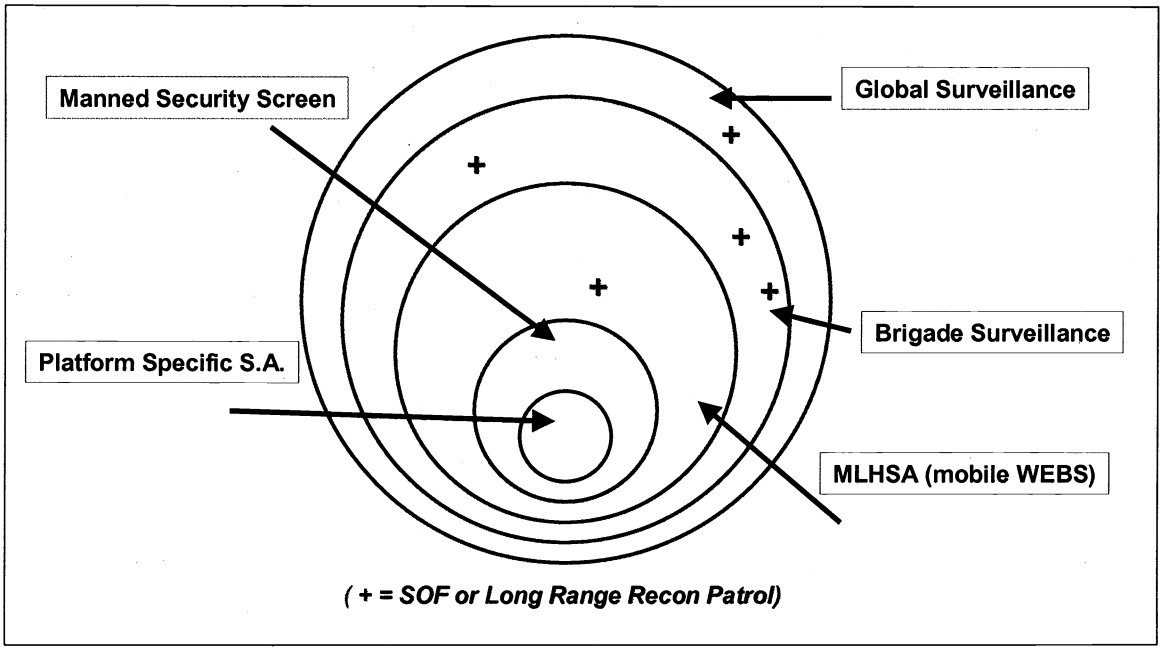

Figure 2. Layered sensor network corresponding to regions on the battlefield.

Whereas the first two layers of the sensor network are assigned to beyond line of sight, the remaining layers are closer in to the FCS force. The Mobile Local Hostile Situation Awareness (MLHSA) sensors cover the area directly in front and on the flanks of the force. The sensors in MLHSA are mini-UAVs, unmanned ground vehicles and unattended ground sensors (UGS). The UGS may be hand implanted, aerial dropped or artillery emplaced. As the sensor network gets closer to the force, man-in-the-loop sensors will be required to detect any threat that may have slipped through the outer layers undetected. The final layer is the platform specific set of sensors, such as Second Generation FLIRs and Multifunction Staring Sensor Suites on the combat vehicles and head tracked sensors for close combat indicative of urban terrain.

The biggest challenge for the FCS task force in offensive operations is to detect targets in deep hide in complex terrain. The solution to this challenge is a combination of a network of unmanned sensors, sensor platforms that give multiple looks both high and low, and continuous tracking with cross cueing. Once detection of the threat has been made, there must be instantaneous retaliation as deterrence.

An FCS force without heavy armor must place new emphasis on integrated protection from threat sensors. Each of the onion layers in Figure 2 has a corresponding countermeasure concept to prevent detection by the opposing force. In the outermost layer, terrain masking provides protection. When it is necessary to expose a friendly vehicle, the next layer of sensor protection is signature reduction. Inside this layer, threat warning sensors and smoke provide platform masking. In the next to last layer, countermeasure decoys and jammers are required. Finally, the last layer involves active protection from threat rounds. This protection concept in layers may be somewhat simplistic. The variety of the possible threats and the challenge of the fast long rod penetrator emphasize the need for networked protection. The combat vehicle protection suite should adopt the aviation paradigm for platform protection, but at a reduced cost in order to be affordable for the entire FCS force.

Army Science Board statements attest that sensors and situation awareness are critical to FCS:

Tactical and engagement level situation awareness, and extended range tactical engagement (including beyond line of sight), have the highest payoff of any protection option"[4]

Both on-board and off-board sensors are important to the FCS concept of operations. The necessity to deal with threat targets in a complex terrain implies a mix of both types of sensors. Affordability will be the critical parameter in making the mix and basis of issue decisions.

3.2 Information management/superiority goals

The primary objective of information management and information superiority is victory in an information network centric warfare. A robust information infrastructure capable of sustaining the battlefield commander's requirements offensively and defensively is achieved by networking sensors, command and control, and weapons. The integration of these networks into a common architecture is supported by a distributed, robust, mobile communications network. The communication network supplies the interconnectivity among the inputs and needs of the other networks. The primary advantage of the integrated network structure is timely, accurate, unprecedented information that provides shared situational awareness, increased speed of command, higher operation tempo, greater lethality, increased survivability, and synchronized weapon allocation.

Utilizing the wealth of data gathered by the sensor component, great improvements in the decision making process are possible using advanced algorithmic and computational capabilities. Intelligent software agent technology will soon transform data, via the context of the situation, to information. The commander then transforms this information to knowledge and understanding on which a decision is formed. Prime examples include the tactical planning process and course-of-action (COA) generation coupled with "what if" analysis. Such tools will assess and generate plans that consider terrain, weather, structures, line-of-sight (multispectral), mobility and visibility mapping, red/blue sensor coverage, and route planning. These tools will be extended to the development of very fast parallel COA tools that would be available to commanders and staff via reachback facilities to minimize the logistics footprint. Such a capability will considerably enhance the responsiveness and agility of the Objective Force.

The information management network must also be provided with protection from cyber-attack, just as in the case of the networked sensors. Attacks can take many forms, including malicious software (viruses and Trojan Horses), denial of service, message flooding, message and identity compromise, malicious insider and overrun/capture. The network must be able to predict and detect attacks from a wide variety of threats. Required features are host & network intrusion detection, malicious code detection, anomalous behavior detection and prediction via neural network techniques. Protection approaches include secure configuration by shutting off non-essential services (email/web) and issuing file privileges. Also, user identification & authentication with passwords/biometrics, message authentication and host software protection will be achieved. In network centric warfare, the information network must be capable of reacting to attacks. Reaction techniques include tightening access control, identifying attack source and skill level, re-routing traffic, eliminating attack process, damaging assessment/recovery, eradicating malicious code, and conducting tactical forensics. The challenge of protecting the systems and networks of the tactical internet from information attacks is the ever increasing number and types of attacks.

4. SENSOR/INFORMATION NETWORK KEYS AND INITIAL CAPABILITIES

The existence of an array of networked sensors and a management information system by themselves will not ensure the victory in a network centric warfare scenario. The sensor network and management information system must be utilized appropriately. The utilization of the information network centric warfare resources is key to the victory.

The first key is the converting of sensor data to useful information. The processing capability that generates the information from sensor data and archival data bases must not only be fast and efficient, but also must be intelligent. The cognitive process of creating knowledge from information should be based on the information needs of the various levels of the command structure. Full frame video may be of value to a tank commander, but only an icon on a digital map may be needed by the division commander. Similarly, the axis of the enemy advance is valuable information, but knowledge of all possible variations in the route would be much more valuable to the commander. Lists of available indirect and direct fire support and servicing profiles are necessary for informed command decisions and contribute to battle knowledge. The creation of knowledge coupled with a sustained information distribution environment permits collaborative planning and mission rehearsal. The real time capability of such an asset then allows real time adjustments to any combat exigency.

Another key to successful implementation and utilization of a combat information network is the set of characteristics of the network itself. The information transmitted across the net must be structured to accommodate the bandwidth of the network. Information and network assets have to be dynamically allocated, have object oriented architecture for versatility and compliant protocols. In addition, routing and distribution of messages must ensure that the correct message gets to the appropriate user in a timely manner. There can be no backlog of inputs to the commander's decision making nor from the commander to the execution unit commander. Finally, all these capabilities and characteristics must be provided in an information assurance environment. Information and data have to be sent and received uncorrupted and uncompromised. A combat information network that does not assure the integrity of the information passed is a serious liability that can allow catastrophic defeat.

The characteristics of the information network mentioned above set the requirements on the command, control, communications, computer, surveillance, intelligence, and reconnaissance (C4SIR) network. The ultimate C4SIR network capable of prosecuting the network centric warfare envisioned will take time and resources before implementation and fielding. However, there are several thrusts in the US Army R&D community that will realize a first step capability for network centric warfare in the initial fielding of the FCS. The sensing technologies are available such that the sensing of the battlespace and collecting of the sensor data can be realized in the near term. The use of sensor data and information will become a component of the initial command and control architecture for battle management. Capability for an adaptive robust on-the-move network is also envisioned in the near term. Reductions in the C4SIR footprint can also be demonstrated by versatility in network allocations and graceful degradation, logistics simplifications, dynamic power allocation, and other innovative and technologically realizable concepts.

5. ARMY TECHNOLOGY PROGRAMS

The Communications-Electronics Command's (CECOM) Research, Development & Engineering Center (RDEC) has a number of tech base programs to support the fielding of the FCS system of systems concept in the 2010 time frame. Eleven of the most relevant Strategic Technology Objectives (STOs), Advanced Technology Demonstrators (ATDs) and other Advanced Concepts Technology Demonstrations (ACTDs) efforts are briefly described in this section.

5.1 Joint Intelligence Surveillance & Reconnaissance (JISR)

JISR is a program to provide the warfighter with a comprehensive near-real time view of the intelligence, surveillance and reconnaissance sensor information. Access to data from a combination of national, joint and tactical resources to enhance situation awareness will be available. Besides sensor information, JISR provides information management and integrated software to increase the warfighter's understanding of enemy operations in an expanded battlespace.

5.2 Agile Commander (Command Post XXI)

Agile Commander, previously known as Command Post XXI, is an effort to develop and demonstrate command and control (C2) applications for a functionally and physically agile, rapidly deployable, split-based headquarters. It will enable the commander to execute distributed operations for any level of military operations. C2 tools will include rapid development and analysis of course of action, wargaming and execution monitoring; enterprise information and mobile adaptive computing capabilities enabling C2 systems to conduct operations on-the-move by the commander and staff.

5.3 Logistics Command and Control (Log C2)

Log C2 will develop, demonstrate and transition products that will revolutionize military logistics through information dominance. The objective is to enable the commander to shorten the operations decision cycle and optimize resources. Automated logistics data down to the distributor unit level will be provided.

5.4 Integrated Power Generation & Management

Integrated power management is defined as the planning, organization and control of energy efficient technologies and techniques across all elements of power: sources, storage, distribution and consumption. This includes: (1) hybrids and alternative power sources, (2) electromechanical and (3) power management which includes low power electronics design tools and techniques; low power devices, subsystems and systems; and optimization of system architecture/design and user conservation practices to achieve power and operational efficiencies.

5.5 Integrated Situation Awareness & Targeting (ISAT)

ISAT will demonstrate Horizontal Technology Integration RF, missile and laser warning upgrades to existing threat warning systems. It will provide significantly improved precision hostile situation awareness, target acquisition, geolocation and

combat identification assist for active emitters. Fusion of pre-flight and real time C3I links with on-board emitter fingerprinting will provide enhanced combat ID information to meet rules of engagement and allow weapons release at maximum ranges. Real time bi-directional C4I feeds to the digitized battlefield will provide ground commanders and vehicles with targeting feeds from combined arms systems equipped with ISAT capability.

5.6 Multifunctional On-the-Move Secure Adaptive Integrated Communications (MOSAIC)
Mosaic will demonstrate mobile communications for the battle command infrastructure to support the Objective Force/FCS. There are three focus areas: (1) Bandwidth management – scaled bandwidth request based on precedence, support of bandwidth reservation, proxies to drive bandwidth aware applications, and the addressing of IP quality of service over tactical wireless links. (2) Adaptive network protocols to support infrastructure security. (3) Integration of commercial and DOD developed wireless technologies.

5.7 Countermine
The FCS mine detection and neutralization effort has the goal of providing FCS vehicles with forward looking mine detection at stand off distances and neutralization capability with rates of advance an order of magnitude greater than today's capability. The effort is investigating phenomenology and developing new models and collecting empirical field data with new forward looking sensors. New signal processing techniques and clutter rejection and discrimination algorithms will be developed and new mine neutralization techniques applicable to elimination of on/off route surface and buried antitank mines will be investigated.

5.8 Long range on-board targeting
The premier long range targeting system for combat vehicles being developed is the Multifunction Staring Sensor Suite (MFS3). MFS3 will demonstrate a modular, reconfigurable sensor suite utilizing sensor fusion and multiple advanced sensor components, including staring dual band infrared arrays, eyesafe laser rangefinder, range mapper, multispectral aided target recognition (ATR) algorithms and acoustic arrays. MFS3 performance will provide ground vehicles with a compact, affordable sensor suite for long range non-cooperative target identification, low signature target acquisition, mortar/sniper fire location, and air defense targeting against low signature UAVs and long range helicopters.

5.9 Networked Sensors for FCS
The capstone thrust for a complete array of sensors for FCS and the Objective Force is developing and integrating off board sensor packages onto mobile platforms (e.g. UGVs, mini UAVs, UGS) into a system of systems that can be networked throughout complex terrain (including MOUT). This capability provides the commander reliable and responsive near real time situational awareness for direct and indirect fire weapons and threat avoidance. The off board sensors provide remote monitoring of areas out to approximately 10km without placing soldiers in harm's way, increases a unit's area of coverage (a force multiplier) and situation awareness data for targeting of beyond line of sight weapons and early warning to speed decision making and reaction time.

5.10 Tactical C2 Protect
This ATD will develop, integrate, validate and demonstrate hardware and software that protect the systems and networks of the Objective Force/FCS from modern network attacks. Commercial-off-the-self and DOD programs that target network security technologies will be leveraged. The protect portion of the demonstration will include an integrated security architecture that provides advanced network access control, detection/response and security management within tactical communications networks. The attack portion of the demonstration will be an integrated system that can launch both RF and wire based attacks against threat information systems.

5.11 Enroute Mission Planning & Rehearsal System (EMPRS)
EMPRS provides the ability for a deploying light force to begin the process in garrison by modifying existing plans and, in a seamless fashion, continue to update the plan while at the loading ramp and during the 10 to 15 hour transport phase. This is accomplished without the loss of any of the pre-planning and rehearsal information and with the capability to incorporate the latest intelligence changes while enroute. The best course of action is selected and collaboration is conducted between echelons in the enroute force and with ground commanders. Using EMPRS, the arriving force is ready to immediately engage the threat with fully coordinated and updated plans, significantly increasing their combat effectiveness.

5.12 Battlespace Tactical Navigation (BTN)
The Battlespace Navigation STO will develop technology and integration concepts that improve the robustness of navigation systems and minimize registration errors between sensors and data bases and, hence, ensure the integrity of blue force

situation awareness. Under the BTN program, Global Positioning System (GPS) signal reception in hostile electronic countermeasures (ECM) environments will be provided by the deployment of ground-based pseudolites and the incorporation of advanced anti-jam GPS technology (i.e. filter, antennas and low-power clocks). Back up navigation capabilities will be provided via the integration of emerging low cost devices suitably scaled to the platform and mission requirements. Sensor/data base registration error minimization will be provided for via the development of advanced software algorithms that recognize distinguishable features, determine offsets and apply corrections.

6. SUMMARY

The Future Combat System and the Objective Force are System of Systems. The design of weapons, sensors, communications, and logistics must be considered in a total system of systems concept. The key to victory will be through information superiority in network centric warfare. Critical enablers for information superiority are integrated sensors and information management. The US Army is committed to the transformation of our "Industrial Age" Cold War force to an "Information Age" force at the earliest possible date. ***There will be an information revolution on the battlefield.***

---

[1] Louis C. Marquet and James A. Ratches, "Future directions of information systems in the Army After Next", Proc. SPIE, Vol. 3393, pp. 20-26, 1998.
[2] Louis C. Marquet and James A. Ratches, "Sensor systems for the digital battlefield", Proc. SPIE, Vol. 3080, pp. 6-15, 1997.
[3] *Cyberwar: Security, Strategy and Conflict in the Information Age,* edited by Campen, Dearth and Goodden, "From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift" by Phillipe Baumard, pp. 147, AFCEA International Press, Fairfax, VA, 1996.
[4] "Full Spectrum Protection for 2025 Era Ground Combat Vehicles", Report of FY99 Army Science Board Summer Study, 16 July 1999.